IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Klaus Finkenzeller, et al.	
U.S. Patent No.:	8,581,706	Attorney Docket No.: 39843-0132IP1
Issue Date:	November 12, 2013	
Appl. Serial No.:	12/304,653	
Filing Date:	March 4, 2009	
Title:	DATA STORAGE MEDIUM AND METHOD FOR CONTACTLESS COMMUNICATION BETWEEN THE DATA STORAGE MEDIUM AND A READER	

DECLARATION OF JUNE ANN MUNFORD

INTRODUCTION

1. My name is June Ann Munford. I am over the age of 18, have personal knowledge of the facts set forth herein, and am competent to testify to the same.

2. I earned a Master of Library and Information Science (MLIS) from the University of Wisconsin-Milwaukee in 2009. I have over ten years of experience in the library/information science field. Beginning in 2004, I have served in various positions in the public library sector including Assistant Librarian, Youth Services Librarian and Library Director. I have attached my Curriculum Vitae as Appendix CV.

3. During my career in the library profession, I have been responsible for materials acquisition for multiple libraries. In that position, I have cataloged, purchased and processed incoming library works. That includes purchasing materials directly from vendors, recording publishing data from the material in question, creating detailed material records for library catalogs and physically preparing that material for circulation. In addition to my experience in acquisitions, I was also responsible for analyzing large collections of library materials, tailoring library records for optimal catalog

search performance and creating lending agreements between libraries during my time as a Library Director.

4. I am familiar with the Internet Archive, a digital library formally certified by the State of California as a public library. Among other services that the Internet Archive makes available to the general public is the Wayback Machine, an online archive. The Internet Archive's Wayback Machine service archives webpages as of a certain capture date to track changes in the web over time. The Internet Archive has been in operation as a nonprofit library since 1996 and has hosted the Wayback Machine service since its inception in 2001. During my time as a librarian, I frequently used the Internet Archive's Wayback Machine for research and instruction purposes. This includes teaching instructional classes on using the Wayback Machine to library patrons and using the Wayback Machine to research reference inquiries that require hard-to-find online resources. I consider the Internet Archive's recordskeeping to be as rigorous and detailed as other formal library recordskeeping practices such as MARC records, OCLC records and Dublin Core.

5. I have been retained by Fish & Richardson P.C. on behalf of Samsung Electronics Co., Ltd. ("Petitioner" or "Samsung"). I understand that

Samsung is requesting that the Patent Trial and Appeal Board ("PTAB") or "Board") institute an *inter partes* review ("IPR") proceeding of U.S. Patent No. 8,581,706 ("the '706 patent").

6. I am being compensated for my services in this matter at the rate of $100.00 per hour plus reasonable expenses. My statements are objective, and my compensation does not depend on the outcome of this matter.

7. I have been asked to provide assistance in authenticating and assessing the public accessibility of the following three documents, which I understand to be cited in Samsung's IPR petition against the '706 patent:

a. **Exhibit SAMSUNG-1011**: *Java Card 2.1 Runtime Environment (JCRE) Specification (Revision 1.0)* by Sun Microsystems

b. **Exhibit SAMSUNG-1012**: *Java Card 2.1 Virtual Machine Specification (Revision 1.0)* by Sun Microsystems

c. **Exhibit SAMSUNG-1013**: *Java Card 2.1 Application Programming Interface (Revision 1.0)* by Sun Microsystems

d. **Exhibit SAMSUNG-1009**: *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification* by Klaus Finkenzeller

AUTHENTICATION OF EXHIBIT SAMSUNG-1011: *Java Card 2.1 Runtime Environment (JCRE) Specification (Revision 1.0)*

8. I have reviewed Exhibit **SAMSUNG-1011**, a document entitled *Java Card 2.1 Runtime Environment (JCRE) Specification (Revision 1.0)* by Sun Microsystems.

9. Attached hereto as Appendix JCRE01 is a PDF copy of *Java Card 2.1 Runtime Environment (JCRE) Specification (Revision 1.0)* titled 'jcre.pdf'. I secured this file myself from http://aszt.inf.elte.hu/~javabook/java-1.2/javacard/standard/pdf/jcre.pdf. In comparing 'jcre.pdf' to Exhibit SAMSUNG-1011, it is my determination that Exhibit SAMSUNG-1011 is a true and correct copy of *Java Card 2.1 Runtime Environment (JCRE) Specification (Revision 1.0)* by Sun Microsystems.

AUTHENTICATION OF EXHIBIT SAMSUNG-1012: *Java Card 2.1 Virtual Machine Specification (Revision 1.0)*

10. I have reviewed Exhibit SAMSUNG-1012, a document entitled *Java Card 2.1 Virtual Machine Specification (Revision 1.0)* by Sun Microsystems.

11. Attached hereto as Appendix JCVM01 is a PDF copy of *Java Card 2.1 Virtual Machine Specification (Revision 1.0)* titled 'jcvm.pdf'. I secured this file myself from http://aszt.inf.elte.hu/~javabook/java-1.2/javacard/standard/pdf/jcvm.pdf. In comparing 'jcvm.pdf' to Exhibit SAMSUNG-1012, it is my determination that Exhibit SAMSUNG-1012 is a true and correct copy of *Java Card 2.1 Virtual Machine Specification (Revision 1.0)* by Sun Microsystems.

AUTHENTICATION OF EXHIBIT SAMSUNG-1013: *Java Card 2.1 Application Programming Interface (Revision 1.0)*

12. I have reviewed Exhibit SAMSUNG-1013, a document entitled *Java Card 2.1 Application Programming Interface (Revision 1.0)* by Sun Microsystems.

13. Attached hereto as Appendix JCAPI01 is a PDF copy of *Java Card 2.1 Application Programming Interface (Revision 1.0)* titled 'jcapi.pdf'. I secured this file myself from http://aszt.inf.elte.hu/~javabook/java-1.2/javacard/standard/pdf/jcapi.pdf. In comparing 'jcapi.pdf' to Exhibit SAMSUNG-1013, it is my determination that Exhibit SAMSUNG-1013 is a true and correct copy of *Java Card 2.1 Application Programming Interface (Revision 1.0)* by Sun Microsystems.

PUBLIC AVAILABILITY OF EXHIBITS SAMSUNG-1011, SAMSUNG-1012, SAMSUNG-1013

14. Attached hereto as Appendix JCAPI02 is a PDF copy of *Java Card 2.1 Application Programming Interface (Revision 1.0)* entitled 'JavaCard21API.pdf'. I secured this copy of *Java Card 2.1 Application Programming Interface (Revision 1.0)* from the Internet Archive's Wayback Machine at https://web.archive.org/web/20030611045849/http://java.sun.com/products/javacard/JavaCard21API.pdf. In comparing 'JavaCard21API.pdf'to Appendix JCAPI01 and Exhibit SAMSUNG-1013, it is my determination that Appendix JCAPI02 is a true and correct copy of *Java Card 2.1 Application Programming Interface (Revision 1.0).*

15. Attached hereto as Appendix JCAPI03 is the Internet Archive record for 'JavaCard21API.pdf' found at http://java.sun.com/products/javacard/JavaCard21API.pdf. I secured these screen captures myself from https://web.archive.org/web/20030611045849/http://java.sun.com/products/javacard/JavaCard21API.pdf. Based on this record, The Internet Archive first preserved http://java.sun.com/products/javacard/JavaCard21API.pdf as of June 11, 2003, ensuring public access to *Java Card 2.1 Application Programming Interface (Revision 1.0)* as of June 11, 2003.

16. Attached hereto as Appendix JCAPI04 is the Internet Archive record for 'Java Card 2.1 Platform' found at http://www.java.sun.com/products/javacard/javacard21.html. I secured these screen captures myself from https://web.archive.org/web/19991103041851/http:/www.java.sun.com:80/products/javacard/javacard21.html. Based on this record, The Internet Archive first preserved http://www.java.sun.com/products/javacard/javacard21.html as of November 3, 1999.

17. On page 2 of the record included in Appendix JCAPI04 under the heading 'Java Card 2.1 Platform Documentation', there are several web links to the JavaCard 2.1 documentation discussed in this declaration: 'Java Card 2.1 API Specification (in a single PDF file)', 'Java Card 2.1 Runtime Environment (JCRE) Specification (PDF)' and 'Java Card 2.1 Virtual Machine (JCVM) Specification (PDF)'. If a user were to follow the link entitled 'Java Card 2.1 API Specification (in a single PDF file)', the Internet Archive presents 'JavaCard21API.pdf', a true and correct copy of *Java Card 2.1 Application Programming Interface (Revision 1.0)* as presented in Appendix JCAPI02.

18. The record presented in JCAPI04 was first preserved by the Internet Archive as of November 3, 1999. Considering the page entitled 'Java Card 2.1 Platform' as presented in Appendix JCAPI04 advertises and features a direct link to a copy of *Java Card 2.1 Application Programming Interface (Revision 1.0)* and that copy is identical to the versions of *Java Card 2.1 Application Programming Interface (Revision 1.0)* presented in Exhibit SAMSUNG-1013 and Appendix JCAPI01, it is my determination that Sun Microsystems first made *Java Card 2.1 Application Programming Interface (Revision 1.0)* available and accessible to the public as of November 3, 1999 if not earlier.

19. Although the Internet Archive does not feature full PDF copies of *Java Card 2.1 Runtime Environment (JCRE) Specification (Revision 1.0)* or *Java Card 2.1 Virtual Machine Specification (Revision 1.0)* in their records, the Sun Microsystems page entitled 'Java Card 2.1 Platform Documentation' presented as Appendix JCAPI04 does advertise and present a link to both documents in the same fashion as *Java Card 2.1 Application Programming Interface (Revision 1.0)*. As such, it is also my determination that *Java Card 2.1 Runtime Environment (JCRE) Specification (Revision 1.0)* and *Java Card 2.1 Virtual Machine Specification (Revision 1.0)* were both made accessible and available to the public by Sun Microsystems as of November 3, 1999 if not earlier.

AUTHENTICATION AND PUBLIC AVAILABILITY OF EXHIBIT SAMSUNG-1009: *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification* by Klaus Finkenzeller

20. I have reviewed Exhibit SAMSUNG-1009, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification* by Klaus Finkenzeller, 2nd Edition.

21. Attached hereto as Appendix FINKENZELLER01 is a true and correct copy of the MARC record for *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification* as held by the Penn State University library. I secured this record myself from the library's public catalog. The MARC record contained within Appendix FINKENZELLER01 accurately describes the title, author, publisher, and ISBN number of *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd Edition.

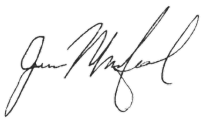
22. Attached hereto as Appendix FINKENZELLER02 is a true and correct copy of selections from *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd Edition. I secured these scans myself from Penn State University's holdings for *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*. In comparing Exhibit SAMSUNG-1009 to Appendix FINKENZELLER02, it is my determination that Exhibit SAMSUNG-1009 is a true and correct copy of *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd Edition by Klaus Finkenzeller.

23. The 008 field of the MARC record in Appendix FINKENZELLER01 indicates the date of record creation. The 008 field of Appendix FINKENZELLER01 indicates Penn State University library first acquired this book as of December 10, 2002. Considering this information, it is my determination that *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification,* 2nd Edition was made available to the public shortly after its initial acquisition in December 2002.

CONCLUSION

24. I declare under penalty of perjury that the foregoing is true and correct. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of this proceeding.

Dated: 4/28/2022



June Ann Munford

J. Munford
Curriculum Vitae

Education

University of Wisconsin-Milwaukee - MS, Library & Information Science, 2009
Milwaukee, WI

- Coursework included cataloging, metadata, data analysis, library systems, management strategies and collection development.
- Specialized in library advocacy, cataloging and public administration.

Grand Valley State University - BA, English Language & Literature, 2008
Allendale, MI

- Coursework included linguistics, documentation and literary analysis.
- Minor in political science with a focus in local-level economics and government.

Professional Experience

Researcher / Expert Witness, October 2017 – present
Freelance ● Pittsburgh, Pennsylvania & Grand Rapids, Michigan

- Material authentication and public accessibility determination. Declarations of authenticity and/or public accessibility provided upon research completion. Experienced with appeals and deposition process.

- Research provided on topics of public library operations, material publication history, digital database services and legacy web resources.

- Past clients include Alston & Bird, Arnold & Porter, Baker Botts, Fish & Richardson, Erise IP, Irell & Manella, O'Melveny & Myers, Perkins-Coie, Pillsbury Winthrop Shaw Pittman and Slayden Grubert Beard.

Library Director, February 2013 - March 2015
Dowagiac District Library ● Dowagiac, Michigan

- Executive administrator of the Dowagiac District Library. Located in

Southwest Michigan, this library has a service area of 13,000, an annual operating budget of over $400,000 and total assets of approximately $1,300,000.

● Developed careful budgeting guidelines to produce a 15% surplus during the 2013-2014 & 2014-2015 fiscal years while being audited.

● Using this budget surplus, oversaw significant library investments including the purchase of property for a future building site, demolition of existing buildings and building renovation projects on the current facility.

● Led the organization and digitization of the library's archival records.

● Served as the public representative for the library, developing business relationships with local school, museum and tribal government entities.

● Developed an objective-based analysis system for measuring library services - including a full collection analysis of the library's 50,000+ circulating items and their records.

November 2010 - January 2013
Librarian & Branch Manager, Anchorage Public Library ● Anchorage, Alaska

● Headed the 2013 Anchorage Reads community reading campaign including event planning, staging public performances and creating marketing materials for mass distribution.

● Co-led the social media department of the library's marketing team, drafting social media guidelines, creating original content and instituting long-term planning via content calendars.

● Developed business relationships with The Boys & Girls Club, Anchorage School District and the US Army to establish summer reading programs for children.

June 2004 - September 2005, September 2006 - October 2013
Library Assistant, Hart Area Public Library
Hart, MI

● Responsible for verifying imported MARC records and original MARC

cataloging for the local-level collection as well as the Michigan Electronic Library.

● Handled OCLC Worldcat interlibrary loan requests & fulfillment via ongoing communication with lending libraries.

Professional Involvement

Alaska Library Association - Anchorage Chapter
- Treasurer, 2012

Library Of Michigan
- Level VII Certification, 2008
- Level II Certification, 2013

Michigan Library Association Annual Conference 2014
- New Directors Conference Panel Member

Southwest Michigan Library Cooperative
- Represented the Dowagiac District Library, 2013-2015

Professional Development

Library Of Michigan Beginning Workshop, May 2008
Petoskey, MI
- Received training in cataloging, local history, collection management, children's literacy and reference service.

Public Library Association Intensive Library Management Training, October 2011
Nashville, TN
- Attended a five-day workshop focused on strategic planning, staff management, statistical analysis, collections and cataloging theory.

Alaska Library Association Annual Conference 2012 - Fairbanks, February 2012
Fairbanks, AK
- Attended seminars on EBSCO advanced search methods, budgeting, cataloging, database usage and marketing.

Depositions

2019 ● Fish & Richardson
IPR Petitions of 865 Patent, Apple v. Qualcomm (IPR2018-001281 / 39521-00421IP & IPR2018-01282 / 39521-00421IP2)

2019 ● Erise IP
Implicit, LLC v. Netscout Systems, Inc (Civil Action No. 2:18-cv-53-JRG)

2019 ● Perkins-Coie
Adobe Inc. v. RAH Color Technologies LLC (Cases IPR2019-00627, IPR2019-00628, IPR2019-00629 and IPR2019-00646)

2020 ● O'Melveny & Myers
Maxell, Ltd. v. Apple Inc. (Case 5:19-cv-00036-RWS)

2021 ● Pillsbury Winthrop Shaw Pittman LLP
Intel v. SRC (Case IPR2020-1449)

Limited Case History & Potential Conflicts

Alston & Bird
- Nokia (v. Neptune Subsea, Xtera)

Arnold & Porter
- Ivantis (v. Glaukos)

Erise I.P.
- Apple
  - v. Future Link Systems (IPRs 6317804, 6622108, 6807505, and 7917680)
  - v. INVT
  - v. Navblazer LLC (Case No. IPR2020-01253)

v. Qualcomm (IPR2018-001281, 39521-00421IP, IPR2018-01282, 39521-00421IP2)

v. Quest Nettech Corp, Wynn Technologies (Case No. IPR2019-00XXX, RE. Patent Re38137)

- Fanduel (v CGT)

- Garmin (v. Phillips North America LLC, Case No. 2:19-cv-6301-AB-KS Central District of California)

- Netscout

  v. Longhorn HD LLC)

  v. Implicit, LLC (Civil Action No. 2:18-cv-53-JRG)

- Sony Interactive Entertainment LLC

  v. Bot M8 LLC

  v. Infernal Technology LLC

- Unified Patents (v GE Video Compression, Civil Action No. 2:19-cv-248)

Fish & Richardson

- Apple

  v. LBS Innovations

  v. Masimo (IPR 50095-0012IP1, 50095-0012IP2, 50095-0013IP1, 50095-0013IP2, 50095-0006IP1)

  v. Neonode

  v. Qualcomm (IPR2018-001281, 39521-00421IP, IPR2018-01282, 39521-00421IP2)

- Dish Network

  v. Realtime Adaptive Streaming, Case No 1:17-CV-02097-RBJ)

v. TQ Delta LLC

- Huawei (IPR 76933211)
- Kianxis
- LG Electronics (v. Bell Northern Research LLC, Case No. 3:18-cv-2864-CAB-BLM)
- Metaswitch
- MLC Intellectual Property (v. MicronTech, Case No. 3:14-cv-03657-SI)
- Realtek Semiconductor
- Quectel
- Samsung (v. Bell Northern Research, Civil Action No. 2:19-cv-00286-JRG)
- Texas Instruments

Irell & Manella

- Curium

O'Melveny & Myers

- Apple (v. Maxell, Case 5:19-cv-00036-RWS)

Perkins-Coie

- TCL Industries (v. Koninklijke Philips NV, PTAB Case Nos. IPR2021-00495, IPR2021-00496, and IPR2021-00497)

Pillsbury Winthrop Shaw Pittman

- Intel (v. FG SRC LLC, Case No. 6:20-cv-00315 W.D. Tex)

Java Card 2.1 Application Programming Interface

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303 USA
650 960-1300

Final Revision 1.0, February 24, 1999

Appendix JCAPI01

Java Card API

Table of Contents

Java Card™ 2.1 Platform API Specification

Final Revision 1.0

This document is the specification for the Java Card 2.1 Application Programming Interface.

See:

Description

Packages	
java.lang	Provides classes that are fundamental to the design of the Java Card technology subset of the Java programming language.
javacard.framework	Provides framework of classes and interfaces for the core functionality of a Java Card applet.
javacard.security	Provides the classes and interfaces for the Java Card security framework.
javacardx.crypto	Extension package containing security classes and interfaces for export-controlled functionality.

This document is the specification for the Java Card 2.1 Application Programming Interface.

Java Card 2.1 API Notes

Referenced Standards

ISO - International Standards Organization

- Information Technology - Identification cards - integrated circuit cards with contacts: ISO 7816
- Information Technology - Security Techniques - Digital Signature Scheme Giving Message Recovery: ISO 9796
- Information Technology - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm: ISO 9797
- Information technology - Security techniques - Digital signatures with appendix : ISO 14888

RSA Data Security, Inc.

- RSA Encryption Standard: PKCS #1 Version 2.0
- Password-Based Encryption Standard: PKCS #5 Version 1.5

EMV

- The EMV ’96 ICC Specifications for Payments systems Version 3.0

IPSec

- The Internet Key Exchange (IKE) document RFC 2409 (STD 1)

Standard Names for Security and Crypto

- SHA (also SHA-1): Secure Hash Algorithm, as defined in Secure Hash Standard, NIST FIPS 180-1.
- MD5: The Message Digest algorithm RSA-MD5, as defined by RSA DSI in RFC 1321.
- RIPEMD-160 : as defined in ISO/IEC 10118-3:1998 Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions
- DSA: Digital Signature Algorithm, as defined in Digital Signature Standard, NIST FIPS 186.
- DES: The Data Encryption Standard, as defined by NIST in FIPS 46-1 and 46-2.
- RSA: The Rivest, Shamir and Adleman Asymmetric Cipher algorithm.

Parameter Checking

Policy

All Java Card API implementations must conform to the Java model of parameter checking. That is, the API code should not check for those parameter errors which the VM is expected to detect. These include all parameter errors, such as null pointers, index out of bounds, and so forth, that result in standard runtime exceptions. The runtime exceptions that are thrown by the Java Card VM are:

- ArithmeticException
- ArrayStoreException
- ClassCastException
- IllegalArgumentException
- IllegalStateException
- IndexOutOfBoundsException
- ArrayIndexOutOfBoundsException
- NegativeArraySizeException
- NullPointerException
- SecurityException

Exceptions to the Policy

In some cases, it may be necessary to explicitly check parameters. These exceptions to the policy are documented in the Java Card API specification. A Java Card API implementation must not perform parameter checking with the intent to avoid runtime exceptions, unless this is clearly specified by the Java Card API specification.

Note: If multiple erroneous input parameters exist, any one of several runtime exceptions will be thrown by the VM. Java programmers rely on this behavior, but they do not rely on getting a specific exception. It is not necessary (nor is it reasonable or practical) to document the precise error handling for all possible combinations of equivalence classes of erroneous inputs. The value of this behavior is that the logic error in the calling program is detected and exposed via the runtime exception mechanism, rather than being masked by a normal return.

Hierarchy For All Packages

Package Hierarchies:

java.lang, javacard.framework, javacard.security, javacardx.crypto

Class Hierarchy

- class java.lang.**Object**
  - class javacard.framework.**AID**
  - class javacard.framework.**APDU**
  - class javacard.framework.**Applet**
  - class javacardx.crypto.**Cipher**
  - class javacard.framework.**JCSystem**
  - class javacard.security.**KeyBuilder**
  - class javacard.security.**MessageDigest**
  - class javacard.framework.**OwnerPIN** (implements javacard.framework.PIN)
  - class javacard.security.**RandomData**
  - class javacard.security.**Signature**
  - class java.lang.**Throwable**
    - class java.lang.**Exception**
      - class javacard.framework.**CardException**
        - class javacard.framework.**UserException**
      - class java.lang.**RuntimeException**
        - class java.lang.**ArithmeticException**
        - class java.lang.**ArrayStoreException**
        - class javacard.framework.**CardRuntimeException**
          - class javacard.framework.**APDUException**
          - class javacard.security.**CryptoException**
          - class javacard.framework.**ISOException**
          - class javacard.framework.**PINException**
          - class javacard.framework.**SystemException**
          - class javacard.framework.**TransactionException**
        - class java.lang.**ClassCastException**
        - class java.lang.**IndexOutOfBoundsException**
          - class java.lang.**ArrayIndexOutOfBoundsException**
        - class java.lang.**NegativeArraySizeException**
        - class java.lang.**NullPointerException**
        - class java.lang.**SecurityException**
  - class javacard.framework.**Util**

Interface Hierarchy

- interface javacard.security.**DSAKey**
  - interface javacard.security.**DSAPrivateKey**(also extends javacard.security.PrivateKey)
  - interface javacard.security.**DSAPublicKey**(also extends javacard.security.PublicKey)
- interface javacard.framework.**ISO7816**
- interface javacard.security.**Key**
  - interface javacard.security.**PrivateKey**
    - interface javacard.security.**DSAPrivateKey**(also extends javacard.security.DSAKey)
    - interface javacard.security.**RSAPrivateCrtKey**
    - interface javacard.security.**RSAPrivateKey**
  - interface javacard.security.**PublicKey**
    - interface javacard.security.**DSAPublicKey**(also extends javacard.security.DSAKey)
    - interface javacard.security.**RSAPublicKey**
  - interface javacard.security.**SecretKey**
    - interface javacard.security.**DESKey**
- interface javacardx.crypto.**KeyEncryption**
- interface javacard.framework.**PIN**
- interface javacard.framework.**Shareable**

Package java.lang

Provides classes that are fundamental to the design of the Java Card technology subset of the Java programming language.

See:

Description

Class Summary	
Object	Class `Object` is the root of the Java Card class hierarchy.
Throwable	The Throwable class is the superclass of all errors and exceptions in the Java Card subset of the Java language.

Exception Summary	
ArithmeticException	A JCRE owned instance of `ArithmethicException` is thrown when an exceptional arithmetic condition has occurred.
ArrayIndexOutOfBoundsException	A JCRE owned instance of `IndexOutOfBoundsException` is thrown to indicate that an array has been accessed with an illegal index.
ArrayStoreException	A JCRE owned instance of `ArrayStoreException` is thrown to indicate that an attempt has been made to store the wrong type of object into an array of objects.
ClassCastException	A JCRE owned instance of `ClassCastException` is thrown to indicate that the code has attempted to cast an object to a subclass of which it is not an instance.
Exception	The class `Exception` and its subclasses are a form of `Throwable` that indicates conditions that a reasonable applet might want to catch.
IndexOutOfBoundsException	A JCRE owned instance of `IndexOutOfBoundsException` is thrown to indicate that an index of some sort (such as to an array) is out of range.
NegativeArraySizeException	A JCRE owned instance of `NegativeArraySizeException` is thrown if an applet tries to create an array with negative size.
NullPointerException	A JCRE owned instance of `NullPointerException`is thrown when an applet attempts to use `null` in a case where an object is required.
RuntimeException	`RuntimeException` is the superclass of those exceptions that can be thrown during the normal operation of the Java Card Virtual Machine. A method is not required to declare in its throws clause any subclasses of `RuntimeException` that might be thrown during the execution of the method but not caught.
SecurityException	A JCRE owned instance of `SecurityException` is thrown by the Java Card Virtual Machine to indicate a security violation. This exception is thrown when an attempt is made to illegally access an object belonging to a another applet.

Package java.lang Description

Provides classes that are fundamental to the design of the Java Card technology subset of the Java programming language.

---

java.lang
Class ArithmeticException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--java.lang.ArithmeticException
```

public class **ArithmeticException**
extends RuntimeException

A JCRE owned instance of `ArithmethicException` is thrown when an exceptional arithmetic condition has occurred. For example, a "divide by zero" is an exceptional arithmentic condition.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`ArithmeticException``()` Constructs an `ArithmeticException`.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

ArithmeticException

`public` **`ArithmeticException`**`()`

Constructs an `ArithmeticException`.

---

java.lang
Class ArrayIndexOutOfBoundsException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--java.lang.IndexOutOfBoundsException
                          |
                          +--java.lang.ArrayIndexOutOfBoundsException
```

public class **ArrayIndexOutOfBoundsException**
extends IndexOutOfBoundsException

A JCRE owned instance of `IndexOutOfBoundsException` is thrown to indicate that an array has been accessed with an illegal index. The index is either negative or greater than or equal to the size of the array.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`ArrayIndexOutOfBoundsException``()` Constructs an `ArrayIndexOutOfBoundsException`.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

ArrayIndexOutOfBoundsException

`public` **`ArrayIndexOutOfBoundsException`**`()`

Constructs an `ArrayIndexOutOfBoundsException`.

---

java.lang
Class ArrayStoreException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--java.lang.ArrayStoreException
```

public class **ArrayStoreException**
extends RuntimeException

A JCRE owned instance of `ArrayStoreException` is thrown to indicate that an attempt has been made to store the wrong type of object into an array of objects. For example, the following code generates an `ArrayStoreException`:

```
Object x[] = new AID[3];
x[0] = new OwnerPIN( (byte) 3, (byte) 8);
```

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`ArrayStoreException``()` Constructs an `ArrayStoreException`.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

ArrayStoreException

`public` **`ArrayStoreException`**`()`

Constructs an `ArrayStoreException`.

---

java.lang
Class ClassCastException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--java.lang.ClassCastException
```

public class **ClassCastException**
extends RuntimeException

A JCRE owned instance of `ClassCastException` is thrown to indicate that the code has attempted to cast an object to a subclass of which it is not an instance. For example, the following code generates a `ClassCastException`:

```
Object x = new OwnerPIN( (byte)3, (byte)8);
JCSystem.getAppletShareableInterfaceObject( (AID)x, (byte)5 );
```

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`ClassCastException``()` Constructs a `ClassCastException`.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

ClassCastException

`public` **`ClassCastException`**`()`

Constructs a `ClassCastException`.

---

java.lang
Class Exception

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
```

Direct Known Subclasses:
CardException, RuntimeException

public class **Exception**
extends Throwable

The class `Exception` and its subclasses are a form of `Throwable` that indicates conditions that a reasonable applet might want to catch.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`Exception``()` Constructs an `Exception` instance.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

Exception

`public` **`Exception`**`()`

Constructs an `Exception` instance.

java.lang
Class IndexOutOfBoundsException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--java.lang.IndexOutOfBoundsException
```

Direct Known Subclasses:
ArrayIndexOutOfBoundsException

---

public class **IndexOutOfBoundsException**
extends RuntimeException

A JCRE owned instance of `IndexOutOfBoundsException` is thrown to indicate that an index of some sort (such as to an array) is out of range.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`IndexOutOfBoundsException``()` Constructs an `IndexOutOfBoundsException`.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

IndexOutOfBoundsException

`public` **`IndexOutOfBoundsException`**`()`

Constructs an `IndexOutOfBoundsException`.

---

java.lang
Class NegativeArraySizeException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--java.lang.NegativeArraySizeException
```

public class **NegativeArraySizeException**
extends RuntimeException

A JCRE owned instance of `NegativeArraySizeException` is thrown if an applet tries to create an array with negative size.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`NegativeArraySizeException``()` Constructs a `NegativeArraySizeException`.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

NegativeArraySizeException

```
public NegativeArraySizeException()
```

Constructs a `NegativeArraySizeException`.

---

java.lang
Class NullPointerException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--java.lang.NullPointerException
```

public class **NullPointerException**
extends RuntimeException

A JCRE owned instance of `NullPointerException`is thrown when an applet attempts to use `null` in a case where an object is required. These include:

- Calling the instance method of a `null` object.
- Accessing or modifying the field of a `null` object.
- Taking the length of `null` as if it were an array.
- Accessing or modifying the slots of `null` as if it were an array.
- Throwing `null` as if it were a `Throwable` value.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`NullPointerException``()` Constructs a `NullPointerException`.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

NullPointerException

```
public NullPointerException()
```

Constructs a `NullPointerException`.

---

java.lang
Class Object

java.lang.Object

public class **Object**

Class `Object` is the root of the Java Card class hierarchy. Every class has `Object` as a superclass. All objects, including arrays, implement the methods of this class.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

Object()	

Method Summary

boolean	**equals**(Object obj) Compares two Objects for equality.

Constructor Detail

Object

public **Object**()

Method Detail

equals

public boolean **equals**(Object obj)

Compares two Objects for equality.

The `equals` method implements an equivalence relation:

- It is *reflexive*: for any reference value `x`, `x.equals(x)` should return `true`.
- It is *symmetric*: for any reference values `x` and `y`, `x.equals(y)` should return `true` if and only if `y.equals(x)` returns `true`.
- It is *transitive*: for any reference values `x`, `y`, and `z`, if `x.equals(y)` returns `true` and `y.equals(z)` returns `true`, then `x.equals(z)` should return `true`.
- It is *consistent*: for any reference values `x` and `y`, multiple invocations of `x.equals(y)` consistently return `true` or consistently return `false`.
- For any reference value `x`, `x.equals(null)` should return `false`.

The equals method for class `Object` implements the most discriminating possible equivalence relation on objects; that is, for any reference values `x` and `y`, this method returns `true` if and only if `x` and `y` refer to the same object (`x==y` has the value `true`).

Parameters:

`obj` - the reference object with which to compare.

Returns:

`true` if this object is the same as the obj argument; `false` otherwise.

---

java.lang
Class RuntimeException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
```

Direct Known Subclasses:
ArithmeticException, ArrayStoreException, CardRuntimeException, ClassCastException, IndexOutOfBoundsException, NegativeArraySizeException, NullPointerException, SecurityException

---

public class **RuntimeException**
extends Exception

`RuntimeException` is the superclass of those exceptions that can be thrown during the normal operation of the Java Card Virtual Machine.

A method is not required to declare in its throws clause any subclasses of `RuntimeException` that might be thrown during the execution of the method but not caught.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`RuntimeException``()` Constructs a `RuntimeException` instance.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

RuntimeException

`public` **`RuntimeException`**`()`

Constructs a `RuntimeException` instance.

---

java.lang
Class SecurityException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--java.lang.SecurityException
```

public class **SecurityException**
extends RuntimeException

A JCRE owned instance of `SecurityException` is thrown by the Java Card Virtual Machine to indicate a security violation.

This exception is thrown when an attempt is made to illegally access an object belonging to a another applet. It may optionally be thrown by a Java Card VM implementation to indicate fundamental language restrictions, such as attempting to invoke a private method in another class.

For security reasons, the JCRE implementation may mute the card instead of throwing this exception.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`SecurityException``()` Constructs a `SecurityException`.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

SecurityException

```
public SecurityException()
```

Constructs a `SecurityException`.

java.lang
Class Throwable

```
java.lang.Object
  |
  +--java.lang.Throwable
```

Direct Known Subclasses:
Exception

public class **Throwable**
extends Object

The Throwable class is the superclass of all errors and exceptions in the Java Card subset of the Java language. Only objects that are instances of this class (or of one of its subclasses) are thrown by the Java Card Virtual Machine or can be thrown by the Java `throw` statement. Similarly, only this class or one of its subclasses can be the argument type in a `catch` clause.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`Throwable``()` Constructs a new `Throwable`.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

Throwable

```
public Throwable()
```

Constructs a new `Throwable`.

Package javacard.framework

Provides framework of classes and interfaces for the core functionality of a Java Card applet.

See:

Description

Interface Summary	
ISO7816	`ISO7816` encapsulates constants related to ISO 7816-3 and ISO 7816-4.
PIN	This interface represents a PIN.
Shareable	The Shareable interface serves to identify all shared objects.

Class Summary	
AID	This class encapsulates the Application Identifier(AID) associated with an applet.
APDU	Application Protocol Data Unit (APDU) is the communication format between the card and the off-card applications.
Applet	This abstract class defines an applet in Java Card.
JCSystem	The `JCSystem` class includes a collection of methods to control applet execution, resource management, atomic transaction management and inter-applet object sharing in Java Card.
OwnerPIN	This class represents an Owner PIN.
Util	The `Util` class contains common utility functions.

Exception Summary	
APDUException	`APDUException` represents an `APDU` related exception.
CardException	The `CardException` class defines a field `reason` and two accessor methods `getReason()` and `setReason()`.
CardRuntimeException	The `CardRuntimeException` class defines a field `reason` and two accessor methods `getReason()` and `setReason()`.
ISOException	`ISOException` class encapsulates an ISO 7816-4 response status word as its `reason` code.
PINException	`PINException` represents a `OwnerPIN` class access-related exception.
SystemException	`SystemException` represents a `JCSystem` class related exception.
TransactionException	`TransactionException` represents an exception in the transaction subsystem.
UserException	`UserException` represents a User exception.

Package javacard.framework Description

Provides framework of classes and interfaces for the core functionality of a Java Card applet.

javacard.framework
Class AID

```
java.lang.Object
  |
  +--javacard.framework.AID
```

public final class **AID**
extends Object

This class encapsulates the Application Identifier(AID) associated with an applet. An AID is defined in ISO 7816-5 to be a sequence of bytes between 5 and 16 bytes in length.

The JCRE creates instances of `AID` class to identify and manage every applet on the card. Applets need not create instances of this class. An applet may request and use the JCRE owned instances to identify itself and other applet instances.

JCRE owned instances of `AID` are permanent JCRE Entry Point Objects and can be accessed from any applet context. References to these permanent objects can be stored and re-used.

An applet instance can obtain a reference to JCRE owned instances of its own `AID` object by using the `JCSystem.getAID()` method and another applet's `AID` object via the `JCSystem.lookupAID()` method.

An applet uses `AID` instances to request to share another applet's object or to control access to its own shared object from another applet. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

See Also:
`JCSystem`, `SystemException`

Constructor Summary

`AID``(byte[] bArray, short offset, byte length)` The JCRE uses this constructor to create a new `AID` instance encapsulating the specified AID bytes.

Method Summary	
boolean	**equals**(byte[] bArray, short offset, byte length) Checks if the specified AID bytes in bArray are the same as those encapsulated in this AID object.
boolean	**equals**(Object anObject) Compares the AID bytes in this AID instance to the AID bytes in the specified object.
byte	**getBytes**(byte[] dest, short offset) Called to get the AID bytes encapsulated within AID object.
boolean	**partialEquals**(byte[] bArray, short offset, byte length) Checks if the specified partial AID byte sequence matches the first length bytes of the encapsulated AID bytes within this AID object.
boolean	**RIDEquals**(AID otherAID) Checks if the RID (National Registered Application provider identifier) portion of the encapsulated AID bytes within the otherAID object matches that of this AID object.

Constructor Detail

AID

```
public AID(byte[] bArray,
           short offset,
           byte length)
    throws SystemException
```

The JCRE uses this constructor to create a new AID instance encapsulating the specified AID bytes.

Parameters:

bArray - the byte array containing the AID bytes.
offset - the start of AID bytes in bArray.
length - the length of the AID bytes in bArray.

Throws:

SystemException - with the following reason code:

- SystemException.ILLEGAL_VALUE if the length parameter is less than 5 or greater than 16.

Method Detail

getBytes

```
public byte getBytes(byte[] dest,
                     short offset)
```

Called to get the AID bytes encapsulated within `AID` object.

Parameters:

`dest` - byte array to copy the AID bytes.

`offset` - within dest where the AID bytes begin.

Returns:

the length of the AID bytes.

---

equals

```
public boolean equals(Object anObject)
```

Compares the AID bytes in `this AID` instance to the AID bytes in the specified object. The result is `true` if and only if the argument is not `null` and is an `AID` object that encapsulates the same AID bytes as `this` object.

This method does not throw `NullPointerException`.

Parameters:

`anObject` - the object to compare `this AID` against.

Returns:

`true` if the AID byte values are equal, `false` otherwise.

Overrides:

equals in class Object

---

equals

```
public boolean equals(byte[] bArray,
                      short offset,
                      byte length)
```

Checks if the specified AID bytes in `bArray` are the same as those encapsulated in `this AID` object. The result is `true` if and only if the `bArray` argument is not `null` and the AID bytes encapsulated in `this AID` object are equal to the specified AID bytes in `bArray`.

This method does not throw `NullPointerException`.

Parameters:

`bArray` - containing the AID bytes

`offset` - within bArray to begin

`length` - of AID bytes in bArray

Returns:

`true` if equal, `false` otherwise.

partialEquals

```
public boolean partialEquals(byte[] bArray,
                             short offset,
                             byte length)
```

Checks if the specified partial AID byte sequence matches the first `length` bytes of the encapsulated AID bytes within `this AID` object. The result is `true` if and only if the `bArray` argument is not `null` and the input `length` is less than or equal to the length of the encapsulated AID bytes within `this AID` object and the specified bytes match.

This method does not throw `NullPointerException`.

Parameters:

`bArray` - containing the partial AID byte sequence
`offset` - within bArray to begin
`length` - of partial AID bytes in bArray

Returns:

`true` if equal, `false` otherwise.

RIDEquals

```
public boolean RIDEquals(AID otherAID)
```

Checks if the RID (National Registered Application provider identifier) portion of the encapsulated AID bytes within the `otherAID` object matches that of `this AID` object. The first 5 bytes of an AID byte sequence is the RID. See ISO 7816-5 for details. The result is `true` if and only if the argument is not `null` and is an `AID` object that encapsulates the same RID bytes as `this` object.

This method does not throw `NullPointerException`.

Parameters:

`otherAID` - the `AID` to compare against.

Returns:

`true` if the RID bytes match, `false` otherwise.

javacard.framework
Class APDU

```
java.lang.Object
  |
  +--javacard.framework.APDU
```

public final class **APDU**
extends Object

Application Protocol Data Unit (APDU) is the communication format between the card and the off-card applications. The format of the APDU is defined in ISO specification 7816-4.

This class only supports messages which conform to the structure of command and response defined in ISO 7816-4. The behavior of messages which use proprietary structure of messages (for example with header CLA byte in range 0xD0-0xFE) is undefined. This class does not support extended length fields.

The APDU object is owned by the JCRE. The APDU class maintains a byte array buffer which is used to transfer incoming APDU header and data bytes as well as outgoing data. The buffer length must be at least 37 bytes (5 bytes of header and 32 bytes of data). The JCRE must zero out the APDU buffer before each new message received from the CAD.

The JCRE designates the APDU object as a temporary JCRE Entry Point Object (See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details). A temporary JCRE Entry Point Object can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components.

The JCRE similarly marks the APDU buffer as a global array (See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details). A global array can be accessed from any applet context. References to global arrays cannot be stored in class variables or instance variables or array components.

The applet receives the APDU instance to process from the JCRE in the `Applet.process(APDU)` method, and the first five bytes [CLA, INS, P1, P2, P3] are available in the APDU buffer.

The APDU class API is designed to be transport protocol independent. In other words, applets can use the same APDU methods regardless of whether the underlying protocol in use is T=0 or T=1 (as defined in ISO 7816-3).

The incoming APDU data size may be bigger than the APDU buffer size and may therefore need to be read in portions by the applet. Similarly, the outgoing response APDU data size may be bigger than the APDU buffer size and may need to be written in portions by the applet. The APDU class has methods to facilitate this.

For sending large byte arrays as response data, the APDU class provides a special method `sendBytesLong()` which manages the APDU buffer.

```
 // The purpose of this example is to show most of the methods
 // in use and not to depict any particular APDU processing

public void process(APDU apdu){
  // ...
  byte[] buffer = apdu.getBuffer();
  byte cla = buffer[ISO7816.OFFSET_CLA];
  byte ins = buffer[ISO7816.OFFSET_INS];
  ...
  // assume this command has incoming data
  // Lc tells us the incoming apdu command length
  short bytesLeft = (short) (buffer[ISO7816.OFFSET_LC] & 0x00FF);
  if (bytesLeft < (short)55) ISOException.throwIt( ISO7816.SW_WRONG_LENGTH );

  short readCount = apdu.setIncomingAndReceive();
  while ( bytesLeft > 0){
      // process bytes in buffer[5] to buffer[readCount+4];
      bytesLeft -= readCount;
      readCount = apdu.receiveBytes ( ISO7816.OFFSET_CDATA );
      }
  //
  //...
  //
  // Note that for a short response as in the case illustrated here
  // the three APDU method calls shown : setOutgoing(),setOutgoingLength() & sendBytes()
  // could be replaced by one APDU method call : setOutgoingAndSend().

  // construct the reply APDU
  short le = apdu.setOutgoing();
  if (le < (short)2) ISOException.throwIt( ISO7816.SW_WRONG_LENGTH );
  apdu.setOutgoingLength( (short)3 );

  // build response data in apdu.buffer[ 0.. outCount-1 ];
  buffer[0] = (byte)1; buffer[1] = (byte)2; buffer[3] = (byte)3;
  apdu.sendBytes ( (short)0 , (short)3 );
  // return good complete status 90 00
  }
```

See Also:

`APDUException`, `ISOException`

Field Summary

static byte	**`PROTOCOL_T0`** ISO 7816 transport protocol type T=0
static byte	**`PROTOCOL_T1`** ISO 7816 transport protocol type T=1

Method Summary

byte[]	**getBuffer**() Returns the APDU buffer byte array.
static short	**getInBlockSize**() Returns the configured incoming block size. In T=1 protocol, this corresponds to IFSC (information field size for ICC), the maximum size of incoming data blocks into the card. In T=0 protocol, this method returns 1.
byte	**getNAD**() In T=1 protocol, this method returns the Node Address byte, NAD. In T=0 protocol, this method returns 0.
static short	**getOutBlockSize**() Returns the configured outgoing block size. In T=1 protocol, this corresponds to IFSD (information field size for interface device), the maximum size of outgoing data blocks to the CAD. In T=0 protocol, this method returns 258 (accounts for 2 status bytes).
static byte	**getProtocol**() Returns the ISO 7816 transport protocol type, T=1 or T=0 in progress.
short	**receiveBytes**(short bOff) Gets as many data bytes as will fit without APDU buffer overflow, at the specified offset `bOff`. Gets all the remaining bytes if they fit.
void	**sendBytes**(short bOff, short len) Sends `len` more bytes from APDU buffer at specified offset `bOff`.
void	**sendBytesLong**(byte[] outData, short bOff, short len) Sends `len` more bytes from `outData` byte array starting at specified offset `bOff`.
short	**setIncomingAndReceive**() This is the primary receive method.
short	**setOutgoing**() This method is used to set the data transfer direction to outbound and to obtain the expected length of response (Le).
void	**setOutgoingAndSend**(short bOff, short len) This is the "convenience" send method.
void	**setOutgoingLength**(short len) Sets the actual length of response data.
short	**setOutgoingNoChaining**() This method is used to set the data transfer direction to outbound without using BLOCK CHAINING(See ISO 7816-3/4) and to obtain the expected length of response (Le).
void	**waitExtension**() Requests additional processsing time from CAD.

Methods inherited from class java.lang.Object
equals

Field Detail

PROTOCOL_T0

```
public static final byte PROTOCOL_T0
```

ISO 7816 transport protocol type T=0

PROTOCOL_T1

```
public static final byte PROTOCOL_T1
```

ISO 7816 transport protocol type T=1

Method Detail

getBuffer

```
public byte[] getBuffer()
```

Returns the APDU buffer byte array.

Notes:

- *References to the APDU buffer byte array cannot be stored in class variables or instance variables or array components. See* Java Card Runtime Environment (JCRE) 2.1 Specification *for details.*

Returns:

byte array containing the APDU buffer

---

getInBlockSize

```
public static short getInBlockSize()
```

Returns the configured incoming block size. In T=1 protocol, this corresponds to IFSC (information field size for ICC), the maximum size of incoming data blocks into the card. In T=0 protocol, this method returns 1. IFSC is defined in ISO 7816-3.

This information may be used to ensure that there is enough space remaining in the APDU buffer when `receiveBytes()` is invoked.

Notes:

- *On* `receiveBytes()` *the* `bOff` *param should account for this potential blocksize.*

Returns:

incoming block size setting.

See Also:

`receiveBytes(short)`

---

getOutBlockSize

```
public static short getOutBlockSize()
```

Returns the configured outgoing block size. In T=1 protocol, this corresponds to IFSD (information field size for interface device), the maximum size of outgoing data blocks to the CAD. In T=0 protocol, this method returns 258 (accounts for 2 status bytes). IFSD is defined in ISO 7816-3.

This information may be used prior to invoking the `setOutgoingLength()` method, to limit the length of outgoing messages when BLOCK CHAINING is not allowed.

Notes:

- *On* `setOutgoingLength()` *the* `len` *param should account for this potential blocksize.*

Returns:

outgoing block size setting.

See Also:

`setOutgoingLength(short)`

---

getProtocol

```
public static byte getProtocol()
```

Returns the ISO 7816 transport protocol type, T=1 or T=0 in progress.

Returns:

the protocol type in progress. One of `PROTOCOL_T0`, `PROTOCOL_T1` listed above.

---

getNAD

```
public byte getNAD()
```

In T=1 protocol, this method returns the Node Address byte, NAD. In T=0 protocol, this method returns 0. This may be used as additional information to maintain multiple contexts.

Returns:

NAD transport byte as defined in ISO 7816-3.

setOutgoing

```
public short setOutgoing()
                  throws APDUException
```

This method is used to set the data transfer direction to outbound and to obtain the expected length of response (Le).

Notes.

- *Any remaining incoming data will be discarded.*
- *In T=0 (Case 4) protocol, this method will return 256.*

Returns:

Le, the expected length of response.

Throws:

APDUException - with the following reason codes:

- `APDUException.ILLEGAL_USE` if this method or `setOutgoingNoChaining()` method already invoked.
- `APDUException.IO_ERROR` on I/O error.

setOutgoingNoChaining

```
public short setOutgoingNoChaining()
                           throws APDUException
```

This method is used to set the data transfer direction to outbound without using BLOCK CHAINING(See ISO 7816-3/4) and to obtain the expected length of response (Le). This method should be used in place of the `setOutgoing()` method by applets which need to be compatible with legacy CAD/terminals which do not support ISO 7816-3/4 defined block chaining. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Notes.

- *Any remaining incoming data will be discarded.*
- *In T=0 (Case 4) protocol, this method will return 256.*
- *When this method is used, the* `waitExtension()` *method cannot be used.*
- *In T=1 protocol, retransmission on error may be restricted.*
- *In T=0 protocol, the outbound transfer must be performed without using response status chaining.*
- *In T=1 protocol, the outbound transfer must not set the More(M) Bit in the PCB of the I block. See ISO 7816-3.*

Returns:

Le, the expected length of response data.

Throws:

APDUException - with the following reason codes:

- `APDUException.ILLEGAL_USE` if this method or `setOutgoing()` method already invoked.

- `APDUException.IO_ERROR` on I/O error.

---

setOutgoingLength

```
public void setOutgoingLength(short len)
                      throws APDUException
```

Sets the actual length of response data. Default is 0.

Note:

- *In T=0 (Case 2&4) protocol, the length is used by the JCRE to prompt the CAD for GET RESPONSE commands.*

Parameters:

`len` - the length of response data.

Throws:

APDUException - with the following reason codes:

- `APDUException.ILLEGAL_USE` if `setOutgoing()` not called or this method already invoked.
- `APDUException.BAD_LENGTH` if `len` is greater than 256 or if non BLOCK CHAINED data transfer is requested and `len` is greater than (IFSD-2), where IFSD is the Outgoing Block Size. The -2 accounts for the status bytes in T=1.
- `APDUException.IO_ERROR` on I/O error.

See Also:

`getOutBlockSize()`

---

receiveBytes

```
public short receiveBytes(short bOff)
                  throws APDUException
```

Gets as many data bytes as will fit without APDU buffer overflow, at the specified offset `bOff`. Gets all the remaining bytes if they fit.

Notes:

- *The space in the buffer must allow for incoming block size.*
- *In T=1 protocol, if all the remaining bytes do not fit in the buffer, this method may return less bytes than the maximum incoming block size (IFSC).*
- *In T=0 protocol, if all the remaining bytes do not fit in the buffer, this method may return less than a full buffer of bytes to optimize and reduce protocol overhead.*
- *In T=1 protocol, if this method throws an* `APDUException` *with* `T1_IFD_ABORT` *reason code, the JCRE will restart APDU command processing using the newly received command. No more input data can be received. No output data can be transmitted. No error status response can be returned.*

Parameters:

`bOff` - the offset into APDU buffer.

Returns:
number of bytes read. Returns 0 if no bytes are available.
Throws:
APDUException - with the following reason codes:
- `APDUException.ILLEGAL_USE` if `setIncomingAndReceive()` not called or if `setOutgoing()` or `setOutgoingNoChaining()` previously invoked.
- `APDUException.BUFFER_BOUNDS` if not enough buffer space for incoming block size.
- `APDUException.IO_ERROR` on I/O error.
- `APDUException.T1_IFD_ABORT` if T=1 protocol is in use and the CAD sends in an ABORT S-Block command to abort the data transfer.

See Also:
`getInBlockSize()`

---

setIncomingAndReceive

```
public short setIncomingAndReceive()
                          throws APDUException
```

This is the primary receive method. Calling this method indicates that this APDU has incoming data. This method gets as many bytes as will fit without buffer overflow in the APDU buffer following the header. It gets all the incoming bytes if they fit.

Notes:
- *In T=0 (Case 3&4) protocol, the P3 param is assumed to be Lc.*
- *Data is read into the buffer at offset 5.*
- *In T=1 protocol, if all the incoming bytes do not fit in the buffer, this method may return less bytes than the maximum incoming block size (IFSC).*
- *In T=0 protocol, if all the incoming bytes do not fit in the buffer, this method may return less than a full buffer of bytes to optimize and reduce protocol overhead.*
- *This method sets the transfer direction to be inbound and calls* `receiveBytes(5)`.
- *This method may only be called once in a* `Applet.process()` *method.*

Returns:
number of bytes read. Returns 0 if no bytes are available.
Throws:
APDUException - with the following reason codes:
- `APDUException.ILLEGAL_USE` if `setIncomingAndReceive()` already invoked or if `setOutgoing()` or `setOutgoingNoChaining()` previously invoked.
- `APDUException.IO_ERROR` on I/O error.
- `APDUException.T1_IFD_ABORT` if T=1 protocol is in use and the CAD sends in an ABORT S-Block command to abort the data transfer.

---

sendBytes

```
public void sendBytes(short bOff,
                      short len)
               throws APDUException
```

Sends `len` more bytes from APDU buffer at specified offset `bOff`.

If the last part of the response is being sent by the invocation of this method, the APDU buffer must not be altered. If the data is altered, incorrect output may be sent to the CAD. Requiring that the buffer not be altered allows the implementation to reduce protocol overhead by transmitting the last part of the response along with the status bytes.

Notes:

- *If* `setOutgoingNoChaining()` *was invoked, output block chaining must not be used.*
- *In T=0 protocol, if* `setOutgoingNoChaining()` *was invoked, Le bytes must be transmitted before response status is returned.*
- *In T=0 protocol, if this method throws an* `APDUException` *with* `NO_T0_GETRESPONSE` *reason code, the JCRE will restart APDU command processing using the newly received command. No more output data can be transmitted. No error status response can be returned.*
- *In T=1 protocol, if this method throws an* `APDUException` *with* `T1_IFD_ABORT` *reason code, the JCRE will restart APDU command processing using the newly received command. No more output data can be transmitted. No error status response can be returned.*

Parameters:

`bOff` - the offset into APDU buffer.
`len` - the length of the data in bytes to send.

Throws:

APDUException - with the following reason codes:

- `APDUException.ILLEGAL_USE` if `setOutgoingLen()` not called or `setOutgoingAndSend()` previously invoked or response byte count exeeded or if `APDUException.NO_T0_GETRESPONSE` previously thrown.
- `APDUException.BUFFER_BOUNDS` if the sum of `bOff` and `len` exceeds the buffer size.
- `APDUException.IO_ERROR` on I/O error.
- `APDUException.NO_T0_GETRESPONSE` if T=0 protocol is in use and the CAD does not respond to response status with GET RESPONSE command.
- `APDUException.T1_IFD_ABORT` if T=1 protocol is in use and the CAD sends in an ABORT S-Block command to abort the data transfer.

See Also:

`setOutgoing()`, `setOutgoingNoChaining()`

---

sendBytesLong

```
public void sendBytesLong(byte[] outData,
                          short bOff,
                          short len)
                   throws APDUException
```

Sends `len` more bytes from `outData` byte array starting at specified offset `bOff`.

If the last of the response is being sent by the invocation of this method, the APDU buffer must not be altered. If the data is altered, incorrect output may be sent to the CAD. Requiring that the buffer not be altered allows the implementation to reduce protocol overhead by transmitting the last part of the response along with the status bytes.

The JCRE may use the APDU buffer to send data to the CAD.

Notes:

- *If* `setOutgoingNoChaining()` *was invoked, output block chaining must not be used.*
- *In T=0 protocol, if* `setOutgoingNoChaining()` *was invoked, Le bytes must be transmitted before response status is returned.*
- *In T=0 protocol, if this method throws an* `APDUException` *with NO_T0_GETRESPONSE reason code, the JCRE will restart APDU command processing using the newly received command. No more output data can be transmitted. No error status response can be returned.*
- *In T=1 protocol, if this method throws an* `APDUException` *with* `T1_IFD_ABORT` *reason code, the JCRE will restart APDU command processing using the newly received command. No more output data can be transmitted. No error status response can be returned.*

Parameters:

`outData` - the source data byte array.
`bOff` - the offset into OutData array.
`len` - the bytelength of the data to send.

Throws:

APDUException - with the following reason codes:

- `APDUException.ILLEGAL_USE` if `setOutgoingLen()` not called or `setOutgoingAndSend()` previously invoked or response byte count exeeded or if `APDUException.NO_T0_GETRESPONSE` previously thrown.
- `APDUException.IO_ERROR` on I/O error.
- `APDUException.NO_T0_GETRESPONSE` if T=0 protocol is in use and CAD does not respond to response status with GET RESPONSE command.
- `APDUException.T1_IFD_ABORT` if T=1 protocol is in use and the CAD sends in an ABORT S-Block command to abort the data transfer.

See Also:

`setOutgoing()`, `setOutgoingNoChaining()`

---

setOutgoingAndSend

```
public void setOutgoingAndSend(short bOff,
                               short len)
                        throws APDUException
```

This is the "convenience" send method. It provides for the most efficient way to send a short response which fits in the buffer and needs the least protocol overhead. This method is a combination of `setOutgoing(), setOutgoingLength( len )` followed by `sendBytes ( bOff, len )`. In addition, once this method is invoked, `sendBytes()` and `sendBytesLong()` methods cannot be invoked and the APDU buffer must not be altered.

Sends `len` byte response from the APDU buffer at starting specified offset `bOff`.

Notes:

- *No other* `APDU` *send methods can be invoked.*
- *The APDU buffer must not be altered. If the data is altered, incorrect output may be sent to the CAD.*
- *The actual data transmission may only take place on return from* `Applet.process()`

Parameters:

`bOff` - the offset into APDU buffer.
`len` - the bytelength of the data to send.

Throws:

APDUException - with the following reason codes:

- `APDUException.ILLEGAL_USE` if `setOutgoing()` or `setOutgoingAndSend()` previously invoked or response byte count exeeded.
- `APDUException.IO_ERROR` on I/O error.

---

waitExtension

```
public void waitExtension()
                  throws APDUException
```

Requests additional processsing time from CAD. The implementation should ensure that this method needs to be invoked only under unusual conditions requiring excessive processing times.

Notes:

- *In T=0 protocol, a NULL procedure byte is sent to reset the work waiting time (see ISO 7816-3).*
- *In T=1 protocol, the implementation needs to request the same T=0 protocol work waiting time quantum by sending a T=1 protocol request for wait time extension(see ISO 7816-3).*
- *If the implementation uses an automatic timer mechanism instead, this method may do nothing.*

Throws:

APDUException - with the following reason codes:

- `APDUException.ILLEGAL_USE` if `setOutgoingNoChaining()` previously

invoked.

- `APDUException.IO_ERROR` on I/O error.

---

javacard.framework
Class APDUException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--javacard.framework.CardRuntimeException
                          |
                          +--javacard.framework.APDUException
```

public class **APDUException**
extends CardRuntimeException

`APDUException` represents an `APDU` related exception.

The `APDU` class throws JCRE owned instances of `APDUException`.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

See Also:
`APDU`

Field Summary

static short	**BAD_LENGTH** This reason code is used by the APDU.setOutgoingLength() method to indicate that the length parameter is greater that 256 or if non BLOCK CHAINED data transfer is requested and len is greater than (IFSD-2), where IFSD is the Outgoing Block Size.
static short	**BUFFER_BOUNDS** This reason code is used by the APDU.sendBytes() method to indicate that the sum of buffer offset parameter and the byte length parameter exceeds the APDU buffer size.
static short	**ILLEGAL_USE** This APDUException reason code indicates that the method should not be invoked based on the current state of the APDU.
static short	**IO_ERROR** This reason code indicates that an unrecoverable error occurred in the I/O transmission layer.
static short	**NO_T0_GETRESPONSE** This reason code indicates that during T=0 protocol, the CAD did not return a GET RESPONSE command in response to a <61xx> response status to send additional data.
static short	**T1_IFD_ABORT** This reason code indicates that during T=1 protocol, the CAD returned an ABORT S-Block command and aborted the data transfer.

Constructor Summary

APDUException(short reason) Constructs an APDUException.	

Method Summary

static void	**throwIt**(short reason) Throws the JCRE owned instance of APDUException with the specified reason.

Methods inherited from class javacard.framework.CardRuntimeException
`getReason, setReason`

Methods inherited from class java.lang.Object
`equals`

Field Detail

ILLEGAL_USE

```
public static final short ILLEGAL_USE
```

This APDUException reason code indicates that the method should not be invoked based on the current state of the APDU.

BUFFER_BOUNDS

```
public static final short BUFFER_BOUNDS
```

This reason code is used by the `APDU.sendBytes()` method to indicate that the sum of buffer offset parameter and the byte length parameter exceeds the APDU buffer size.

BAD_LENGTH

```
public static final short BAD_LENGTH
```

This reason code is used by the `APDU.setOutgoingLength()` method to indicate that the length parameter is greater that 256 or if non BLOCK CHAINED data transfer is requested and `len` is greater than (IFSD-2), where IFSD is the Outgoing Block Size.

IO_ERROR

```
public static final short IO_ERROR
```

This reason code indicates that an unrecoverable error occurred in the I/O transmission layer.

NO_T0_GETRESPONSE

```
public static final short NO_T0_GETRESPONSE
```

This reason code indicates that during T=0 protocol, the CAD did not return a GET RESPONSE command in response to a <61xx> response status to send additional data. The outgoing transfer has been aborted. No more data or status can be sent to the CAD in this `APDU.process()` method.

T1_IFD_ABORT

```
public static final short T1_IFD_ABORT
```

This reason code indicates that during T=1 protocol, the CAD returned an ABORT S-Block command and aborted the data transfer. The incoming or outgoing transfer has been aborted. No more data can be received from the CAD. No more data or status can be sent to the CAD in this `APDU.process()` method.

Constructor Detail

APDUException

```
public APDUException(short reason)
```

Constructs an APDUException. To conserve on resources use `throwIt()` to use the JCRE owned instance of this class.

Parameters:

`reason` - the reason for the exception.

Method Detail

throwIt

```
public static void throwIt(short reason)
```

Throws the JCRE owned instance of `APDUException` with the specified reason.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Parameters:

`reason` - the reason for the exception.

Throws:

APDUException - always.

javacard.framework
Class Applet

```
java.lang.Object
  |
  +--javacard.framework.Applet
```

public abstract class **Applet**
extends Object

This abstract class defines an applet in Java Card.

The `Applet` class should be extended by any applet that is intended to be loaded onto, installed into and executed on a Java Card compliant smart card.

Example usage of `Applet`

```
public class MyApplet extends javacard.framework.Applet{
static byte someByteArray[];

public static void install( byte[] bArray, short bOffset, byte bLength  ) throws ISOException {
  // make all my allocations here, so I do not run
  // out of memory later
  MyApplet theApplet = new MyApplet();

  // check incoming parameter
  byte bLen = bArray[bOffset];
  if ( bLen!=0 ) { someByteArray = new byte[bLen]; theApplet.register(); return; }
  else ISOException.throwIt(ISO7816.SW_FUNC_NOT_SUPPORTED);
  }

public boolean select(){
  // selection initialization
  someByteArray[17] = 42; // set selection state
  return true;
  }

public void process(APDU apdu) throws ISOException{
 byte[] buffer = apdu.getBuffer();
 // .. process the incoming data and reply
 if ( buffer[ISO7816.OFFSET_CLA] == (byte)0 ) {
    switch ( buffer[ISO7816.OFFSET_INS] ) {
        case ISO.INS_SELECT:
            ...
            // send response data to select command
            short Le =  apdu.setOutgoing();
            // assume data containing response bytes in replyData[] array.
            if ( Le < ..) ISOException.throwIt( ISO7816.SW_WRONG_LENGTH);
            apdu.setOutgoingLength( (short)replyData.length );
            apdu.sendBytesLong(replyData, (short) 0, (short)replyData.length);
            break;
        case ...
        }
     }
```

```
  }
}
```

See Also:
`SystemException`, `JCSystem`

Constructor Summary

`protected`	**`Applet`**`()` Only this class's `install()` method should create the applet object.

Method Summary

`void`	**`deselect`**`()` Called by the JCRE to inform this currently selected applet that another (or the same) applet will be selected.
`Shareable`	**`getShareableInterfaceObject`**`(AID clientAID, byte parameter)` Called by the JCRE to obtain a shareable interface object from this server applet, on behalf of a request from a client applet.
`static void`	**`install`**`(byte[] bArray, short bOffset, byte bLength)` To create an instance of the `Applet` subclass, the JCRE will call this static method first.
`abstract void`	**`process`**`(APDU apdu)` Called by the JCRE to process an incoming APDU command.
`protected void`	**`register`**`()` This method is used by the applet to register `this` applet instance with the JCRE and to assign the `Applet` subclass AID bytes as its instance AID bytes.
`protected void`	**`register`**`(byte[] bArray, short bOffset, byte bLength)` This method is used by the applet to register `this` applet instance with the JCRE and assign the specified AID bytes as its instance AID bytes.
`boolean`	**`select`**`()` Called by the JCRE to inform this applet that it has been selected.
`protected boolean`	**`selectingApplet`**`()` This method is used by the applet `process()` method to distinguish the SELECT APDU command which selected `this` applet, from all other other SELECT APDU commands which may relate to file or internal applet state selection.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

Applet

```
protected Applet()
```

Only this class's `install()` method should create the applet object.

Method Detail

install

```
public static void install(byte[] bArray,
                           short bOffset,
                           byte bLength)
                    throws ISOException
```

To create an instance of the `Applet` subclass, the JCRE will call this static method first.

The applet should perform any necessary initializations and must call one of the `register()` methods. The installation is considered successful when the call to `register()` completes without an exception. The installation is deemed unsuccessful if the `install` method does not call a `register()` method, or if an exception is thrown from within the `install` method prior to the call to a `register()` method, or if the `register()` method throws an exception. If the installation is unsuccessful, the JCRE must perform all the necessary clean up when it receives control. Successful installation makes the applet instance capable of being selected via a SELECT APDU command.

Installation parameters are supplied in the byte array parameter and must be in a format defined by the applet. The `bArray` object is a global array. If the applet desires to preserve any of this data, it should copy the data into its own object.

`bArray` is zeroed by the JCRE after the return from the `install()` method.

References to the `bArray` object cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

The implementation of this method provided by `Applet` class throws an `ISOException` with reason code = `ISO7816.SW_FUNC_NOT_SUPPORTED`.

Note:

- *Exceptions thrown by this method after successful installation are caught by the JCRE and processed by the Installer.*

Parameters:

`bArray` - the array containing installation parameters.
`bOffset` - the starting offset in bArray.
`bLength` - the length in bytes of the parameter data in bArray. The maximum value of bLength is 32.

---

process

```
public abstract void process(APDU apdu)
                     throws ISOException
```

Called by the JCRE to process an incoming APDU command. An applet is expected to perform the action requested and return response data if any to the terminal.

Upon normal return from this method the JCRE sends the ISO 7816-4 defined success status (90 00) in APDU response. If this method throws an `ISOException` the JCRE sends the associated reason code as the response status instead.

The JCRE zeroes out the APDU buffer before receiving a new APDU command from the CAD. The five header bytes of the APDU command are available in APDU buffer[0..4] at the time this method is called.

The `APDU` object parameter is a temporary JCRE Entry Point Object. A temporary JCRE Entry Point Object can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components.

Notes:

- *APDU buffer[5..] is undefined and should not be read or written prior to invoking the* `APDU.setIncomingAndReceive()` *method if incoming data is expected. Altering the APDU buffer[5..] could corrupt incoming data.*

Parameters:

`apdu` - the incoming `APDU` object

Throws:

ISOException - with the response bytes per ISO 7816-4

See Also:

`APDU`

---

select

```
public boolean select()
```

Called by the JCRE to inform this applet that it has been selected.

It is called when a SELECT APDU command is received and before the applet is selected. SELECT APDU commands use instance AID bytes for applet selection. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

A subclass of `Applet` should override this method if it should perform any initialization that may be required to process APDU commands that may follow. This method returns a boolean to indicate that it is ready to accept incoming APDU commands via its `process()` method. If this method returns false, it indicates to the JCRE that this Applet declines to be selected.

The implementation of this method provided by `Applet` class returns `true`.

Returns:

`true` to indicate success, `false` otherwise.

---

deselect

```
public void deselect()
```

Called by the JCRE to inform this currently selected applet that another (or the same) applet will be selected. It is called when a SELECT APDU command is received by the JCRE. This method is invoked prior to another applets or this very applets `select()` method being invoked.

A subclass of `Applet` should override this method if it has any cleanup or bookkeeping work to be performed before another applet is selected.

The default implementation of this method provided by `Applet` class does nothing.

Notes:

- *Unchecked exceptions thrown by this method are caught by the JCRE but the applet is deselected.*
- *Transient objects of* `JCSystem.CLEAR_ON_DESELECT` *clear event type are cleared to their default value by the JCRE after this method.*
- *This method is NOT called on reset or power loss.*

---

getShareableInterfaceObject

```
public Shareable getShareableInterfaceObject(AID clientAID,
                                             byte parameter)
```

Called by the JCRE to obtain a shareable interface object from this server applet, on behalf of a request from a client applet. This method executes in the applet context of `this` applet instance. The client applet initiated this request by calling the `JCSystem.getAppletShareableInterfaceObject()` method. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Parameters:

`clientAID` - the `AID` object of the client applet.

`parameter` - optional parameter byte. The parameter byte may be used by the client to specify which shareable interface object is being requested.

Returns:

the shareable interface object or `null`. Note:

- *The* `clientAID` *parameter is a JCRE owned* `AID` *instance. JCRE owned instances of* `AID` *are permanent JCRE Entry Point Objects and can be accessed from any applet context. References to these permanent objects can be stored and re-used.*

See Also:

`JCSystem.getAppletShareableInterfaceObject(AID, byte)`

---

register

```
protected final void register()
                      throws SystemException
```

This method is used by the applet to register `this` applet instance with the JCRE and to assign the `Applet` subclass AID bytes as its instance AID bytes. One of the `register()` methods must be called from within `install()` to be registered with the JCRE. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Throws:

SystemException - with the following reason codes:

- `SystemException.ILLEGAL_AID` if the `Applet` subclass AID bytes are in use or if the applet instance has previously called one of the `register()` methods.

---

register

```
protected final void register(byte[] bArray,
                              short bOffset,
                              byte bLength)
                      throws SystemException
```

This method is used by the applet to register `this` applet instance with the JCRE and assign the specified AID bytes as its instance AID bytes. One of the `register()` methods must be called from within `install()` to be registered with the JCRE. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Parameters:

`bArray` - the byte array containing the AID bytes.

`bOffset` - the start of AID bytes in bArray.

`bLength` - the length of the AID bytes in bArray.

Throws:

APDUException - with the following reason codes:

SystemException - with the following reason code:

- `SystemException.ILLEGAL_VALUE` if the `bLength` parameter is less than `5` or greater than `16`.
- `SystemException.ILLEGAL_AID` if the specified instance AID bytes are in use or if the RID portion of the AID bytes in the `bArray` parameter does not match the RID portion of the `Applet` subclass AID bytes or if the applet instance has previously called one of the `register()` methods.

---

selectingApplet

```
protected final boolean selectingApplet()
```

This method is used by the applet `process()` method to distinguish the SELECT APDU command which selected `this` applet, from all other other SELECT APDU commands which may relate to file or internal applet state selection.

Returns:

`true` if `this` applet is being selected.

---

javacard.framework
Class CardException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--javacard.framework.CardException
```

Direct Known Subclasses:
UserException

public class **CardException**
extends Exception

The `CardException` class defines a field `reason` and two accessor methods `getReason()` and `setReason()`. The `reason` field encapsulates exception cause identifier in Java Card. All Java Card checked Exception classes should extend `CardException`. This class also provides a resource-saving mechanism (`throwIt()` method) for using a JCRE owned instance of this class.

Constructor Summary

`CardException``(short reason)` Construct a CardException instance with the specified reason.

Method Summary

`short`	**`getReason`**`()` Get reason code
`void`	**`setReason`**`(short reason)` Set reason code
`static void`	**`throwIt`**`(short reason)` Throw the JCRE owned instance of `CardException` class with the specified reason.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

CardException

```
public CardException(short reason)
```

Construct a CardException instance with the specified reason. To conserve on resources, use the `throwIt()` method to use the JCRE owned instance of this class.

Parameters:

`reason` - the reason for the exception

Method Detail

getReason

```
public short getReason()
```

Get reason code

Returns:

the reason for the exception

---

setReason

```
public void setReason(short reason)
```

Set reason code

Parameters:

`reason` - the reason for the exception

---

throwIt

```
public static void throwIt(short reason)
                    throws CardException
```

Throw the JCRE owned instance of `CardException` class with the specified reason.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1*

Specification for details.

Parameters:

`reason` - the reason for the exception

Throws:

CardException - always.

---

javacard.framework
Class CardRuntimeException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--javacard.framework.CardRuntimeException
```

Direct Known Subclasses:
APDUException, CryptoException, ISOException, PINException, SystemException, TransactionException

---

public class **CardRuntimeException**
extends RuntimeException

The `CardRuntimeException` class defines a field `reason` and two accessor methods `getReason()` and `setReason()`. The `reason` field encapulates exception cause identifier in Java Card. All Java Card unchecked Exception classes should extend `CardRuntimeException`. This class also provides a resource-saving mechanism (`throwIt()` method) for using a JCRE owned instance of this class.

Constructor Summary

`CardRuntimeException``(short reason)` Construct a CardRuntimeException instance with the specified reason.

Method Summary

`short`	**`getReason`**`()` Get reason code
`void`	**`setReason`**`(short reason)` Set reason code
`static void`	**`throwIt`**`(short reason)` Throw the JCRE owned instance of the `CardRuntimeException` class with the specified reason.

Methods inherited from class java.lang.Object
equals

Constructor Detail

CardRuntimeException

```
public CardRuntimeException(short reason)
```

Construct a CardRuntimeException instance with the specified reason. To conserve on resources, use `throwIt()` method to use the JCRE owned instance of this class.

Parameters:

`reason` - the reason for the exception

Method Detail

getReason

```
public short getReason()
```

Get reason code

Returns:

the reason for the exception

---

setReason

```
public void setReason(short reason)
```

Set reason code

Parameters:

`reason` - the reason for the exception

---

throwIt

```
public static void throwIt(short reason)
                    throws CardRuntimeException
```

Throw the JCRE owned instance of the `CardRuntimeException` class with the specified reason.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Parameters:

`reason` - the reason for the exception

Throws:

CardRuntimeException - always.

---

javacard.framework
Interface ISO7816

public abstract interface **ISO7816**

`ISO7816` encapsulates constants related to ISO 7816-3 and ISO 7816-4. `ISO7816` interface contains only static fields.

The static fields with `SW_` prefixes define constants for the ISO 7816-4 defined response status word. The fields which use the `_00` suffix require the low order byte to be customized appropriately e.g (ISO7816.SW_CORRECT_LENGTH_00 + (0x0025 & 0xFF)).

The static fields with `OFFSET_` prefixes define constants to be used to index into the APDU buffer byte array to access ISO 7816-4 defined header information.

Field Summary

static byte	**CLA_ISO7816** APDU command CLA : ISO 7816 = 0x00
static byte	**INS_EXTERNAL_AUTHENTICATE** APDU command INS : EXTERNAL AUTHENTICATE = 0x82
static byte	**INS_SELECT** APDU command INS : SELECT = 0xA4
static byte	**OFFSET_CDATA** APDU command data offset : CDATA = 5
static byte	**OFFSET_CLA** APDU header offset : CLA = 0
static byte	**OFFSET_INS** APDU header offset : INS = 1
static byte	**OFFSET_LC** APDU header offset : LC = 4
static byte	**OFFSET_P1** APDU header offset : P1 = 2
static byte	**OFFSET_P2** APDU header offset : P2 = 3
static short	**SW_APPLET_SELECT_FAILED** Response status : Applet selection failed = 0x6999;

static short	**SW_BYTES_REMAINING_00** Response status : Response bytes remaining = 0x6100
static short	**SW_CLA_NOT_SUPPORTED** Response status : CLA value not supported = 0x6E00
static short	**SW_COMMAND_NOT_ALLOWED** Response status : Command not allowed (no current EF) = 0x6986
static short	**SW_CONDITIONS_NOT_SATISFIED** Response status : Conditions of use not satisfied = 0x6985
static short	**SW_CORRECT_LENGTH_00** Response status : Correct Expected Length (Le) = 0x6C00
static short	**SW_DATA_INVALID** Response status : Data invalid = 0x6984
static short	**SW_FILE_FULL** Response status : Not enough memory space in the file = 0x6A84
static short	**SW_FILE_INVALID** Response status : File invalid = 0x6983
static short	**SW_FILE_NOT_FOUND** Response status : File not found = 0x6A82
static short	**SW_FUNC_NOT_SUPPORTED** Response status : Function not supported = 0x6A81
static short	**SW_INCORRECT_P1P2** Response status : Incorrect parameters (P1,P2) = 0x6A86
static short	**SW_INS_NOT_SUPPORTED** Response status : INS value not supported = 0x6D00
static short	**SW_NO_ERROR** Response status : No Error = (short)0x9000
static short	**SW_RECORD_NOT_FOUND** Response status : Record not found = 0x6A83
static short	**SW_SECURITY_STATUS_NOT_SATISFIED** Response status : Security condition not satisfied = 0x6982
static short	**SW_UNKNOWN** Response status : No precise diagnosis = 0x6F00
static short	**SW_WRONG_DATA** Response status : Wrong data = 0x6A80
static short	**SW_WRONG_LENGTH** Response status : Wrong length = 0x6700

static short	**SW_WRONG_P1P2** Response status : Incorrect parameters (P1,P2) = 0x6B00

Field Detail

SW_NO_ERROR

```
public static final short SW_NO_ERROR
```

Response status : No Error = (short)0x9000

SW_BYTES_REMAINING_00

```
public static final short SW_BYTES_REMAINING_00
```

Response status : Response bytes remaining = 0x6100

SW_WRONG_LENGTH

```
public static final short SW_WRONG_LENGTH
```

Response status : Wrong length = 0x6700

SW_SECURITY_STATUS_NOT_SATISFIED

```
public static final short SW_SECURITY_STATUS_NOT_SATISFIED
```

Response status : Security condition not satisfied = 0x6982

SW_FILE_INVALID

```
public static final short SW_FILE_INVALID
```

Response status : File invalid = 0x6983

SW_DATA_INVALID

```
public static final short SW_DATA_INVALID
```

Response status : Data invalid = 0x6984

SW_CONDITIONS_NOT_SATISFIED

```
public static final short SW_CONDITIONS_NOT_SATISFIED
```

Response status : Conditions of use not satisfied = 0x6985

SW_COMMAND_NOT_ALLOWED

```
public static final short SW_COMMAND_NOT_ALLOWED
```

Response status : Command not allowed (no current EF) = 0x6986

SW_APPLET_SELECT_FAILED

```
public static final short SW_APPLET_SELECT_FAILED
```

Response status : Applet selection failed = 0x6999;

SW_WRONG_DATA

```
public static final short SW_WRONG_DATA
```

Response status : Wrong data = 0x6A80

SW_FUNC_NOT_SUPPORTED

```
public static final short SW_FUNC_NOT_SUPPORTED
```

Response status : Function not supported = 0x6A81

SW_FILE_NOT_FOUND

```
public static final short SW_FILE_NOT_FOUND
```

Response status : File not found = 0x6A82

SW_RECORD_NOT_FOUND

```
public static final short SW_RECORD_NOT_FOUND
```

Response status : Record not found = 0x6A83

SW_INCORRECT_P1P2

```
public static final short SW_INCORRECT_P1P2
```

Response status : Incorrect parameters (P1,P2) = 0x6A86

SW_WRONG_P1P2

```
public static final short SW_WRONG_P1P2
```

Response status : Incorrect parameters (P1,P2) = 0x6B00

SW_CORRECT_LENGTH_00

```
public static final short SW_CORRECT_LENGTH_00
```

Response status : Correct Expected Length (Le) = 0x6C00

SW_INS_NOT_SUPPORTED

```
public static final short SW_INS_NOT_SUPPORTED
```

Response status : INS value not supported = 0x6D00

SW_CLA_NOT_SUPPORTED

```
public static final short SW_CLA_NOT_SUPPORTED
```

Response status : CLA value not supported = 0x6E00

SW_UNKNOWN

```
public static final short SW_UNKNOWN
```

Response status : No precise diagnosis = 0x6F00

SW_FILE_FULL

```
public static final short SW_FILE_FULL
```

Response status : Not enough memory space in the file = 0x6A84

OFFSET_CLA

```
public static final byte OFFSET_CLA
```

APDU header offset : CLA = 0

OFFSET_INS

```
public static final byte OFFSET_INS
```

APDU header offset : INS = 1

OFFSET_P1

```
public static final byte OFFSET_P1
```

APDU header offset : P1 = 2

OFFSET_P2

```
public static final byte OFFSET_P2
```

APDU header offset : P2 = 3

OFFSET_LC

```
public static final byte OFFSET_LC
```

APDU header offset : LC = 4

OFFSET_CDATA

```
public static final byte OFFSET_CDATA
```

APDU command data offset : CDATA = 5

CLA_ISO7816

```
public static final byte CLA_ISO7816
```

APDU command CLA : ISO 7816 = 0x00

INS_SELECT

```
public static final byte INS_SELECT
```

APDU command INS : SELECT = 0xA4

INS_EXTERNAL_AUTHENTICATE

```
public static final byte INS_EXTERNAL_AUTHENTICATE
```

APDU command INS : EXTERNAL AUTHENTICATE = 0x82

javacard.framework
Class ISOException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--javacard.framework.CardRuntimeException
                          |
                          +--javacard.framework.ISOException
```

public class **ISOException**
extends CardRuntimeException

`ISOException` class encapsulates an ISO 7816-4 response status word as its `reason` code.

The `APDU` class throws JCRE owned instances of `ISOException`.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Constructor Summary

`ISOException``(short sw)` Constructs an ISOException instance with the specified status word.	

Method Summary

`static void`	**`throwIt`**`(short sw)` Throws the JCRE owned instance of the ISOException class with the specified status word.

Methods inherited from class javacard.framework.CardRuntimeException
`getReason, setReason`

Methods inherited from class java.lang.Object
equals

Constructor Detail

ISOException

```
public ISOException(short sw)
```

Constructs an ISOException instance with the specified status word. To conserve on resources use `throwIt()` to use the JCRE owned instance of this class.

Parameters:

`sw` - the ISO 7816-4 defined status word

Method Detail

throwIt

```
public static void throwIt(short sw)
```

Throws the JCRE owned instance of the ISOException class with the specified status word.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Parameters:

`sw` - ISO 7816-4 defined status word

Throws:

ISOException - always.

javacard.framework
Class JCSystem

```
java.lang.Object
  |
  +--javacard.framework.JCSystem
```

public final class **JCSystem**
extends Object

The `JCSystem` class includes a collection of methods to control applet execution, resource management, atomic transaction management and inter-applet object sharing in Java Card. All methods in `JCSystem` class are static methods.

The JCSystem class also includes methods to control the persistence and transience of objects. The term *persistent* means that objects and their values persist from one CAD session to the next, indefinitely. Persistent object values are updated atomically using transactions.

The `makeTransient...Array()` methods can be used to create *transient* arrays with primitive data components. Transient array data is lost (in an undefined state, but the real data is unavailable) immediately upon power loss, and is reset to the default value at the occurrence of certain events such as card reset or deselect. Updates to the values of transient arrays are not atomic and are not affected by transactions.

The JCRE maintains an atomic transaction commit buffer which is initialized on card reset (or power on). When a transaction is in progress, the JCRE journals all updates to persistent data space into this buffer so that it can always guarantee, at commit time, that everything in the buffer is written or nothing at all is written. The `JCSystem` includes methods to control an atomic transaction. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

See Also:
`SystemException`, `TransactionException`, `Applet`

Field Summary

`static byte`	**`CLEAR_ON_DESELECT`** This event code indicates that the contents of the transient object are cleared to the default value on applet deselection event or in `CLEAR_ON_RESET` cases.
`static byte`	**`CLEAR_ON_RESET`** This event code indicates that the contents of the transient object are cleared to the default value on card reset (or power on) event.
`static byte`	**`NOT_A_TRANSIENT_OBJECT`** This event code indicates that the object is not transient.

Method Summary	
static void	**abortTransaction**() Aborts the atomic transaction.
static void	**beginTransaction**() Begins an atomic transaction.
static void	**commitTransaction**() Commits an atomic transaction.
static AID	**getAID**() Returns the JCRE owned instance of the AID object associated with the current applet context.
static Shareable	**getAppletShareableInterfaceObject**(AID serverAID, byte parameter) This method is called by a client applet to get a server applet's shareable interface object.
static short	**getMaxCommitCapacity**() Returns the total number of bytes in the commit buffer.
static AID	**getPreviousContextAID**() This method is called to obtain the JCRE owned instance of the AID object associated with the previously active applet context.
static byte	**getTransactionDepth**() Returns the current transaction nesting depth level.
static short	**getUnusedCommitCapacity**() Returns the number of bytes left in the commit buffer.
static short	**getVersion**() Returns the current major and minor version of the Java Card API.
static byte	**isTransient**(Object theObj) Used to check if the specified object is transient.
static AID	**lookupAID**(byte[] buffer, short offset, byte length) Returns the JCRE owned instance of the AID object, if any, encapsulating the specified AID bytes in the buffer parameter if there exists a successfully installed applet on the card whose instance AID exactly matches that of the specified AID bytes.
static boolean[]	**makeTransientBooleanArray**(short length, byte event) Create a transient boolean array with the specified array length.
static byte[]	**makeTransientByteArray**(short length, byte event) Create a transient byte array with the specified array length.

`static Object[]`	**`makeTransientObjectArray`**`(short length, byte event)` Create a transient array of `Object` with the specified array length.
`static short[]`	**`makeTransientShortArray`**`(short length, byte event)` Create a transient short array with the specified array length.

Methods inherited from class java.lang.Object
`equals`

Field Detail

NOT_A_TRANSIENT_OBJECT

`public static final byte` **`NOT_A_TRANSIENT_OBJECT`**

This event code indicates that the object is not transient.

CLEAR_ON_RESET

`public static final byte` **`CLEAR_ON_RESET`**

This event code indicates that the contents of the transient object are cleared to the default value on card reset (or power on) event.

CLEAR_ON_DESELECT

`public static final byte` **`CLEAR_ON_DESELECT`**

This event code indicates that the contents of the transient object are cleared to the default value on applet deselection event or in `CLEAR_ON_RESET` cases.

Notes:

- `CLEAR_ON_DESELECT` *transient objects can be accessed only when the applet which created the object is the currently the selected applet.*
- *The JCRE will throw a* `SecurityException` *if a* `CLEAR_ON_DESELECT` *transient object is accessed when the currently selected applet is not the applet which created the object.*

Method Detail

isTransient

```
public static byte isTransient(Object theObj)
```

Used to check if the specified object is transient.

Notes:

This method returns `NOT_A_TRANSIENT_OBJECT` *if the specified object is* `null` *or is not an array type.*

Parameters:

`theObj` - the object being queried.

Returns:

`NOT_A_TRANSIENT_OBJECT`, `CLEAR_ON_RESET`, or `CLEAR_ON_DESELECT`.

See Also:

`makeTransientBooleanArray(short, byte)`,
`makeTransientByteArray(short, byte)`,
`makeTransientShortArray(short, byte)`,
`makeTransientObjectArray(short, byte)`

---

makeTransientBooleanArray

```
public static boolean[] makeTransientBooleanArray(short length,
                                                  byte event)
                                           throws SystemException
```

Create a transient boolean array with the specified array length.

Parameters:

`length` - the length of the boolean array.

`event` - the `CLEAR_ON...` event which causes the array elements to be cleared.

Throws:

SystemException - with the following reason codes:

- `SystemException.ILLEGAL_VALUE` if event is not a valid event code.
- `SystemException.NO_TRANSIENT_SPACE` if sufficient transient space is not available.
- `SystemException.ILLEGAL_TRANSIENT` if the current applet context is not the currently selected applet context and `CLEAR_ON_DESELECT` is specified.

---

makeTransientByteArray

```
public static byte[] makeTransientByteArray(short length,
                                            byte event)
                                     throws SystemException
```

Create a transient byte array with the specified array length.

Parameters:

`length` - the length of the byte array.

`event` - the `CLEAR_ON...` event which causes the array elements to be cleared.

Throws:

SystemException - with the following reason codes:

- `SystemException.ILLEGAL_VALUE` if event is not a valid event code.
- `SystemException.NO_TRANSIENT_SPACE` if sufficient transient space is not available.
- `SystemException.ILLEGAL_TRANSIENT` if the current applet context is not the currently selected applet context and `CLEAR_ON_DESELECT` is specified.

---

makeTransientShortArray

```
public static short[] makeTransientShortArray(short length,
                                              byte event)
                                       throws SystemException
```

Create a transient short array with the specified array length.

Parameters:

`length` - the length of the short array.

`event` - the `CLEAR_ON...` event which causes the array elements to be cleared.

Throws:

SystemException - with the following reason codes:

- `SystemException.ILLEGAL_VALUE` if event is not a valid event code.
- `SystemException.NO_TRANSIENT_SPACE` if sufficient transient space is not available.
- `SystemException.ILLEGAL_TRANSIENT` if the current applet context is not the currently selected applet context and `CLEAR_ON_DESELECT` is specified.

---

makeTransientObjectArray

```
public static Object[] makeTransientObjectArray(short length,
                                                byte event)
                                         throws SystemException
```

Create a transient array of `Object` with the specified array length.

Parameters:

`length` - the length of the `Object` array.

`event` - the `CLEAR_ON...` event which causes the array elements to be cleared.

Throws:

SystemException - with the following reason codes:

- `SystemException.ILLEGAL_VALUE` if event is not a valid event code.
- `SystemException.NO_TRANSIENT_SPACE` if sufficient transient space is not available.
- `SystemException.ILLEGAL_TRANSIENT` if the current applet context is not the currently selected applet context and `CLEAR_ON_DESELECT` is specified.

getVersion

```
public static short getVersion()
```

Returns the current major and minor version of the Java Card API.

Returns:

version number as byte.byte (major.minor)

getAID

```
public static AID getAID()
```

Returns the JCRE owned instance of the `AID` object associated with the current applet context. Returns `null` if the `Applet.register()` method has not yet been invoked.

JCRE owned instances of `AID` are permanent JCRE Entry Point Objects and can be accessed from any applet context. References to these permanent objects can be stored and re-used.

See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Returns:

the `AID` object.

lookupAID

```
public static AID lookupAID(byte[] buffer,
                            short offset,
                            byte length)
```

Returns the JCRE owned instance of the `AID` object, if any, encapsulating the specified AID bytes in the `buffer` parameter if there exists a successfully installed applet on the card whose instance AID exactly matches that of the specified AID bytes.

JCRE owned instances of `AID` are permanent JCRE Entry Point Objects and can be accessed from any applet context. References to these permanent objects can be stored and re-used.

See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Parameters:

`buffer` - byte array containing the AID bytes.
`offset` - offset within buffer where AID bytes begin.
`length` - length of AID bytes in buffer.

Returns:

the `AID` object, if any; `null` otherwise. A VM exception is thrown if `buffer` is `null`, or if `offset` or `length` are out of range.

beginTransaction

```
public static void beginTransaction()
                            throws TransactionException
```

Begins an atomic transaction. If a transaction is already in progress (transactionDepth != 0), a TransactionException is thrown.

Throws:

TransactionException - with the following reason codes:

- `TransactionException.IN_PROGRESS` if a transaction is already in progress.

See Also:

`commitTransaction()`, `abortTransaction()`

---

abortTransaction

```
public static void abortTransaction()
                            throws TransactionException
```

Aborts the atomic transaction. The contents of the commit buffer is discarded.

Notes:

- *Do not call this method from within a transaction which creates new objects because the JCRE may not recover the heap space used by the new object instances.*
- *The JCRE ensures that any variable of reference type which references an object instantiated from within this aborted transaction is equivalent to a* `null` *reference.*

Throws:

TransactionException - with the following reason codes:

- `TransactionException.NOT_IN_PROGRESS` if a transaction is not in progress.

See Also:

`beginTransaction()`, `commitTransaction()`

---

commitTransaction

```
public static void commitTransaction()
                             throws TransactionException
```

Commits an atomic transaction. The contents of commit buffer is atomically commited. If a transaction is not in progress (transactionDepth == 0) then a TransactionException is thrown.

Throws:

TransactionException - with the following reason codes:

- `TransactionException.NOT_IN_PROGRESS` if a transaction is not in progress.

See Also:

`beginTransaction()`, `abortTransaction()`

getTransactionDepth

```
public static byte getTransactionDepth()
```

Returns the current transaction nesting depth level. At present, only 1 transaction can be in progress at a time.

Returns:

1 if transaction in progress, 0 if not.

getUnusedCommitCapacity

```
public static short getUnusedCommitCapacity()
```

Returns the number of bytes left in the commit buffer.

Returns:

the number of bytes left in the commit buffer

See Also:

`getMaxCommitCapacity()`

getMaxCommitCapacity

```
public static short getMaxCommitCapacity()
```

Returns the total number of bytes in the commit buffer. This is approximately the maximum number of bytes of persistent data which can be modified during a transaction. However, the transaction subsystem requires additional bytes of overhead data to be included in the commit buffer, and this depends on the number of fields modified and the implementation of the transaction subsystem. The application cannot determine the actual maximum amount of data which can be modified during a transaction without taking these overhead bytes into consideration.

Returns:

the total number of bytes in the commit buffer

See Also:

`getUnusedCommitCapacity()`

getPreviousContextAID

```
public static AID getPreviousContextAID()
```

This method is called to obtain the JCRE owned instance of the `AID` object associated with the previously active applet context. This method is typically used by a server applet, while executing a shareable interface method to determine the identity of its client and thereby control access privileges.

JCRE owned instances of `AID` are permanent JCRE Entry Point Objects and can be accessed from any applet context. References to these permanent objects can be stored and re-used.

See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Returns:

the `AID` object of the previous context, or `null` if JCRE.

---

getAppletShareableInterfaceObject

```
public static Shareable getAppletShareableInterfaceObject(AID serverAID,
                                                          byte parameter)
```

This method is called by a client applet to get a server applet's shareable interface object.

This method returns `null` if the `Applet.register()` has not yet been invoked or if the server does not exist or if the server returns `null`.

Parameters:

`serverAID` - the AID of the server applet.

`parameter` - optional parameter data.

Returns:

the shareable interface object or `null`.

See Also:

`Applet.getShareableInterfaceObject(AID, byte)`

---

javacard.framework
Class OwnerPIN

```
java.lang.Object
  |
  +--javacard.framework.OwnerPIN
```

public class **OwnerPIN**
extends Object
implements PIN

This class represents an Owner PIN. It implements Personal Identification Number functionality as defined in the `PIN` interface. It provides the ability to update the PIN and thus owner functionality.

The implementation of this class must protect against attacks based on program flow prediction.Even if a transaction is in progress, internal state such as the try counter, the validated flag and the blocking state must not be conditionally updated during PIN presentation.

If an implementation of this class creates transient arrays, it must ensure that they are `CLEAR_ON_RESET` transient objects.

The protected methods `getValidatedFlag` and `setValidatedFlag` allow a subclass of this class to optimize the storage for the validated boolean state.

Some methods of instances of this class are only suitable for sharing when there exists a trust relationship among the applets. A typical shared usage would use a proxy PIN interface which implements both the `PIN` interface and the `Shareable` interface.

Any of the methods of the `OwnerPIN` may be called with a transaction in progress. None of the methods of `OwnerPIN` class initiate or alter the state of the transaction if one is in progress.

See Also:
`PINException`, `PIN`, `Shareable`, `JCSystem`

Constructor Summary

`OwnerPIN``(byte tryLimit, byte maxPINSize)` Constructor.

Method Summary

boolean	**check**(byte[] pin, short offset, byte length) Compares pin against the PIN value.
byte	**getTriesRemaining**() Returns the number of times remaining that an incorrect PIN can be presented before the PIN is blocked.
protected boolean	**getValidatedFlag**() This protected method returns the validated flag.
boolean	**isValidated**() Returns true if a valid PIN has been presented since the last card reset or last call to reset().
void	**reset**() If the validated flag is set, this method resets it.
void	**resetAndUnblock**() This method resets the validated flag and resets the PIN try counter to the value of the PIN try limit.
protected void	**setValidatedFlag**(boolean value) This protected method sets the value of the validated flag.
void	**update**(byte[] pin, short offset, byte length) This method sets a new value for the PIN and resets the PIN try counter to the value of the PIN try limit.

Methods inherited from class java.lang.Object
equals

Constructor Detail

OwnerPIN

```
public OwnerPIN(byte tryLimit,
                byte maxPINSize)
         throws PINException
```

Constructor. Allocates a new PIN instance.

Parameters:

tryLimit - the maximum number of times an incorrect PIN can be presented.

maxPINSize - the maximum allowed PIN size. maxPINSize must be >=1.

Throws:

PINException - with the following reason codes:

- `PINException.ILLEGAL_VALUE` if `maxPINSize` parameter is less than 1.

Method Detail

getValidatedFlag

```
protected boolean getValidatedFlag()
```

This protected method returns the validated flag. This method is intended for subclass of this `OwnerPIN` to access or override the internal PIN state of the `OwnerPIN`.

Returns:

the boolean state of the PIN validated flag.

---

setValidatedFlag

```
protected void setValidatedFlag(boolean value)
```

This protected method sets the value of the validated flag. This method is intended for subclass of this `OwnerPIN` to control or override the internal PIN state of the `OwnerPIN`.

Parameters:

`value` - the new value for the validated flag.

---

getTriesRemaining

```
public byte getTriesRemaining()
```

Returns the number of times remaining that an incorrect PIN can be presented before the `PIN` is blocked.

Specified by:

getTriesRemaining in interface PIN

Returns:

the number of times remaining

---

check

```
public boolean check(byte[] pin,
                     short offset,
                     byte length)
```

Compares `pin` against the PIN value. If they match and the `PIN` is not blocked, it sets the validated flag and resets the try counter to its maximum. If it does not match, it decrements the try counter, and if the counter has reached zero, blocks the `PIN`. Even if a transaction is in progress, internal state such as the try counter, the validated flag and the blocking state must not be conditionally updated.

Specified by:
check in interface PIN
Parameters:
`pin` - the byte array containing the PIN value being checked
`offset` - the starting offset in the pin array
`length` - the length of pin.
Returns:
`true` if the PIN value matches; `false` otherwise

---

isValidated

```
public boolean isValidated()
```

Returns `true` if a valid PIN has been presented since the last card reset or last call to `reset()`.
Specified by:
isValidated in interface PIN
Returns:
`true` if validated; `false` otherwise

---

reset

```
public void reset()
```

If the validated flag is set, this method resets it. If the validated flag is not set, this method does nothing.
Specified by:
reset in interface PIN

---

update

```
public void update(byte[] pin,
                   short offset,
                   byte length)
            throws PINException
```

This method sets a new value for the PIN and resets the `PIN` try counter to the value of the `PIN` try limit. It also resets the validated flag.

This method copies the input pin parameter into an internal representation. If a transaction is in progress, the new pin and try counter update must be conditional i.e the copy operation must use the transaction facility.
Parameters:
`pin` - the byte array containing the new PIN value
`offset` - the starting offset in the pin array
`length` - the length of the new PIN.

Throws:

PINException - with the following reason codes:

- `PINException.ILLEGAL_VALUE` if length is greater than configured maximum PIN size.

See Also:

`JCSystem.beginTransaction()`

---

resetAndUnblock

```
public void resetAndUnblock()
```

This method resets the validated flag and resets the `PIN` try counter to the value of the `PIN` try limit. This method is used by the owner to re-enable the blocked `PIN`.

---

javacard.framework
Interface PIN

All Known Implementing Classes:
OwnerPIN

public abstract interface **PIN**

This interface represents a PIN. An implementation must maintain these internal values:

- PIN value
- try limit, the maximum number of times an incorrect PIN can be presented before the PIN is blocked. When the PIN is blocked, it cannot be validated even on valid PIN presentation.
- max PIN size, the maximum length of PIN allowed
- try counter, the remaining number of times an incorrect PIN presentation is permitted before the `PIN` becomes blocked.
- validated flag, true if a valid PIN has been presented. This flag is reset on every card reset.

This interface does not make any assumptions about where the data for the PIN value comparison is stored.

An owner implementation of this interface must provide a way to initialize/update the PIN value.The owner implemention of the interface must protect against attacks based on program flow prediction. Even if a transaction is in progress, internal state such as the try counter, the validated flag and the blocking state must not be conditionally updated during PIN presentation.

A typical card global PIN usage will combine an instance of `OwnerPIN` class and a a Proxy PIN interface which implements both the `PIN` and the `Shareable` interfaces. The `OwnerPIN` instance would be manipulated only by the owner who has update privilege. All others would access the global PIN functionality via the proxy PIN interface.

See Also:
`OwnerPIN`, `Shareable`

Method Summary	
boolean	**check**(byte[] pin, short offset, byte length) Compares pin against the PIN value.
byte	**getTriesRemaining**() Returns the number of times remaining that an incorrect PIN can be presented before the PIN is blocked.
boolean	**isValidated**() Returns true if a valid PIN value has been presented since the last card reset or last call to reset().
void	**reset**() If the validated flag is set, this method resets it.

Method Detail

getTriesRemaining

```
public byte getTriesRemaining()
```

Returns the number of times remaining that an incorrect PIN can be presented before the PIN is blocked.

Returns:

the number of times remaining

---

check

```
public boolean check(byte[] pin,
                     short offset,
                     byte length)
```

Compares pin against the PIN value. If they match and the PIN is not blocked, it sets the validated flag and resets the try counter to its maximum. If it does not match, it decrements the try counter, and if the counter has reached zero, blocks the PIN. Even if a transaction is in progress, internal state such as the try counter, the validated flag and the blocking state must not be conditionally updated.

Parameters:

pin - the byte array containing the PIN value being checked
offset - the starting offset in the pin array
length - the length of the PIN value.

Returns:

true if the PIN value matches; false otherwise

isValidated

```
public boolean isValidated()
```

Returns `true` if a valid PIN value has been presented since the last card reset or last call to `reset()`.

Returns:

`true` if validated; `false` otherwise

reset

```
public void reset()
```

If the validated flag is set, this method resets it. If the validated flag is not set, this method does nothing.

javacard.framework
Class PINException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--javacard.framework.CardRuntimeException
                          |
                          +--javacard.framework.PINException
```

public class **PINException**
extends CardRuntimeException

`PINException` represents a `OwnerPIN` class access-related exception.

The `OwnerPIN` class throws JCRE owned instances of `PINException`.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

See Also:
`OwnerPIN`

Field Summary

`static short`	**`ILLEGAL_VALUE`** This reason code is used to indicate that one or more input parameters is out of allowed bounds.

Constructor Summary

`PINException``(short reason)` Constructs a PINException.	

Method Summary

`static void`	**`throwIt`**`(short reason)` Throws the JCRE owned instance of `PINException` with the specified reason.

Methods inherited from class javacard.framework.CardRuntimeException

`getReason, setReason`

Methods inherited from class java.lang.Object

`equals`

Field Detail

ILLEGAL_VALUE

```
public static final short ILLEGAL_VALUE
```

This reason code is used to indicate that one or more input parameters is out of allowed bounds.

Constructor Detail

PINException

```
public PINException(short reason)
```

Constructs a PINException. To conserve on resources use `throwIt()` to use the JCRE owned instance of this class.

Parameters:

`reason` - the reason for the exception.

Method Detail

throwIt

```
public static void throwIt(short reason)
```

Throws the JCRE owned instance of `PINException` with the specified reason.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Parameters:

`reason` - the reason for the exception.

Throws:

PINException - always.

---

javacard.framework
Interface Shareable

public abstract interface **Shareable**

The Shareable interface serves to identify all shared objects. Any object that needs to be shared through the applet firewall must directly or indirectly implement this interface. Only those methods specified in a shareable interface are available through the firewall. Implementation classes can implement any number of shareable interfaces and can extend other shareable implementation classes.

javacard.framework
Class SystemException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--javacard.framework.CardRuntimeException
                          |
                          +--javacard.framework.SystemException
```

public class **SystemException**
extends CardRuntimeException

`SystemException` represents a `JCSystem` class related exception. It is also thrown by the `javacard.framework.Applet.register()` methods and by the `AID` class constructor.

These API classes throw JCRE owned instances of `SystemException`.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

See Also:
`JCSystem`, `Applet`, `AID`

Field Summary

static short	**ILLEGAL_AID** This reason code is used by the `javacard.framework.Applet.register()` method to indicate that the input AID parameter is not a legal AID value.
static short	**ILLEGAL_TRANSIENT** This reason code is used to indicate that the request to create a transient object is not allowed in the current applet context.
static short	**ILLEGAL_VALUE** This reason code is used to indicate that one or more input parameters is out of allowed bounds.
static short	**NO_RESOURCE** This reason code is used to indicate that there is insufficient resource in the Card for the request.
static short	**NO_TRANSIENT_SPACE** This reason code is used by the `makeTransient..()` methods to indicate that no room is available in volatile memory for the requested object.

Constructor Summary

SystemException(short reason) Constructs a SystemException.	

Method Summary

static void	**throwIt**(short reason) Throws the JCRE owned instance of `SystemException` with the specified reason.

Methods inherited from class javacard.framework.CardRuntimeException
getReason, setReason

Methods inherited from class java.lang.Object
`equals`

Field Detail

ILLEGAL_VALUE

`public static final short` **`ILLEGAL_VALUE`**

This reason code is used to indicate that one or more input parameters is out of allowed bounds.

NO_TRANSIENT_SPACE

`public static final short` **`NO_TRANSIENT_SPACE`**

This reason code is used by the `makeTransient..()` methods to indicate that no room is available in volatile memory for the requested object.

ILLEGAL_TRANSIENT

`public static final short` **`ILLEGAL_TRANSIENT`**

This reason code is used to indicate that the request to create a transient object is not allowed in the current applet context. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

ILLEGAL_AID

`public static final short` **`ILLEGAL_AID`**

This reason code is used by the `javacard.framework.Applet.register()` method to indicate that the input AID parameter is not a legal AID value.

NO_RESOURCE

`public static final short` **`NO_RESOURCE`**

This reason code is used to indicate that there is insufficient resource in the Card for the request.

For example, the Java Card Virtual Machine may `throw` this exception reason when there is insufficient heap space to create a new instance.

Constructor Detail

SystemException

```
public SystemException(short reason)
```

Constructs a SystemException. To conserve on resources use `throwIt()` to use the JCRE owned instance of this class.

Parameters:

`reason` - the reason for the exception.

Method Detail

throwIt

```
public static void throwIt(short reason)
```

Throws the JCRE owned instance of `SystemException` with the specified reason.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Parameters:

`reason` - the reason for the exception.

Throws:

SystemException - always.

javacard.framework
Class TransactionException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--javacard.framework.CardRuntimeException
                          |
                          +--javacard.framework.TransactionException
```

public class **TransactionException**
extends CardRuntimeException

`TransactionException` represents an exception in the transaction subsystem. The methods referred to in this class are in the `JCSystem` class.

The `JCSystem` class and the transaction facility throw JCRE owned instances of `TransactionException`.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

See Also:
`JCSystem`

Field Summary

static short	**BUFFER_FULL** This reason code is used during a transaction to indicate that the commit buffer is full.
static short	**IN_PROGRESS** This reason code is used by the `beginTransaction` method to indicate a transaction is already in progress.
static short	**INTERNAL_FAILURE** This reason code is used during a transaction to indicate an internal JCRE problem (fatal error).
static short	**NOT_IN_PROGRESS** This reason code is used by the `abortTransaction` and `commintTransaction` methods when a transaction is not in progress.

Constructor Summary

TransactionException(short reason) Constructs a TransactionException with the specified reason.

Method Summary

static void	**throwIt**(short reason) Throws the JCRE owned instance of `TransactionException` with the specified reason.

Methods inherited from class javacard.framework.CardRuntimeException
`getReason, setReason`

Methods inherited from class java.lang.Object
`equals`

Field Detail

IN_PROGRESS

```
public static final short IN_PROGRESS
```

This reason code is used by the `beginTransaction` method to indicate a transaction is already in progress.

NOT_IN_PROGRESS

```
public static final short NOT_IN_PROGRESS
```

This reason code is used by the `abortTransaction` and `commintTransaction` methods when a transaction is not in progress.

BUFFER_FULL

```
public static final short BUFFER_FULL
```

This reason code is used during a transaction to indicate that the commit buffer is full.

INTERNAL_FAILURE

```
public static final short INTERNAL_FAILURE
```

This reason code is used during a transaction to indicate an internal JCRE problem (fatal error).

Constructor Detail

TransactionException

```
public TransactionException(short reason)
```

Constructs a TransactionException with the specified reason. To conserve on resources use `throwIt()` to use the JCRE owned instance of this class.

Method Detail

throwIt

```
public static void throwIt(short reason)
```

Throws the JCRE owned instance of `TransactionException` with the specified reason.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Throws:

TransactionException - always.

---

javacard.framework
Class UserException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--javacard.framework.CardException
                    |
                    +--javacard.framework.UserException
```

public class **UserException**
extends CardException

`UserException` represents a User exception. This class also provides a resource-saving mechanism (the `throwIt()` method) for user exceptions by using a JCRE owned instance.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Constructor Summary

`UserException``()` Constructs a `UserException` with reason = 0.
`UserException``(short reason)` Constructs a `UserException` with the specified reason.

Method Summary

`static void`	**`throwIt`**`(short reason)` Throws the JCRE owned instance of `UserException` with the specified reason.

Methods inherited from class javacard.framework.CardException
`getReason, setReason`

Methods inherited from class java.lang.Object
equals

Constructor Detail

UserException

```
public UserException()
```

Constructs a `UserException` with reason = 0. To conserve on resources use `throwIt()` to use the JCRE owned instance of this class.

UserException

```
public UserException(short reason)
```

Constructs a `UserException` with the specified reason. To conserve on resources use `throwIt()` to use the JCRE owned instance of this class.

Parameters:

`reason` - the reason for the exception.

Method Detail

throwIt

```
public static void throwIt(short reason)
                    throws UserException
```

Throws the JCRE owned instance of `UserException` with the specified reason.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Parameters:

`reason` - the reason for the exception.

Throws:

UserException - always.

javacard.framework
Class Util

```
java.lang.Object
  |
  +--javacard.framework.Util
```

public class **Util**
extends Object

The `Util` class contains common utility functions. Some of the methods may be implemented as native functions for performance reasons. All methods in `Util`, class are static methods.

Some methods of `Util` namely `arrayCopy()`, `arrayCopyNonAtomic()`, `arrayFillNonAtomic()` and `setShort()`, refer to the persistence of array objects. The term *persistent* means that arrays and their values persist from one CAD session to the next, indefinitely. The `JCSystem` class is used to control the persistence and transience of objects.

See Also:
`JCSystem`

Method Summary	
static byte	**arrayCompare**(byte[] src, short srcOff, byte[] dest, short destOff, short length) Compares an array from the specified source array, beginning at the specified position, with the specified position of the destination array from left to right.
static short	**arrayCopy**(byte[] src, short srcOff, byte[] dest, short destOff, short length) Copies an array from the specified source array, beginning at the specified position, to the specified position of the destination array.
static short	**arrayCopyNonAtomic**(byte[] src, short srcOff, byte[] dest, short destOff, short length) Copies an array from the specified source array, beginning at the specified position, to the specified position of the destination array (non-atomically).
static short	**arrayFillNonAtomic**(byte[] bArray, short bOff, short bLen, byte bValue) Fills the byte array (non-atomically) beginning at the specified position, for the specified length with the specified byte value.
static short	**getShort**(byte[] bArray, short bOff) Concatenates two bytes in a byte array to form a short value.
static short	**makeShort**(byte b1, byte b2) Concatenates the two parameter bytes to form a short value.
static short	**setShort**(byte[] bArray, short bOff, short sValue) Deposits the short value as two successive bytes at the specified offset in the byte array.

Methods inherited from class java.lang.Object
equals

Method Detail

arrayCopy

```
public static final short arrayCopy(byte[] src,
                                    short srcOff,
                                    byte[] dest,
                                    short destOff,
```

```
                short length)
        throws IndexOutOfBoundsException,
                NullPointerException,
                TransactionException
```

Copies an array from the specified source array, beginning at the specified position, to the specified position of the destination array.

Notes:

- *If* `srcOff` *or* `destOff` *or* `length` *parameter is negative an* `IndexOutOfBoundsException` *exception is thrown.*
- *If* `srcOff+length` *is greater than* `src.length`*, the length of the* `src` *array a* `IndexOutOfBoundsException` *exception is thrown and no copy is performed.*
- *If* `destOff+length` *is greater than* `dest.length`*, the length of the* `dest` *array an* `IndexOutOfBoundsException` *exception is thrown and no copy is performed.*
- *If* `src` *or* `dest` *parameter is* `null` *a* `NullPointerException` *exception is thrown.*
- *If the* `src` *and* `dest` *arguments refer to the same array object, then the copying is performed as if the components at positions* `srcOff` *through* `srcOff+length-1` *were first copied to a temporary array with length components and then the contents of the temporary array were copied into positions* `destOff` *through* `destOff+length-1` *of the argument array.*
- *If the destination array is persistent, the entire copy is performed atomically.*
- *The copy operation is subject to atomic commit capacity limitations. If the commit capacity is exceeded, no copy is performed and a* `TransactionException` *exception is thrown.*

Parameters:

`src` - source byte array.
`srcOff` - offset within source byte array to start copy from.
`dest` - destination byte array.
`destOff` - offset within destination byte array to start copy into.
`length` - byte length to be copied.

Returns:

`destOff+length`

Throws:

IndexOutOfBoundsException - - if copying would cause access of data outside array bounds.
NullPointerException - - if either `src` or `dest` is `null`.
TransactionException - - if copying would cause the commit capacity to be exceeded.

See Also:

`JCSystem.getUnusedCommitCapacity()`

---

arrayCopyNonAtomic

```
public static final short arrayCopyNonAtomic(byte[] src,
                                             short srcOff,
                                             byte[] dest,
                                             short destOff,
                                             short length)
                                      throws IndexOutOfBoundsException,
                                             NullPointerException
```

Copies an array from the specified source array, beginning at the specified position, to the specified position of the destination array (non-atomically).

This method does not use the transaction facility during the copy operation even if a transaction is in progress. Thus, this method is suitable for use only when the contents of the destination array can be left in a partially modified state in the event of a power loss in the middle of the copy operation.

Notes:

- *If* `srcOff` *or* `destOff` *or* `length` *parameter is negative an* `IndexOutOfBoundsException` *exception is thrown.*
- *If* `srcOff+length` *is greater than* `src.length`*, the length of the* `src` *array a* `IndexOutOfBoundsException` *exception is thrown and no copy is performed.*
- *If* `destOff+length` *is greater than* `dest.length`*, the length of the* `dest` *array an* `IndexOutOfBoundsException` *exception is thrown and no copy is performed.*
- *If* `src` *or* `dest` *parameter is* `null` *a* `NullPointerException` *exception is thrown.*
- *If the* `src` *and* `dest` *arguments refer to the same array object, then the copying is performed as if the components at positions* `srcOff` *through* `srcOff+length-1` *were first copied to a temporary array with length components and then the contents of the temporary array were copied into positions* `destOff` *through* `destOff+length-1` *of the argument array.*
- *If power is lost during the copy operation and the destination array is persistent, a partially changed destination array could result.*
- *The copy* `length` *parameter is not constrained by the atomic commit capacity limitations.*

Parameters:

`src` - source byte array.
`srcOff` - offset within source byte array to start copy from.
`dest` - destination byte array.
`destOff` - offset within destination byte array to start copy into.
`length` - byte length to be copied.

Returns:

`destOff+length`

Throws:

IndexOutOfBoundsException - - if copying would cause access of data outside array bounds.
NullPointerException - - if either `src` or `dest` is `null`.

See Also:

`JCSystem.getUnusedCommitCapacity()`

---

arrayFillNonAtomic

```
public static final short arrayFillNonAtomic(byte[] bArray,
                                              short bOff,
                                              short bLen,
                                              byte bValue)
                                       throws IndexOutOfBoundsException,
                                              NullPointerException
```

Fills the byte array (non-atomically) beginning at the specified position, for the specified length with the specified byte value.

This method does not use the transaction facility during the fill operation even if a transaction is in progress. Thus, this method is suitable for use only when the contents of the byte array can be left in a partially filled state in the event of a power loss in the middle of the fill operation.

Notes:

- *If* `bOff` *or* `bLen` *parameter is negative an* `IndexOutOfBoundsException` *exception is thrown.*
- *If* `bOff+bLen` *is greater than* `bArray.length`*, the length of the* `bArray` *array an* `IndexOutOfBoundsException` *exception is thrown.*
- *If* `bArray` *parameter is* `null` *a* `NullPointerException` *exception is thrown.*
- *If power is lost during the copy operation and the byte array is persistent, a partially changed byte array could result.*
- *The* `bLen` *parameter is not constrained by the atomic commit capacity limitations.*

Parameters:

`bArray` - the byte array.
`bOff` - offset within byte array to start filling bValue into.
`bLen` - byte length to be filled.
`bValue` - the value to fill the byte array with.

Returns:

`bOff+bLen`

Throws:

IndexOutOfBoundsException - - if the fill operation would cause access of data outside array bounds.
NullPointerException - - if bArray is `null`

See Also:

`JCSystem.getUnusedCommitCapacity()`

---

arrayCompare

```
public static final byte arrayCompare(byte[] src,
                                       short srcOff,
                                       byte[] dest,
                                       short destOff,
                                       short length)
                                throws IndexOutOfBoundsException,
                                       NullPointerException
```

Compares an array from the specified source array, beginning at the specified position, with the specified position of the destination array from left to right. Returns the ternary result of the comparison : less than(-1), equal(0) or greater than(1).

Notes:

- *If* `srcOff` *or* `destOff` *or* `length` *parameter is negative an* `IndexOutOfBoundsException` *exception is thrown.*

- *If* `srcOff+length` *is greater than* `src.length`*, the length of the* `src` *array a* `IndexOutOfBoundsException` *exception is thrown.*
- *If* `destOff+length` *is greater than* `dest.length`*, the length of the* `dest` *array an* `IndexOutOfBoundsException` *exception is thrown.*
- *If* `src` *or* `dest` *parameter is* `null` *a* `NullPointerException` *exception is thrown.*

Parameters:

`src` - source byte array.
`srcOff` - offset within source byte array to start compare.
`dest` - destination byte array.
`destOff` - offset within destination byte array to start compare.
`length` - byte length to be compared.

Returns:

the result of the comparison as follows:

- `0` if identical
- `-1` if the first miscomparing byte in source array is less than that in destination array,
- `1` if the first miscomparing byte in source array is greater that that in destination array.

Throws:

IndexOutOfBoundsException - - if comparing all bytes would cause access of data outside array bounds.
NullPointerException - - if either `src` or `dest` is `null`.

---

makeShort

```
public static final short makeShort(byte b1,
                                    byte b2)
```

Concatenates the two parameter bytes to form a short value.

Parameters:

`b1` - the first byte (high order byte).
`b2` - the second byte (low order byte).

Returns:

the short value - the concatenated result

---

getShort

```
public static final short getShort(byte[] bArray,
                                   short bOff)
```

Concatenates two bytes in a byte array to form a short value.

Parameters:

`bArray` - byte array.
`bOff` - offset within byte array containing first byte (the high order byte).

Returns:

the short value - the concatenated result

setShort

```
public static final short setShort(byte[] bArray,
                                   short bOff,
                                   short sValue)
                            throws TransactionException
```

Deposits the short value as two successive bytes at the specified offset in the byte array.

Parameters:

`bArray` - byte array.

`bOff` - offset within byte array to deposit the first byte (the high order byte).

`sValue` - the short value to set into array.

Returns:

`bOff+2`

Note:

- *If the byte array is persistent, this operation is performed atomically. If the commit capacity is exceeded, no operation is performed and a* `TransactionException` *exception is thrown.*

Throws:

TransactionException - - if the operation would cause the commit capacity to be exceeded.

See Also:

`JCSystem.getUnusedCommitCapacity()`

Package javacard.security

Provides the classes and interfaces for the Java Card security framework.

See:

Description

Interface Summary	
DESKey	`DESKey` contains an 8/16/24 byte key for single/2 key triple DES/3 key triple DES operations.
DSAKey	The DSAKey interface is the base interface for the DSA algorithms private and public key implementaions.
DSAPrivateKey	The `DSAPrivateKey` interface is used to sign data using the DSA algorithm.
DSAPublicKey	The `DSAPublicKey` interface is used to verify signatures on signed data using the DSA algorithm.
Key	The `Key` interface is the base interface for all keys.
PrivateKey	The `PrivateKey` class is the base class for private keys used in asymmetric algorithms.
PublicKey	The `PublicKey` class is the base class for public keys used in asymmetric algorithms.
RSAPrivateCrtKey	The `RSAPrivateCrtKey` interface is used to sign data using the RSA algorithm in its Chinese Remainder Theorem form.
RSAPrivateKey	The `RSAPrivateKey` class is used to sign data using the RSA algorithm in its modulus/exponent form.
RSAPublicKey	The `RSAPublicKey` is used to verify signatures on signed data using the RSA algorithm.
SecretKey	The `SecretKey` class is the base interface for keys used in symmetric alogrightms (e.g. DES).

Class Summary	
KeyBuilder	The `KeyBuilder` class is a key object factory.
MessageDigest	The `MessageDigest` class is the base class for hashing algorthims.
RandomData	The `RandomData` abstract class is the base class for random number generation.
Signature	The `Signature` class is the base class for Signature algorthims.

Exception Summary	
CryptoException	`CryptoException` represents a cryptography-related exception.

Package javacard.security Description

Provides the classes and interfaces for the Java Card security framework.

javacard.security
Class CryptoException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--javacard.framework.CardRuntimeException
                          |
                          +--javacard.security.CryptoException
```

public class **CryptoException**
extends CardRuntimeException

`CryptoException` represents a cryptography-related exception.

The API classes throw JCRE owned instances of `SystemException`.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components.

See Also:
`KeyBuilder`, `MessageDigest`, `Signature`, `RandomData`, `Cipher`

Field Summary

static short	**ILLEGAL_USE** This reason code is used to indicate that the signature or cipher algorithm does not pad the incoming message and the input message is not block aligned.
static short	**ILLEGAL_VALUE** This reason code is used to indicate that one or more input parameters is out of allowed bounds.
static short	**INVALID_INIT** This reason code is used to indicate that the signature or cipher object has not been correctly initialized for the requested operation.
static short	**NO_SUCH_ALGORITHM** This reason code is used to indicate that the requested algorithm or key type is not supported.
static short	**UNINITIALIZED_KEY** This reason code is used to indicate that the key is uninitialized.

Constructor Summary

CryptoException(short reason) Constructs a CryptoException with the specified reason.

Method Summary

static void	**throwIt**(short reason) Throws the JCRE owned instance of CryptoException with the specified reason.

Methods inherited from class javacard.framework.CardRuntimeException
getReason, setReason

Methods inherited from class java.lang.Object
equals

Field Detail

ILLEGAL_VALUE

```
public static final short ILLEGAL_VALUE
```

This reason code is used to indicate that one or more input parameters is out of allowed bounds.

UNINITIALIZED_KEY

```
public static final short UNINITIALIZED_KEY
```

This reason code is used to indicate that the key is uninitialized.

NO_SUCH_ALGORITHM

```
public static final short NO_SUCH_ALGORITHM
```

This reason code is used to indicate that the requested algorithm or key type is not supported.

INVALID_INIT

```
public static final short INVALID_INIT
```

This reason code is used to indicate that the signature or cipher object has not been correctly initialized for the requested operation.

ILLEGAL_USE

```
public static final short ILLEGAL_USE
```

This reason code is used to indicate that the signature or cipher algorithm does not pad the incoming message and the input message is not block aligned.

Constructor Detail

CryptoException

```
public CryptoException(short reason)
```

Constructs a `CryptoException` with the specified reason. To conserve on resources use `throwIt()` to use the JCRE owned instance of this class.

Parameters:

`reason` - the reason for the exception.

Method Detail

throwIt

```
public static void throwIt(short reason)
```

Throws the JCRE owned instance of `CryptoException` with the specified reason.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Parameters:

`reason` - the reason for the exception.

Throws:

CryptoException - always.

javacard.security
Interface DESKey

public abstract interface **DESKey**
extends SecretKey

`DESKey` contains an 8/16/24 byte key for single/2 key triple DES/3 key triple DES operations.

When the key data is set, the key is initialized and ready for use.

See Also:
`KeyBuilder`, `Signature`, `Cipher`, `KeyEncryption`

Method Summary

byte	**`getKey`**`(byte[] keyData, short kOff)` Returns the `Key` data in plain text.
void	**`setKey`**`(byte[] keyData, short kOff)` Sets the `Key` data.

Methods inherited from interface javacard.security.Key
`clearKey, getSize, getType, isInitialized`

Method Detail

setKey

```
public void setKey(byte[] keyData,
                   short kOff)
            throws CryptoException
```

Sets the `Key` data. The plaintext length of input key data is 8 bytes for DES, 16 bytes for 2 key triple DES and 24 bytes for 3 key triple DES. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input key data is copied into the internal representation.

Parameters:

`keyData` - byte array containing key initialization data
`kOff` - offset within keyData to start

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input key data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`, `keyData` *is decrypted using the* `Cipher` *object.*

---

getKey

```
public byte getKey(byte[] keyData,
                   short kOff)
```

Returns the `Key` data in plain text. The length of output key data is 8 bytes for DES, 16 bytes for 2 key triple DES and 24 bytes for 3 key triple DES. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`keyData` - byte array to return key data

`kOff` - offset within `keyData` to start.

Returns:

the byte length of the key data returned.

---

javacard.security
Interface DSAKey

All Known Subinterfaces:
DSAPrivateKey, DSAPublicKey

public abstract interface **DSAKey**

The DSAKey interface is the base interface for the DSA algorithms private and public key implementaions. A DSA private key implementation must also implement the `DSAPrivateKey` interface methods. A DSA public key implementation must also implement the `DSAPublicKey` interface methods.

When all four components of the key (X or Y,P,Q,G) are set, the key is initialized and ready for use.

See Also:
`DSAPublicKey`, `DSAPrivateKey`, `KeyBuilder`, `Signature`, `KeyEncryption`

Method Summary

`short`	**`getG`**`(byte[] buffer, short offset)` Returns the subprime parameter value of the key in plain text.
`short`	**`getP`**`(byte[] buffer, short offset)` Returns the base parameter value of the key in plain text.
`short`	**`getQ`**`(byte[] buffer, short offset)` Returns the prime parameter value of the key in plain text.
`void`	**`setG`**`(byte[] buffer, short offset, short length)` Sets the subprime parameter value of the key.
`void`	**`setP`**`(byte[] buffer, short offset, short length)` Sets the base parameter value of the key.
`void`	**`setQ`**`(byte[] buffer, short offset, short length)` Sets the prime parameter value of the key.

Method Detail

setP

```
public void setP(byte[] buffer,
                 short offset,
                 short length)
          throws CryptoException
```

Sets the base parameter value of the key. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input base parameter data is copied into the internal representation.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer at which the base parameter value begins
`length` - the length of the base parameter value

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input parameter data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the base parameter value is decrypted using the* `Cipher` *object.*

---

setQ

```
public void setQ(byte[] buffer,
                 short offset,
                 short length)
          throws CryptoException
```

Sets the prime parameter value of the key. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input prime parameter data is copied into the internal representation.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer at which the prime parameter value begins
`length` - the length of the prime parameter value

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input parameter data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the prime parameter value is decrypted using the* `Cipher` *object.*

setG

```
public void setG(byte[] buffer,
                 short offset,
                 short length)
          throws CryptoException
```

Sets the subprime parameter value of the key. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input subprime parameter data is copied into the internal representation.

Parameters:

`buffer` - the input buffer

`offset` - the offset into the input buffer at which the subprime parameter value begins

`length` - the length of the subprime parameter value

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input parameter data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the subprime parameter value is decrypted using the* `Cipher` *object.*

getP

```
public short getP(byte[] buffer,
                  short offset)
```

Returns the base parameter value of the key in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer

`offset` - the offset into the output buffer at which the base parameter value starts

Returns:

the byte length of the base parameter value returned

getQ

```
public short getQ(byte[] buffer,
                  short offset)
```

Returns the prime parameter value of the key in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer

`offset` - the offset into the output buffer at which the prime parameter value begins

Returns:

the byte length of the prime parameter value returned

---

getG

```
public short getG(byte[] buffer,
                  short offset)
```

Returns the subprime parameter value of the key in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer

`offset` - the offset into the output buffer at which the subprime parameter value begins

Returns:

the byte length of the subprime parameter value returned

---

javacard.security
Interface DSAPrivateKey

public abstract interface **DSAPrivateKey**
extends PrivateKey, DSAKey

The `DSAPrivateKey` interface is used to sign data using the DSA algorithm. An implementation of `DSAPrivateKey` interface must also implement the `DSAKey` interface methods.

When all four components of the key (X,P,Q,G) are set, the key is initialized and ready for use.

See Also:
`DSAPublicKey`, `KeyBuilder`, `Signature`, `KeyEncryption`

Method Summary

`short`	**`getX`**`(byte[] buffer, short offset)` Returns the value of the key in plain text.
`void`	**`setX`**`(byte[] buffer, short offset, short length)` Sets the value of the key.

Methods inherited from interface javacard.security.DSAKey

`getG, getP, getQ, setG, setP, setQ`

Methods inherited from interface javacard.security.Key

`clearKey, getSize, getType, isInitialized`

Method Detail

setX

```
public void setX(byte[] buffer,
                 short offset,
                 short length)
          throws CryptoException
```

Sets the value of the key. When the base, prime and subprime parameters are intialized and the key value is set, the key is ready for use. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input key data is copied into the internal representation.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer at which the modulus value begins
`length` - the length of the modulus

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input key data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the key value is decrypted using the* `Cipher` *object.*

---

getX

```
public short getX(byte[] buffer,
                  short offset)
```

Returns the value of the key in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer
`offset` - the offset into the output buffer at which the key value starts

Returns:

the byte length of the key value returned

---

javacard.security
Interface DSAPublicKey

public abstract interface **DSAPublicKey**
extends PublicKey, DSAKey

The `DSAPublicKey` interface is used to verify signatures on signed data using the DSA algorithm. An implementation of `DSAPublicKey` interface must also implement the `DSAKey` interface methods.

When all four components of the key (Y,P,Q,G) are set, the key is initialized and ready for use.

See Also:
`DSAPrivateKey`, `KeyBuilder`, `Signature`, `KeyEncryption`

Method Summary

`short`	**`getY`**`(byte[] buffer, short offset)` Returns the value of the key in plain text.
`void`	**`setY`**`(byte[] buffer, short offset, short length)` Sets the value of the key.

Methods inherited from interface javacard.security.DSAKey
`getG, getP, getQ, setG, setP, setQ`

Methods inherited from interface javacard.security.Key
`clearKey, getSize, getType, isInitialized`

Method Detail

setY

```
public void setY(byte[] buffer,
                 short offset,
                 short length)
          throws CryptoException
```

Sets the value of the key. When the base, prime and subprime parameters are intialized and the key value is set, the key is ready for use. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input key data is copied into the internal representation.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer at which the key value begins
`length` - the length of the key value

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input key data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the key value is decrypted using the* `Cipher` *object.*

---

getY

```
public short getY(byte[] buffer,
                  short offset)
```

Returns the value of the key in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer
`offset` - the offset into the input buffer at which the key value starts

Returns:

the byte length of the key value returned

---

javacard.security
Interface Key

All Known Subinterfaces:
DESKey, DSAPrivateKey, DSAPublicKey, PrivateKey, PublicKey, RSAPrivateCrtKey, RSAPrivateKey, RSAPublicKey, SecretKey

public abstract interface **Key**

The `Key` interface is the base interface for all keys.

See Also:
`KeyBuilder`

Method Summary

`void`	**`clearKey`**`()` Clears the key and sets its initialized state to false.
`short`	**`getSize`**`()` Returns the key size in number of bits.
`byte`	**`getType`**`()` Returns the key interface type.
`boolean`	**`isInitialized`**`()` Reports the initialized state of the key.

Method Detail

isInitialized

`public boolean` **`isInitialized`**`()`

Reports the initialized state of the key. Keys must be initialized before being used.

A `Key` object sets its initialized state to true only when all the associated set methods have been invoked at least once since the time the initialized state was set to false.

A newly created `Key` object sets its initialized state to false. Invocation of the `clearKey()` method sets the initialized state to false. A key with transient key data sets its initialized state to false on the associated clear events.

Returns:
`true` if the key has been initialized.

---

clearKey

```
public void clearKey()
```

Clears the key and sets its initialized state to false.

---

getType

```
public byte getType()
```

Returns the key interface type.
Returns:
the key interface type.

See Also:
`KeyBuilder`

---

getSize

```
public short getSize()
```

Returns the key size in number of bits.
Returns:
the key size in number of bits.

---

javacard.security
Class KeyBuilder

```
java.lang.Object
  |
  +--javacard.security.KeyBuilder
```

public class **KeyBuilder**
extends Object

The `KeyBuilder` class is a key object factory.

Field Summary

`static short`	**`LENGTH_DES`** DES Key Length `LENGTH_DES` = 64.
`static short`	**`LENGTH_DES3_2KEY`** DES Key Length `LENGTH_DES3_2KEY` = 128.
`static short`	**`LENGTH_DES3_3KEY`** DES Key Length `LENGTH_DES3_3KEY` = 192.
`static short`	**`LENGTH_DSA_1024`** DSA Key Length `LENGTH_DSA_1024` = 1024.
`static short`	**`LENGTH_DSA_512`** DSA Key Length `LENGTH_DSA_512` = 512.
`static short`	**`LENGTH_DSA_768`** DSA Key Length `LENGTH_DSA_768` = 768.
`static short`	**`LENGTH_RSA_1024`** RSA Key Length `LENGTH_RSA_1024` = 1024.
`static short`	**`LENGTH_RSA_2048`** RSA Key Length `LENGTH_RSA_2048` = 2048.
`static short`	**`LENGTH_RSA_512`** RSA Key Length `LENGTH_RSA_512` = 512.
`static short`	**`LENGTH_RSA_768`** RSA Key Length `LENGTH_RSA_768` = 768.
`static byte`	**`TYPE_DES`** `Key` object which implements interface type `DESKey` with persistent key data.

static byte	**TYPE_DES_TRANSIENT_DESELECT** Key object which implements interface type DESKey with CLEAR_ON_DESELECT transient key data.
static byte	**TYPE_DES_TRANSIENT_RESET** Key object which implements interface type DESKey with CLEAR_ON_RESET transient key data.
static byte	**TYPE_DSA_PRIVATE** Key object which implements the interface type DSAPrivateKey for the DSA algorithm.
static byte	**TYPE_DSA_PUBLIC** Key object which implements the interface type DSAPublicKey for the DSA algorithm.
static byte	**TYPE_RSA_CRT_PRIVATE** Key object which implements interface type RSAPrivateCrtKey which uses Chinese Remainder Theorem.
static byte	**TYPE_RSA_PRIVATE** Key object which implements interface type RSAPrivateKey which uses modulus/exponent form.
static byte	**TYPE_RSA_PUBLIC** Key object which implements interface type RSAPublicKey.

Method Summary

static Key	**buildKey**(byte keyType, short keyLength, boolean keyEncryption) Creates cryptographic keys for signature and cipher algorithms.

Methods inherited from class java.lang.Object
equals

Field Detail

TYPE_DES_TRANSIENT_RESET

`public static final byte` **`TYPE_DES_TRANSIENT_RESET`**

`Key` object which implements interface type `DESKey` with CLEAR_ON_RESET transient key data.

This `Key` object implicitly performs a `clearKey()` on power on or card reset.

TYPE_DES_TRANSIENT_DESELECT

`public static final byte` **`TYPE_DES_TRANSIENT_DESELECT`**

`Key` object which implements interface type `DESKey` with CLEAR_ON_DESELECT transient key data.

This `Key` object implicitly performs a `clearKey()` on power on, card reset and applet deselection.

TYPE_DES

`public static final byte` **`TYPE_DES`**

`Key` object which implements interface type `DESKey` with persistent key data.

TYPE_RSA_PUBLIC

`public static final byte` **`TYPE_RSA_PUBLIC`**

`Key` object which implements interface type `RSAPublicKey`.

TYPE_RSA_PRIVATE

`public static final byte` **`TYPE_RSA_PRIVATE`**

`Key` object which implements interface type `RSAPrivateKey` which uses modulus/exponent form.

TYPE_RSA_CRT_PRIVATE

`public static final byte` **`TYPE_RSA_CRT_PRIVATE`**

`Key` object which implements interface type `RSAPrivateCrtKey` which uses Chinese Remainder Theorem.

TYPE_DSA_PUBLIC

```
public static final byte TYPE_DSA_PUBLIC
```

`Key` object which implements the interface type `DSAPublicKey` for the DSA algorithm.

TYPE_DSA_PRIVATE

```
public static final byte TYPE_DSA_PRIVATE
```

`Key` object which implements the interface type `DSAPrivateKey` for the DSA algorithm.

LENGTH_DES

```
public static final short LENGTH_DES
```

DES Key Length `LENGTH_DES` = 64.

LENGTH_DES3_2KEY

```
public static final short LENGTH_DES3_2KEY
```

DES Key Length `LENGTH_DES3_2KEY` = 128.

LENGTH_DES3_3KEY

```
public static final short LENGTH_DES3_3KEY
```

DES Key Length `LENGTH_DES3_3KEY` = 192.

LENGTH_RSA_512

```
public static final short LENGTH_RSA_512
```

RSA Key Length `LENGTH_RSA_512` = 512.

LENGTH_RSA_768

```
public static final short LENGTH_RSA_768
```

RSA Key Length `LENGTH_RSA_768` = 768.

LENGTH_RSA_1024

```
public static final short LENGTH_RSA_1024
```

RSA Key Length `LENGTH_RSA_1024` = 1024.

LENGTH_RSA_2048

```
public static final short LENGTH_RSA_2048
```

RSA Key Length `LENGTH_RSA_2048` = 2048.

LENGTH_DSA_512

```
public static final short LENGTH_DSA_512
```

DSA Key Length `LENGTH_DSA_512` = 512.

LENGTH_DSA_768

```
public static final short LENGTH_DSA_768
```

DSA Key Length `LENGTH_DSA_768` = 768.

LENGTH_DSA_1024

```
public static final short LENGTH_DSA_1024
```

DSA Key Length `LENGTH_DSA_1024` = 1024.

Method Detail

buildKey

```
public static Key buildKey(byte keyType,
                           short keyLength,
                           boolean keyEncryption)
                    throws CryptoException
```

Creates cryptographic keys for signature and cipher algorithms. Instances created by this method may be the only key objects used to initialize instances of `Signature` and `Cipher`. Note that the object returned must be cast to their appropriate key type interface.

Parameters:

`keyType` - the type of key to be generated. Valid codes listed in TYPE.. constants.
`keyLength` - the key size in bits. The valid key bit lengths are key type dependent. See above.
`keyEncryption` - if `true` this boolean requests a key implementation which implements the `javacardx.cipher.KeyEncryption` interface.

Returns:

the key object instance of the requested key type, length and encrypted access.

Throws:

CryptoException - with the following reason codes:

- `CryptoException.NO_SUCH_ALGORITHM` if the requested algorithm associated with the specified type, size of key and key encryption interface is not supported.

---

javacard.security
Class MessageDigest

```
java.lang.Object
  |
  +--javacard.security.MessageDigest
```

public abstract class **MessageDigest**
extends Object

The `MessageDigest` class is the base class for hashing algorthims. Implementations of MessageDigest algorithms must extend this class and implement all the abstract methods.

Field Summary

static byte	**ALG_MD5** Message Digest algorithm MD5.
static byte	**ALG_RIPEMD160** Message Digest algorithm RIPE MD-160.
static byte	**ALG_SHA** Message Digest algorithm SHA.

Constructor Summary

protected	**MessageDigest**() Protected Constructor

Method Summary	
abstract short	**doFinal**(byte[] inBuff, short inOffset, short inLength, byte[] outBuff, short outOffset) Generates a hash of all/last input data.
abstract byte	**getAlgorithm**() Gets the Message digest algorithm.
static MessageDigest	**getInstance**(byte algorithm, boolean externalAccess) Creates a MessageDigest object instance of the selected algorithm.
abstract byte	**getLength**() Returns the byte length of the hash.
abstract void	**update**(byte[] inBuff, short inOffset, short inLength) Accumulates a hash of the input data.

Methods inherited from class java.lang.Object
equals

Field Detail

ALG_SHA

```
public static final byte ALG_SHA
```

Message Digest algorithm SHA.

ALG_MD5

```
public static final byte ALG_MD5
```

Message Digest algorithm MD5.

ALG_RIPEMD160

```
public static final byte ALG_RIPEMD160
```

Message Digest algorithm RIPE MD-160.

Constructor Detail

MessageDigest

```
protected MessageDigest()
```

Protected Constructor

Method Detail

getInstance

```
public static final MessageDigest getInstance(byte algorithm,
                                               boolean externalAccess)
                                        throws CryptoException
```

Creates a `MessageDigest` object instance of the selected algorithm.

Parameters:

`algorithm` - the desired message digest algorithm. Valid codes listed in ALG_.. constants. See above.

`externalAccess` - if `true` indicates that the instance will be shared among multiple applet instances and that the `MessageDigest` instance will also be accessed (via a `Shareable` interface) when the owner of the `MessageDigest` instance is not the currently selected applet.

Returns:

the `MessageDigest` object instance of the requested algorithm.

Throws:

CryptoException - with the following reason codes:

- `CryptoException.NO_SUCH_ALGORITHM` if the requested algorithm is not supported.

---

getAlgorithm

```
public abstract byte getAlgorithm()
```

Gets the Message digest algorithm.

Returns:

the algorithm code defined above.

---

getLength

```
public abstract byte getLength()
```

Returns the byte length of the hash.

Returns:

hash length

---

doFinal

```
public abstract short doFinal(byte[] inBuff,
                              short inOffset,
                              short inLength,
                              byte[] outBuff,
                              short outOffset)
```

Generates a hash of all/last input data. Completes and returns the hash computation after performing final operations such as padding. The `MessageDigest` object is reset after this call is made.

The input and output buffer data may overlap.

Parameters:

`inBuff` - the input buffer of data to be hashed
`inOffset` - the offset into the input buffer at which to begin hash generation
`inLength` - the byte length to hash
`outBuff` - the output buffer, may be the same as the input buffer
`outOffset` - the offset into the output buffer where the resulting hash value begins

Returns:

number of bytes of hash output in `outBuff`

---

update

```
public abstract void update(byte[] inBuff,
                            short inOffset,
                            short inLength)
```

Accumulates a hash of the input data. When this method is used temporary storage of intermediate results is required. This method should only be used if all the input data required for the hash is not available in one byte array. The doFinal() method is recommended whenever possible.

Parameters:

`inBuff` - the input buffer of data to be hashed
`inOffset` - the offset into the input buffer at which to begin hash generation
`inLength` - the byte length to hash

See Also:

`doFinal(byte[], short, short, byte[], short)`

javacard.security
Interface PrivateKey

All Known Subinterfaces:
DSAPrivateKey, RSAPrivateCrtKey, RSAPrivateKey

public abstract interface **PrivateKey**
extends Key

The `PrivateKey` class is the base class for private keys used in asymmetric algorithms.

Methods inherited from interface javacard.security.Key
`clearKey, getSize, getType, isInitialized`

javacard.security
Interface PublicKey

All Known Subinterfaces:
DSAPublicKey, RSAPublicKey

public abstract interface **PublicKey**
extends Key

The `PublicKey` class is the base class for public keys used in asymmetric algorithms.

Methods inherited from interface javacard.security.Key
`clearKey, getSize, getType, isInitialized`

javacard.security
Interface RSAPrivateCrtKey

public abstract interface **RSAPrivateCrtKey**
extends PrivateKey

The `RSAPrivateCrtKey` interface is used to sign data using the RSA algorithm in its Chinese Remainder Theorem form. It may also be used by the `javacardx.crypto.Cipher` class to encrypt/decrypt messages.

Let $S = m^d \bmod n$, where m is the data to be signed, d is the private key exponent, and n is private key modulus composed of two prime numbers p and q. The following names are used in the initializer methods in this interface:

P, the prime factor p
Q, the prime factor q.
PQ = $q^{-1} \bmod p$
DP1 = $d \bmod (p - 1)$
DQ1 = $d \bmod (q - 1)$

When all five components (P,Q,PQ,DP1,DQ1) of the key are set, the key is initialized and ready for use.

See Also:
`RSAPrivateKey`, `RSAPublicKey`, `KeyBuilder`, `Signature`, `Cipher`, `KeyEncryption`

Method Summary

short	**getDP1**(byte[] buffer, short offset) Returns the value of the DP1 parameter in plain text.
short	**getDQ1**(byte[] buffer, short offset) Returns the value of the DQ1 parameter in plain text.
short	**getP**(byte[] buffer, short offset) Returns the value of the P parameter in plain text.
short	**getPQ**(byte[] buffer, short offset) Returns the value of the PQ parameter in plain text.
short	**getQ**(byte[] buffer, short offset) Returns the value of the Q parameter in plain text.
void	**setDP1**(byte[] buffer, short offset, short length) Sets the value of the DP1 parameter.
void	**setDQ1**(byte[] buffer, short offset, short length) Sets the value of the DQ1 parameter.
void	**setP**(byte[] buffer, short offset, short length) Sets the value of the P parameter.
void	**setPQ**(byte[] buffer, short offset, short length) Sets the value of the PQ parameter.
void	**setQ**(byte[] buffer, short offset, short length) Sets the value of the Q parameter.

Methods inherited from interface javacard.security.Key

clearKey, getSize, getType, isInitialized

Method Detail

setP

```
public void setP(byte[] buffer,
                 short offset,
                 short length)
          throws CryptoException
```

Sets the value of the P parameter. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input P parameter data is copied into the internal representation.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer at which the parameter value begins
`length` - the length of the parameter

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input parameter data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the P parameter value is decrypted using the* `Cipher` *object.*

---

setQ

```
public void setQ(byte[] buffer,
                 short offset,
                 short length)
          throws CryptoException
```

Sets the value of the Q parameter. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input Q parameter data is copied into the internal representation.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer at which the parameter value begins
`length` - the length of the parameter

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input parameter data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the Q parameter value is decrypted using the* `Cipher` *object.*

---

setDP1

```
public void setDP1(byte[] buffer,
                   short offset,
                   short length)
            throws CryptoException
```

Sets the value of the DP1 parameter. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input DP1 parameter data is copied into the internal representation.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer at which the parameter value begins
`length` - the length of the parameter

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input parameter data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the DP1 parameter value is decrypted using the* `Cipher` *object.*

---

setDQ1

```
public void setDQ1(byte[] buffer,
                   short offset,
                   short length)
            throws CryptoException
```

Sets the value of the DQ1 parameter. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input DQ1 parameter data is copied into the internal representation.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer at which the parameter value begins
`length` - the length of the parameter

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input parameter data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the DQ1 parameter value is decrypted using the* `Cipher` *object.*

setPQ

```
public void setPQ(byte[] buffer,
                  short offset,
                  short length)
           throws CryptoException
```

Sets the value of the PQ parameter. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input PQ parameter data is copied into the internal representation.

Parameters:

`buffer` - the input buffer

`offset` - the offset into the input buffer at which the parameter value begins

`length` - the length of the parameter

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input parameter data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the PQ parameter value is decrypted using the* `Cipher` *object.*

---

getP

```
public short getP(byte[] buffer,
                  short offset)
```

Returns the value of the P parameter in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer

`offset` - the offset into the output buffer at which the parameter value begins

Returns:

the byte length of the P parameter value returned

---

getQ

```
public short getQ(byte[] buffer,
                  short offset)
```

Returns the value of the Q parameter in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:
`buffer` - the output buffer
`offset` - the offset into the output buffer at which the parameter value begins
Returns:
the byte length of the Q parameter value returned

---

getDP1

```
public short getDP1(byte[] buffer,
                    short offset)
```

Returns the value of the DP1 parameter in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).
Parameters:
`buffer` - the output buffer
`offset` - the offset into the output buffer at which the parameter value begins
Returns:
the byte length of the DP1 parameter value returned

---

getDQ1

```
public short getDQ1(byte[] buffer,
                    short offset)
```

Returns the value of the DQ1 parameter in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).
Parameters:
`buffer` - the output buffer
`offset` - the offset into the output buffer at which the parameter value begins
Returns:
the byte length of the DQ1 parameter value returned

---

getPQ

```
public short getPQ(byte[] buffer,
                   short offset)
```

Returns the value of the PQ parameter in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).
Parameters:
`buffer` - the output buffer
`offset` - the offset into the output buffer at which the parameter value begins
Returns:
the byte length of the PQ parameter value returned

javacard.security
Interface RSAPrivateKey

public abstract interface **RSAPrivateKey**
extends PrivateKey

The `RSAPrivateKey` class is used to sign data using the RSA algorithm in its modulus/exponent form. It may also be used by the `javacardx.crypto.Cipher` class to encrypt/decrypt messages.

When both the modulus and exponent of the key are set, the key is initialized and ready for use.

See Also:
`RSAPublicKey`, `RSAPrivateCrtKey`, `KeyBuilder`, `Signature`, `Cipher`, `KeyEncryption`

Method Summary

`short`	**`getExponent`**`(byte[] buffer, short offset)` Returns the private exponent value of the key in plain text.
`short`	**`getModulus`**`(byte[] buffer, short offset)` Returns the modulus value of the key in plain text.
`void`	**`setExponent`**`(byte[] buffer, short offset, short length)` Sets the private exponent value of the key.
`void`	**`setModulus`**`(byte[] buffer, short offset, short length)` Sets the modulus value of the key.

Methods inherited from interface javacard.security.Key
`clearKey, getSize, getType, isInitialized`

Method Detail

setModulus

```
public void setModulus(byte[] buffer,
                       short offset,
                       short length)
                throws CryptoException
```

Sets the modulus value of the key. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input modulus data is copied into the internal representation.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer at which the modulus value begins
`length` - the length of the modulus

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input modulus data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the modulus value is decrypted using the* `Cipher` *object.*

---

setExponent

```
public void setExponent(byte[] buffer,
                        short offset,
                        short length)
                 throws CryptoException
```

Sets the private exponent value of the key. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input exponent data is copied into the internal representation.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer at which the exponent value begins
`length` - the length of the exponent

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input exponent data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the exponent value is decrypted using the* `Cipher` *object.*

getModulus

```
public short getModulus(byte[] buffer,
                        short offset)
```

Returns the modulus value of the key in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer

`offset` - the offset into the output buffer at which the modulus value starts

Returns:

the byte length of the modulus value returned

getExponent

```
public short getExponent(byte[] buffer,
                         short offset)
```

Returns the private exponent value of the key in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer

`offset` - the offset into the output buffer at which the exponent value begins

Returns:

the byte length of the private exponent value returned

javacard.security
Interface RSAPublicKey

public abstract interface **RSAPublicKey**
extends PublicKey

The `RSAPublicKey` is used to verify signatures on signed data using the RSA algorithm. It may also used by the `javacardx.crypto.Cipher` class to encrypt/decrypt messages.

When both the modulus and exponent of the key are set, the key is initialized and ready for use.

See Also:
`RSAPrivateKey`, `RSAPrivateCrtKey`, `KeyBuilder`, `Signature`, `Cipher`, `KeyEncryption`

Method Summary

`short`	**`getExponent`**`(byte[] buffer, short offset)` Returns the private exponent value of the key in plain text.
`short`	**`getModulus`**`(byte[] buffer, short offset)` Returns the modulus value of the key in plain text.
`void`	**`setExponent`**`(byte[] buffer, short offset, short length)` Sets the public exponent value of the key.
`void`	**`setModulus`**`(byte[] buffer, short offset, short length)` Sets the modulus value of the key.

Methods inherited from interface javacard.security.Key
`clearKey, getSize, getType, isInitialized`

Method Detail

setModulus

```
public void setModulus(byte[] buffer,
                       short offset,
                       short length)
                throws CryptoException
```

Sets the modulus value of the key. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input modulus data is copied into the internal representation.

Parameters:

`buffer` - the input buffer

`offset` - the offset into the input buffer at which the modulus value begins

`length` - the byte length of the modulus

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input modulus data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the modulus value is decrypted using the* `Cipher` *object.*

---

setExponent

```
public void setExponent(byte[] buffer,
                        short offset,
                        short length)
                 throws CryptoException
```

Sets the public exponent value of the key. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input exponent data is copied into the internal representation.

Parameters:

`buffer` - the input buffer

`offset` - the offset into the input buffer at which the exponent value begins

`length` - the byte length of the exponent

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input exponent data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the exponent value is decrypted using the* `Cipher` *object.*

getModulus

```
public short getModulus(byte[] buffer,
                        short offset)
```

Returns the modulus value of the key in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer

`offset` - the offset into the input buffer at which the modulus value starts

Returns:

the byte length of the modulus value returned

getExponent

```
public short getExponent(byte[] buffer,
                         short offset)
```

Returns the private exponent value of the key in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer

`offset` - the offset into the output buffer at which the exponent value begins

Returns:

the byte length of the public exponent returned

javacard.security
Class RandomData

```
java.lang.Object
  |
  +--javacard.security.RandomData
```

public abstract class **RandomData**
extends Object

The `RandomData` abstract class is the base class for random number generation. Implementations of RandomData algorithms must extend this class and implement all the abstract methods.

Field Summary

static byte	**ALG_PSEUDO_RANDOM** Utility pseudo random number generation algorithms.
static byte	**ALG_SECURE_RANDOM** Cryptographically secure random number generation algorithms.

Constructor Summary

protected	**RandomData**() Protected constructor for subclassing.

Method Summary

abstract void	**generateData**(byte[] buffer, short offset, short length) Generates random data.
static RandomData	**getInstance**(byte algorithm) Creates a `RandomData` instance of the selected algorithm.
abstract void	**setSeed**(byte[] buffer, short offset, short length) Seeds the random data generator.

Methods inherited from class java.lang.Object
equals

Field Detail

ALG_PSEUDO_RANDOM

```
public static final byte ALG_PSEUDO_RANDOM
```

Utility pseudo random number generation algorithms.

ALG_SECURE_RANDOM

```
public static final byte ALG_SECURE_RANDOM
```

Cryptographically secure random number generation algorithms.

Constructor Detail

RandomData

```
protected RandomData()
```

Protected constructor for subclassing.

Method Detail

getInstance

```
public static final RandomData getInstance(byte algorithm)
                                    throws CryptoException
```

Creates a `RandomData` instance of the selected algorithm. The pseudo random `RandomData` instance's seed is initialized to a internal default value.

Parameters:

`algorithm` - the desired random number algorithm. Valid codes listed in ALG_.. constants. See above.

Returns:

the `RandomData` object instance of the requested algorithm.

Throws:

CryptoException - with the following reason codes:

- `CryptoException.NO_SUCH_ALGORITHM` if the requested algorithm is not supported.

---

generateData

```
public abstract void generateData(byte[] buffer,
                                  short offset,
                                  short length)
```

Generates random data.

Parameters:

`buffer` - the output buffer
`offset` - the offset into the output buffer
`length` - the length of random data to generate

---

setSeed

```
public abstract void setSeed(byte[] buffer,
                             short offset,
                             short length)
```

Seeds the random data generator.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer
`length` - the length of the seed data

---

javacard.security
Interface SecretKey

All Known Subinterfaces:
DESKey

public abstract interface **SecretKey**
extends Key

The `SecretKey` class is the base interface for keys used in symmetric alogrightms (e.g. DES).

Methods inherited from interface javacard.security.Key
`clearKey, getSize, getType, isInitialized`

javacard.security
Class Signature

```
java.lang.Object
  |
  +--javacard.security.Signature
```

public abstract class **Signature**
extends Object

The `Signature` class is the base class for Signature algorthims. Implementations of Signature algorithms must extend this class and implement all the abstract methods.

The term "pad" is used in the public key signature algorithms below to refer to all the operations specified in the referenced scheme to transform the message digest into the encryption block size.

Field Summary

`static byte`	**`ALG_DES_MAC4_ISO9797_M1`** Signature algorithm `ALG_DES_MAC4_ISO9797_M1` generates a 4 byte MAC (most significant 4 bytes of encrypted block) using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 1 scheme.
`static byte`	**`ALG_DES_MAC4_ISO9797_M2`** Signature algorithm `ALG_DES_MAC4_ISO9797_M2` generates a 4 byte MAC (most significant 4 bytes of encrypted block) using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 2 (ISO 7816-4, EMV'96) scheme.
`static byte`	**`ALG_DES_MAC4_NOPAD`** Signature algorithm `ALG_DES_MAC4_NOPAD` generates a 4 byte MAC (most significant 4 bytes of encrypted block) using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. This algorithm does not pad input data.
`static byte`	**`ALG_DES_MAC4_PKCS5`** Signature algorithm `ALG_DES_MAC4_PKCS5` generates a 4 byte MAC (most significant 4 bytes of encrypted block) using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the PKCS#5 scheme.
`static byte`	**`ALG_DES_MAC8_ISO9797_M1`** Signature algorithm `ALG_DES_MAC8_ISO9797_M1` generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 1 scheme.

static byte	**ALG_DES_MAC8_ISO9797_M2** Signature algorithm ALG_DES_MAC8_ISO9797_M2 generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 2 (ISO 7816-4, EMV'96) scheme.
static byte	**ALG_DES_MAC8_NOPAD** Signature algorithm ALG_DES_MAC_8_NOPAD generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. This algorithm does not pad input data.
static byte	**ALG_DES_MAC8_PKCS5** Signature algorithm ALG_DES_MAC8_PKCS5 generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the PKCS#5 scheme.
static byte	**ALG_DSA_SHA** Signature algorithm ALG_DSA_SHA signs/verifies the 20 byte SHA digest using DSA.
static byte	**ALG_RSA_MD5_PKCS1** Signature algorithm ALG_RSA_MD5_PKCS1 encrypts the 16 byte MD5 digest using RSA. The digest is padded according to the PKCS#1 (v1.5) scheme.
static byte	**ALG_RSA_MD5_RFC2409** Signature algorithm ALG_RSA_MD5_RFC2409 encrypts the 16 byte MD5 digest using RSA. The digest is padded according to the RFC2409 scheme.
static byte	**ALG_RSA_RIPEMD160_ISO9796** Signature algorithm ALG_RSA_RIPEMD160_ISO9796 encrypts the 20 byte RIPE MD-160 digest using RSA. The digest is padded according to the ISO 9796 scheme.
static byte	**ALG_RSA_RIPEMD160_PKCS1** Signature algorithm ALG_RSA_RIPEMD160_PKCS1 encrypts the 20 byte RIPE MD-160 digest using RSA. The digest is padded according to the PKCS#1 (v1.5) scheme.
static byte	**ALG_RSA_SHA_ISO9796** Signature algorithm ALG_RSA_SHA_ISO9796 encrypts the 20 byte SHA digest using RSA. The digest is padded according to the ISO 9796 (EMV'96) scheme.
static byte	**ALG_RSA_SHA_PKCS1** Signature algorithm ALG_RSA_SHA_PKCS1 encrypts the 20 byte SHA digest using RSA. The digest is padded according to the PKCS#1 (v1.5) scheme.
static byte	**ALG_RSA_SHA_RFC2409** Signature algorithm ALG_RSA_SHA_RFC2409 encrypts the 20 byte SHA digest using RSA. The digest is padded according to the RFC2409 scheme.
static byte	**MODE_SIGN** Used in init() methods to indicate signature sign mode.

static byte	**MODE_VERIFY** Used in `init()` methods to indicate signature verify mode.

Constructor Summary

protected	**Signature**() Protected Constructor

Method Summary

abstract byte	**getAlgorithm**() Gets the Signature algorithm.
static Signature	**getInstance**(byte algorithm, boolean externalAccess) Creates a `Signature` object instance of the selected algorithm.
abstract short	**getLength**() Returns the byte length of the signature data.
abstract void	**init**(Key theKey, byte theMode) Initializes the `Signature` object with the appropriate `Key`.
abstract void	**init**(Key theKey, byte theMode, byte[] bArray, short bOff, short bLen) Initializes the `Signature` object with the appropriate `Key` and algorithm specific parameters.
abstract short	**sign**(byte[] inBuff, short inOffset, short inLength, byte[] sigBuff, short sigOffset) Generates the signature of all/last input data.
abstract void	**update**(byte[] inBuff, short inOffset, short inLength) Accumulates a signature of the input data.
abstract boolean	**verify**(byte[] inBuff, short inOffset, short inLength, byte[] sigBuff, short sigOffset, short sigLength) Verifies the signature of all/last input data against the passed in signature.

Methods inherited from class java.lang.Object
equals

Field Detail

ALG_DES_MAC4_NOPAD

```
public static final byte ALG_DES_MAC4_NOPAD
```

Signature algorithm `ALG_DES_MAC4_NOPAD` generates a 4 byte MAC (most significant 4 bytes of encrypted block) using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. This algorithm does not pad input data. If the input data is not (8 byte) block aligned it throws `CryptoExeption` with the reason code `ILLEGAL_USE`.

ALG_DES_MAC8_NOPAD

```
public static final byte ALG_DES_MAC8_NOPAD
```

Signature algorithm `ALG_DES_MAC_8_NOPAD` generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. This algorithm does not pad input data. If the input data is not (8 byte) block aligned it throws `CryptoExeption` with the reason code `ILLEGAL_USE`.

Note:

- *This algorithm must not be implemented if export restrictions apply.*

ALG_DES_MAC4_ISO9797_M1

```
public static final byte ALG_DES_MAC4_ISO9797_M1
```

Signature algorithm `ALG_DES_MAC4_ISO9797_M1` generates a 4 byte MAC (most significant 4 bytes of encrypted block) using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 1 scheme.

ALG_DES_MAC8_ISO9797_M1

```
public static final byte ALG_DES_MAC8_ISO9797_M1
```

Signature algorithm `ALG_DES_MAC8_ISO9797_M1` generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 1 scheme.

Note:

- *This algorithm must not be implemented if export restrictions apply.*

ALG_DES_MAC4_ISO9797_M2

`public static final byte` **`ALG_DES_MAC4_ISO9797_M2`**

Signature algorithm `ALG_DES_MAC4_ISO9797_M2` generates a 4 byte MAC (most significant 4 bytes of encrypted block) using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 2 (ISO 7816-4, EMV'96) scheme.

ALG_DES_MAC8_ISO9797_M2

`public static final byte` **`ALG_DES_MAC8_ISO9797_M2`**

Signature algorithm `ALG_DES_MAC8_ISO9797_M2` generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 2 (ISO 7816-4, EMV'96) scheme.

Note:

- *This algorithm must not be implemented if export restrictions apply.*

ALG_DES_MAC4_PKCS5

`public static final byte` **`ALG_DES_MAC4_PKCS5`**

Signature algorithm `ALG_DES_MAC4_PKCS5` generates a 4 byte MAC (most significant 4 bytes of encrypted block) using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the PKCS#5 scheme.

ALG_DES_MAC8_PKCS5

`public static final byte` **`ALG_DES_MAC8_PKCS5`**

Signature algorithm ALG_DES_MAC8_PKCS5 generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the PKCS#5 scheme.

Note:

- *This algorithm must not be implemented if export restrictions apply.*

ALG_RSA_SHA_ISO9796

```
public static final byte ALG_RSA_SHA_ISO9796
```

Signature algorithm ALG_RSA_SHA_ISO9796 encrypts the 20 byte SHA digest using RSA. The digest is padded according to the ISO 9796 (EMV'96) scheme.

ALG_RSA_SHA_PKCS1

```
public static final byte ALG_RSA_SHA_PKCS1
```

Signature algorithm ALG_RSA_SHA_PKCS1 encrypts the 20 byte SHA digest using RSA. The digest is padded according to the PKCS#1 (v1.5) scheme.

ALG_RSA_MD5_PKCS1

```
public static final byte ALG_RSA_MD5_PKCS1
```

Signature algorithm ALG_RSA_MD5_PKCS1 encrypts the 16 byte MD5 digest using RSA. The digest is padded according to the PKCS#1 (v1.5) scheme.

ALG_RSA_RIPEMD160_ISO9796

```
public static final byte ALG_RSA_RIPEMD160_ISO9796
```

Signature algorithm ALG_RSA_RIPEMD160_ISO9796 encrypts the 20 byte RIPE MD-160 digest using RSA. The digest is padded according to the ISO 9796 scheme.

ALG_RSA_RIPEMD160_PKCS1

```
public static final byte ALG_RSA_RIPEMD160_PKCS1
```

Signature algorithm ALG_RSA_RIPEMD160_PKCS1 encrypts the 20 byte RIPE MD-160 digest using RSA. The digest is padded according to the PKCS#1 (v1.5) scheme.

ALG_DSA_SHA

```
public static final byte ALG_DSA_SHA
```

Signature algorithm ALG_DSA_SHA signs/verifies the 20 byte SHA digest using DSA.

ALG_RSA_SHA_RFC2409

```
public static final byte ALG_RSA_SHA_RFC2409
```

Signature algorithm `ALG_RSA_SHA_RFC2409` encrypts the 20 byte SHA digest using RSA. The digest is padded according to the RFC2409 scheme.

ALG_RSA_MD5_RFC2409

```
public static final byte ALG_RSA_MD5_RFC2409
```

Signature algorithm `ALG_RSA_MD5_RFC2409` encrypts the 16 byte MD5 digest using RSA. The digest is padded according to the RFC2409 scheme.

MODE_SIGN

```
public static final byte MODE_SIGN
```

Used in `init()` methods to indicate signature sign mode.

MODE_VERIFY

```
public static final byte MODE_VERIFY
```

Used in `init()` methods to indicate signature verify mode.

Constructor Detail

Signature

```
protected Signature()
```

Protected Constructor

Method Detail

getInstance

```
public static final Signature getInstance(byte algorithm,
                                          boolean externalAccess)
                                   throws CryptoException
```

Creates a `Signature` object instance of the selected algorithm.

Parameters:

`algorithm` - the desired Signature algorithm. See above.

`externalAccess` - if `true` indicates that the instance will be shared among multiple applet instances and that the `Signature` instance will also be accessed (via a `Shareable` interface) when the owner of the `Signature` instance is not the currently selected applet.

Returns:

the `Signature` object instance of the requested algorithm.

Throws:

CryptoException - with the following reason codes:

- `CryptoException.NO_SUCH_ALGORITHM` if the requested algorithm is not supported.

---

init

```
public abstract void init(Key theKey,
                          byte theMode)
                   throws CryptoException
```

Initializes the `Signature` object with the appropriate `Key`. This method should be used for algorithms which do not need initialization parameters or use default parameter values.

Note:

- *DES and triple DES algorithms in CBC mode will use 0 for initial vector(IV) if this method is used.*

Parameters:

`theKey` - the key object to use for signing or verifying

`theMode` - one of `MODE_SIGN` or `MODE_VERIFY`

Throws:

CryptoException - with the following reason codes:

- `CryptoException.ILLEGAL_VALUE` if `theMode` option is an undefined value or if the `Key` is inconsistent with `theMode` or with the `Signature` implementation.

---

init

```
public abstract void init(Key theKey,
                          byte theMode,
                          byte[] bArray,
                          short bOff,
                          short bLen)
                   throws CryptoException
```

Initializes the `Signature` object with the appropriate `Key` and algorithm specific parameters.

Note:

- *DES and triple DES algorithms in outer CBC mode expect an 8 byte parameter value for the initial vector(IV) in* `bArray`.

- *RSA and DSA algorithms throw* `CryptoException.ILLEGAL_VALUE`.

Parameters:

`theKey` - the key object to use for signing
`theMode` - one of `MODE_SIGN` or `MODE_VERIFY`
`bArray` - byte array containing algorithm specific initialization info.
`bOff` - offset withing `bArray` where the algorithm specific data begins.
`bLen` - byte length of algorithm specific parameter data

Throws:

CryptoException - with the following reason codes:

- `CryptoException.ILLEGAL_VALUE` if `theMode` option is an undefined value or if a byte array parameter option is not supported by the algorithm or if the `bLen` is an incorrect byte length for the algorithm specific data or if the `Key` is inconsistent with `theMode` or with the `Signature` implementation.

---

getAlgorithm

```
public abstract byte getAlgorithm()
```

Gets the Signature algorithm.

Returns:

the algorithm code defined above.

---

getLength

```
public abstract short getLength()
```

Returns the byte length of the signature data.

Returns:

the byte length of the signature data.

---

update

```
public abstract void update(byte[] inBuff,
                            short inOffset,
                            short inLength)
                     throws CryptoException
```

Accumulates a signature of the input data. When this method is used temporary storage of intermediate results is required. This method should only be used if all the input data required for the signature is not available in one byte array. The `sign()` or `verify()` method is recommended whenever possible.

Parameters:

`inBuff` - the input buffer of data to be signed
`inOffset` - the offset into the input buffer at which to begin signature generation
`inLength` - the byte length to sign

Throws:

CryptoException - with the following reason codes:

- `CryptoException.UNINITIALIZED_KEY` if key not initialized.

See Also:

`sign(byte[], short, short, byte[], short)`, `verify(byte[], short, short, byte[], short, short)`

---

sign

```
public abstract short sign(byte[] inBuff,
                           short inOffset,
                           short inLength,
                           byte[] sigBuff,
                           short sigOffset)
                    throws CryptoException
```

Generates the signature of all/last input data. A call to this method also resets this `Signature` object to the state it was in when previously initialized via a call to `init()`. That is, the object is reset and available to sign another message.

The input and output buffer data may overlap.

Parameters:

`inBuff` - the input buffer of data to be signed
`inOffset` - the offset into the input buffer at which to begin signature generation
`inLength` - the byte length to sign
`sigBuff` - the output buffer to store signature data
`sigOffset` - the offset into sigBuff at which to begin signature data

Returns:

number of bytes of signature output in sigBuff

Throws:

CryptoException - with the following reason codes:

- `CryptoException.UNINITIALIZED_KEY` if key not initialized.
- `CryptoException.INVALID_INIT` if this `Signature` object is not initialized or initialized for signature verify mode.
- `CryptoException.ILLEGAL_USE` if this `Signature` algorithm does not pad the message and the message is not block aligned.

---

verify

```
public abstract boolean verify(byte[] inBuff,
                               short inOffset,
                               short inLength,
                               byte[] sigBuff,
                               short sigOffset,
                               short sigLength)
                        throws CryptoException
```

Verifies the signature of all/last input data against the passed in signature. A call to this method also resets this `Signature` object to the state it was in when previously initialized via a call to `init()`. That is, the object is reset and available to verify another message.

Parameters:

`inBuff` - the input buffer of data to be verified
`inOffset` - the offset into the input buffer at which to begin signature generation
`inLength` - the byte length to sign
`sigBuff` - the input buffer containing signature data
`sigOffset` - the offset into sigBuff where signature data begins.
`sigLength` - the byte length of the signature data

Returns:

`true` if signature verifies `false` otherwise.

Throws:

CryptoException - with the following reason codes:

- `CryptoException.UNINITIALIZED_KEY` if key not initialized.
- `CryptoException.INVALID_INIT` if this `Signature` object is not initialized or initialized for signature sign mode.
- `CryptoException.ILLEGAL_USE` if this `Signature` algorithm does not pad the message and the message is not block aligned.

Package javacardx.crypto

Extension package containing security classes and interfaces for export-controlled functionality.

See:

Description

Interface Summary	
KeyEncryption	`KeyEncryption` interface defines the methods used to enable encrypted key data access to a key implementation.

Class Summary	
Cipher	The `Cipher` class is the abstract base class for Cipher algorthims.

Package javacardx.crypto Description

Extension package containing security classes and interfaces for export-controlled functionality.

javacardx.crypto
Class Cipher

```
java.lang.Object
  |
  +--javacardx.crypto.Cipher
```

public abstract class **Cipher**
extends Object

The `Cipher` class is the abstract base class for Cipher algorthims. Implementations of Cipher algorithms must extend this class and implement all the abstract methods.

The term "pad" is used in the public key cipher algorithms below to refer to all the operations specified in the referenced scheme to transform the message block into the cipher block size.

Field Summary

`static byte`	**`ALG_DES_CBC_ISO9797_M1`** Cipher algorithm `ALG_DES_CBC_ISO9797_M1` provides a cipher using DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 1 scheme.
`static byte`	**`ALG_DES_CBC_ISO9797_M2`** Cipher algorithm `ALG_DES_CBC_ISO9797_M2` provides a cipher using DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 2 (ISO 7816-4, EMV'96) scheme.
`static byte`	**`ALG_DES_CBC_NOPAD`** Cipher algorithm `ALG_DES_CBC_NOPAD` provides a cipher using DES in CBC mode. This algorithm uses outer CBC for triple DES. This algorithm does not pad input data.
`static byte`	**`ALG_DES_CBC_PKCS5`** Cipher algorithm ALG_DES_CBC_PKCS5 provides a cipher using DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the PKCS#5 scheme.
`static byte`	**`ALG_DES_ECB_ISO9797_M1`** Cipher algorithm `ALG_DES_ECB_ISO9797_M1` provides a cipher using DES in ECB mode. Input data is padded according to the ISO 9797 method 1 scheme.
`static byte`	**`ALG_DES_ECB_ISO9797_M2`** Cipher algorithm `ALG_DES_ECB_ISO9797_M2` provides a cipher using DES in ECB mode. Input data is padded according to the ISO 9797 method 2 (ISO 7816-4, EMV'96) scheme.

static byte	**ALG_DES_ECB_NOPAD** Cipher algorithm ALG_DES_ECB_NOPAD provides a cipher using DES in ECB mode. This algorithm does not pad input data.
static byte	**ALG_DES_ECB_PKCS5** Cipher algorithm ALG_DES_ECB_PKCS5 provides a cipher using DES in ECB mode. Input data is padded according to the PKCS#5 scheme.
static byte	**ALG_RSA_ISO14888** Cipher algorithm ALG_RSA_ISO14888 provides a cipher using RSA. Input data is padded according to the ISO 14888 scheme.
static byte	**ALG_RSA_ISO9796** Cipher algorithm ALG_RSA_ISO9796 provides a cipher using RSA. Input data is padded according to the ISO 9796 (EMV'96) scheme.
static byte	**ALG_RSA_PKCS1** Cipher algorithm ALG_RSA_PKCS1 provides a cipher using RSA. Input data is padded according to the PKCS#1 (v1.5) scheme.
static byte	**MODE_DECRYPT** Used in init() methods to indicate decryption mode.
static byte	**MODE_ENCRYPT** Used in init() methods to indicate encryption mode.

Constructor Summary

protected	**Cipher**() Protected Constructor

Method Summary	
abstract short	**doFinal**(byte[] inBuff, short inOffset, short inLength, byte[] outBuff, short outOffset) Generates encrypted/decrypted output from all/last input data.
abstract byte	**getAlgorithm**() Gets the Cipher algorithm.
static Cipher	**getInstance**(byte algorithm, boolean externalAccess) Creates a Cipher object instance of the selected algorithm.
abstract void	**init**(Key theKey, byte theMode) Initializes the Cipher object with the appropriate Key.
abstract void	**init**(Key theKey, byte theMode, byte[] bArray, short bOff, short bLen) Initializes the Cipher object with the appropriate Key and algorithm specific parameters.
abstract short	**update**(byte[] inBuff, short inOffset, short inLength, byte[] outBuff, short outOffset) Generates encrypted/decrypted output from input data.

Methods inherited from class java.lang.Object
equals

Field Detail

ALG_DES_CBC_NOPAD

```
public static final byte ALG_DES_CBC_NOPAD
```

Cipher algorithm ALG_DES_CBC_NOPAD provides a cipher using DES in CBC mode. This algorithm uses outer CBC for triple DES. This algorithm does not pad input data. If the input data is not (8 byte) block aligned it throws CryptoExeption with the reason code ILLEGAL_USE.

ALG_DES_CBC_ISO9797_M1

```
public static final byte ALG_DES_CBC_ISO9797_M1
```

Cipher algorithm ALG_DES_CBC_ISO9797_M1 provides a cipher using DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 1 scheme.

ALG_DES_CBC_ISO9797_M2

```
public static final byte ALG_DES_CBC_ISO9797_M2
```

Cipher algorithm ALG_DES_CBC_ISO9797_M2 provides a cipher using DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 2 (ISO 7816-4, EMV'96) scheme.

ALG_DES_CBC_PKCS5

```
public static final byte ALG_DES_CBC_PKCS5
```

Cipher algorithm ALG_DES_CBC_PKCS5 provides a cipher using DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the PKCS#5 scheme.

ALG_DES_ECB_NOPAD

```
public static final byte ALG_DES_ECB_NOPAD
```

Cipher algorithm ALG_DES_ECB_NOPAD provides a cipher using DES in ECB mode. This algorithm does not pad input data. If the input data is not (8 byte) block aligned it throws CryptoExeption with the reason code ILLEGAL_USE.

ALG_DES_ECB_ISO9797_M1

```
public static final byte ALG_DES_ECB_ISO9797_M1
```

Cipher algorithm ALG_DES_ECB_ISO9797_M1 provides a cipher using DES in ECB mode. Input data is padded according to the ISO 9797 method 1 scheme.

ALG_DES_ECB_ISO9797_M2

```
public static final byte ALG_DES_ECB_ISO9797_M2
```

Cipher algorithm ALG_DES_ECB_ISO9797_M2 provides a cipher using DES in ECB mode. Input data is padded according to the ISO 9797 method 2 (ISO 7816-4, EMV'96) scheme.

ALG_DES_ECB_PKCS5

```
public static final byte ALG_DES_ECB_PKCS5
```

Cipher algorithm `ALG_DES_ECB_PKCS5` provides a cipher using DES in ECB mode. Input data is padded according to the PKCS#5 scheme.

ALG_RSA_ISO14888

```
public static final byte ALG_RSA_ISO14888
```

Cipher algorithm `ALG_RSA_ISO14888` provides a cipher using RSA. Input data is padded according to the ISO 14888 scheme.

ALG_RSA_PKCS1

```
public static final byte ALG_RSA_PKCS1
```

Cipher algorithm `ALG_RSA_PKCS1` provides a cipher using RSA. Input data is padded according to the PKCS#1 (v1.5) scheme.

Note:

- *This algorithm is only suitable for messages of limited length. The total number of input bytes processed may not be more than k-11, where k is the RSA key's modulus size in bytes.*

ALG_RSA_ISO9796

```
public static final byte ALG_RSA_ISO9796
```

Cipher algorithm `ALG_RSA_ISO9796` provides a cipher using RSA. Input data is padded according to the ISO 9796 (EMV'96) scheme.

Note:

- *This algorithm is only suitable for messages of limited length. The total number of input bytes processed may not be more than k/2, where k is the RSA key's modulus size in bytes.*

MODE_DECRYPT

```
public static final byte MODE_DECRYPT
```

Used in `init()` methods to indicate decryption mode.

MODE_ENCRYPT

```
public static final byte MODE_ENCRYPT
```

Used in `init()` methods to indicate encryption mode.

Constructor Detail

Cipher

```
protected Cipher()
```

Protected Constructor

Method Detail

getInstance

```
public static final Cipher getInstance(byte algorithm,
                                       boolean externalAccess)
                                throws CryptoException
```

Creates a `Cipher` object instance of the selected algorithm.

Parameters:

`algorithm` - the desired Cipher algorithm. See above.

`externalAccess` - if `true` indicates that the instance will be shared among multiple applet instances and that the `Cipher` instance will also be accessed (via a `Shareable` interface) when the owner of the `Cipher` instance is not the currently selected applet.

Returns:

the `Cipher` object instance of the requested algorithm.

Throws:

CryptoException - with the following reason codes:

- `CryptoException.NO_SUCH_ALGORITHM` if the requested algorithm is not supported.

---

init

```
public abstract void init(Key theKey,
                          byte theMode)
                   throws CryptoException
```

Initializes the `Cipher` object with the appropriate `Key`. This method should be used for algorithms which do not need initialization parameters or use default parameter values.

Note:

- *DES and triple DES algorithms in CBC mode will use 0 for initial vector(IV) if this method is used.*

Parameters:

`theKey` - the key object to use for signing or verifying
`theMode` - one of `MODE_DECRYPT` or `MODE_ENCRYPT`

Throws:

CryptoException - with the following reason codes:

- `CryptoException.ILLEGAL_VALUE` if `theMode` option is an undefined value or if the `Key` is inconsistent with the `Cipher` implementation.

---

init

```
public abstract void init(Key theKey,
                          byte theMode,
                          byte[] bArray,
                          short bOff,
                          short bLen)
                   throws CryptoException
```

Initializes the `Cipher` object with the appropriate Key and algorithm specific parameters.

Note:

- *DES and triple DES algorithms in outer CBC mode expect an 8 byte parameter value for the initial vector(IV) in* `bArray`.
- *RSA and DSA algorithms throw* `CryptoException.ILLEGAL_VALUE`.

Parameters:

`theKey` - the key object to use for signing
`theMode` - one of `MODE_DECRYPT` or `MODE_ENCRYPT`
`bArray` - byte array containing algorithm specific initialization info.
`bOff` - offset withing bArray where the algorithm specific data begins.
`bLen` - byte length of algorithm specific parameter data

Throws:

CryptoException - with the following reason codes:

- `CryptoException.ILLEGAL_VALUE` if `theMode` option is an undefined value or if a byte array parameter option is not supported by the algorithm or if the `bLen` is an incorrect byte length for the algorithm specific data or if the `Key` is inconsistent with the `Cipher` implementation.

---

getAlgorithm

```
public abstract byte getAlgorithm()
```

Gets the Cipher algorithm.

Returns:
the algorithm code defined above.

---

doFinal

```
public abstract short doFinal(byte[] inBuff,
                              short inOffset,
                              short inLength,
                              byte[] outBuff,
                              short outOffset)
                       throws CryptoException
```

Generates encrypted/decrypted output from all/last input data. A call to this method also resets this `Cipher` object to the state it was in when previously initialized via a call to `init()`. That is, the object is reset and available to encrypt or decrypt (depending on the operation mode that was specified in the call to `init()`) more data.

The input and output buffer data may overlap.

Notes:

- *On decryption operations (except when ISO 9797 method 1 padding is used), the padding bytes are not written to* `outBuff`.
- *On encryption operations, the number of bytes output into* `outBuff` *may be larger than* `inLength`.

Parameters:
`inBuff` - the input buffer of data to be encrypted/decrypted.
`inOffset` - the offset into the input buffer at which to begin encryption/decryption.
`inLength` - the byte length to be encrypted/decrypted.
`outBuff` - the output buffer, may be the same as the input buffer
`outOffset` - the offset into the output buffer where the resulting hash value begins

Returns:
number of bytes output in `outBuff`

Throws:
CryptoException - with the following reason codes:

- `CryptoException.UNINITIALIZED_KEY` if key not initialized.
- `CryptoException.INVALID_INIT` if this `Cipher` object is not initialized.
- `CryptoException.ILLEGAL_USE` if this `Cipher` algorithm does not pad the message and the message is not block aligned or if the input message length is not supported.

---

update

```
public abstract short update(byte[] inBuff,
                             short inOffset,
```

```
                short inLength,
                byte[] outBuff,
                short outOffset)
         throws CryptoException
```

Generates encrypted/decrypted output from input data. When this method is used temporary storage of intermediate results is required. This method should only be used if all the input data required for the cipher is not available in one byte array. The `doFinal()` method is recommended whenever possible.

The input and output buffer data may overlap.

Notes:

- *On decryption operations(except when ISO 9797 method 1 padding is used), the padding bytes are not written to* `outBuff`.
- *On encryption operations, the number of bytes output into* `outBuff` *may be larger than* `inLength`.
- *On encryption and decryption operations(except when ISO 9797 method 1 padding is used), block alignment considerations may require that the number of bytes output into* `outBuff` *be smaller than* `inLength` *or even 0.*

Parameters:

`inBuff` - the input buffer of data to be encrypted/decrypted.
`inOffset` - the offset into the input buffer at which to begin encryption/decryption.
`inLength` - the byte length to be encrypted/decrypted.
`outBuff` - the output buffer, may be the same as the input buffer
`outOffset` - the offset into the output buffer where the resulting hash value begins

Returns:

number of bytes output in `outBuff`

Throws:

CryptoException - with the following reason codes:

- `CryptoException.UNINITIALIZED_KEY` if key not initialized.
- `CryptoException.INVALID_INIT` if this `Cipher` object is not initialized.
- `CryptoException.ILLEGAL_USE` if the input message length is not supported.

---

javacardx.crypto
Interface KeyEncryption

public abstract interface **KeyEncryption**

`KeyEncryption` interface defines the methods used to enable encrypted key data access to a key implementation.

See Also:
`KeyBuilder`, `Cipher`

Method Summary

`Cipher`	**`getKeyCipher`**`()` Returns the `Cipher` object to be used to decrypt the input key data and key parameters in the set methods. Default is `null` - no decryption performed.
`void`	**`setKeyCipher`**`(Cipher keyCipher)` Sets the `Cipher` object to be used to decrypt the input key data and key parameters in the set methods. Default `Cipher` object is `null` - no decryption performed.

Method Detail

setKeyCipher

```
public void setKeyCipher(Cipher keyCipher)
```

Sets the `Cipher` object to be used to decrypt the input key data and key parameters in the set methods.

Default `Cipher` object is `null` - no decryption performed.

Parameters:

`keyCipher` - the decryption `Cipher` object to decrypt the input key data. `null` parameter indicates that no decryption is required.

getKeyCipher

```
public Cipher getKeyCipher()
```

Returns the `Cipher` object to be used to decrypt the input key data and key parameters in the set methods.

Default is `null` - no decryption performed.

Returns:

keyCipher the decryption `Cipher` object to decrypt the input key data. `null` return indicates that no decryption is performed.

A B C D E G I J K L M N O P R S T U V W

A

ALG_DES_MAC4_NOPAD - Static variable in class javacard.security.Signature
Signature algorithm `ALG_DES_MAC4_NOPAD` generates a 4 byte MAC (most significant 4 bytes of encrypted block) using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. This algorithm does not pad input data.

ALG_DES_MAC4_PKCS5 - Static variable in class javacard.security.Signature
Signature algorithm `ALG_DES_MAC4_PKCS5` generates a 4 byte MAC (most significant 4 bytes of encrypted block) using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the PKCS#5 scheme.

ALG_DES_MAC8_ISO9797_M1 - Static variable in class javacard.security.Signature
Signature algorithm `ALG_DES_MAC8_ISO9797_M1` generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 1 scheme.

ALG_DES_MAC8_ISO9797_M2 - Static variable in class javacard.security.Signature
Signature algorithm `ALG_DES_MAC8_ISO9797_M2` generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 2 (ISO 7816-4, EMV'96) scheme.

ALG_DES_MAC8_NOPAD - Static variable in class javacard.security.Signature
Signature algorithm `ALG_DES_MAC_8_NOPAD` generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. This algorithm does not pad input data.

ALG_DES_MAC8_PKCS5 - Static variable in class javacard.security.Signature
Signature algorithm ALG_DES_MAC8_PKCS5 generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the PKCS#5 scheme.

ALG_DSA_SHA - Static variable in class javacard.security.Signature
Signature algorithm `ALG_DSA_SHA` signs/verifies the 20 byte SHA digest using DSA.

ALG_MD5 - Static variable in class javacard.security.MessageDigest
Message Digest algorithm MD5.

ALG_PSEUDO_RANDOM - Static variable in class javacard.security.RandomData
Utility pseudo random number generation algorithms.

ALG_RIPEMD160 - Static variable in class javacard.security.MessageDigest
Message Digest algorithm RIPE MD-160.

ALG_RSA_ISO14888 - Static variable in class javacardx.crypto.Cipher
Cipher algorithm `ALG_RSA_ISO14888` provides a cipher using RSA. Input data is padded according to the ISO 14888 scheme.

ALG_RSA_ISO9796 - Static variable in class javacardx.crypto.Cipher
Cipher algorithm `ALG_RSA_ISO9796` provides a cipher using RSA. Input data is padded according to the ISO 9796 (EMV'96) scheme.

ALG_RSA_MD5_PKCS1 - Static variable in class javacard.security.Signature
Signature algorithm `ALG_RSA_MD5_PKCS1` encrypts the 16 byte MD5 digest using RSA. The digest is padded according to the PKCS#1 (v1.5) scheme.

ALG_RSA_MD5_RFC2409 - Static variable in class javacard.security.Signature
Signature algorithm `ALG_RSA_MD5_RFC2409` encrypts the 16 byte MD5 digest using RSA. The digest is padded according to the RFC2409 scheme.

ALG_RSA_PKCS1 - Static variable in class javacardx.crypto.Cipher
Cipher algorithm `ALG_RSA_PKCS1` provides a cipher using RSA. Input data is padded according to

the PKCS#1 (v1.5) scheme.

ALG_RSA_RIPEMD160_ISO9796 - Static variable in class javacard.security.Signature
Signature algorithm `ALG_RSA_RIPEMD160_ISO9796` encrypts the 20 byte RIPE MD-160 digest using RSA. The digest is padded according to the ISO 9796 scheme.

ALG_RSA_RIPEMD160_PKCS1 - Static variable in class javacard.security.Signature
Signature algorithm `ALG_RSA_RIPEMD160_PKCS1` encrypts the 20 byte RIPE MD-160 digest using RSA. The digest is padded according to the PKCS#1 (v1.5) scheme.

ALG_RSA_SHA_ISO9796 - Static variable in class javacard.security.Signature
Signature algorithm `ALG_RSA_SHA_ISO9796` encrypts the 20 byte SHA digest using RSA. The digest is padded according to the ISO 9796 (EMV'96) scheme.

ALG_RSA_SHA_PKCS1 - Static variable in class javacard.security.Signature
Signature algorithm `ALG_RSA_SHA_PKCS1` encrypts the 20 byte SHA digest using RSA. The digest is padded according to the PKCS#1 (v1.5) scheme.

ALG_RSA_SHA_RFC2409 - Static variable in class javacard.security.Signature
Signature algorithm `ALG_RSA_SHA_RFC2409` encrypts the 20 byte SHA digest using RSA. The digest is padded according to the RFC2409 scheme.

ALG_SECURE_RANDOM - Static variable in class javacard.security.RandomData
Cryptographically secure random number generation algorithms.

ALG_SHA - Static variable in class javacard.security.MessageDigest
Message Digest algorithm SHA.

APDU - class javacard.framework.APDU.
Application Protocol Data Unit (APDU) is the communication format between the card and the off-card applications.

APDUException - exception javacard.framework.APDUException.
`APDUException` represents an `APDU` related exception.

APDUException(short) - Constructor for class javacard.framework.APDUException
Constructs an APDUException.

Applet - class javacard.framework.Applet.
This abstract class defines an applet in Java Card.

Applet() - Constructor for class javacard.framework.Applet
Only this class's `install()` method should create the applet object.

ArithmeticException - exception java.lang.ArithmeticException.
A JCRE owned instance of `ArithmethicException` is thrown when an exceptional arithmetic condition has occurred.

ArithmeticException() - Constructor for class java.lang.ArithmeticException
Constructs an `ArithmeticException`.

arrayCompare(byte[], short, byte[], short, short) - Static method in class javacard.framework.Util
Compares an array from the specified source array, beginning at the specified position, with the specified position of the destination array from left to right.

arrayCopy(byte[], short, byte[], short, short) - Static method in class javacard.framework.Util
Copies an array from the specified source array, beginning at the specified position, to the specified position of the destination array.

arrayCopyNonAtomic(byte[], short, byte[], short, short) - Static method in class javacard.framework.Util
Copies an array from the specified source array, beginning at the specified position, to the specified position of the destination array (non-atomically).

arrayFillNonAtomic(byte[], short, short, byte) - Static method in class javacard.framework.Util
Fills the byte array (non-atomically) beginning at the specified position, for the specified length with the specified byte value.

ArrayIndexOutOfBoundsException - exception java.lang.ArrayIndexOutOfBoundsException.
A JCRE owned instance of `IndexOutOfBoundsException` is thrown to indicate that an array has been accessed with an illegal index.

ArrayIndexOutOfBoundsException() - Constructor for class java.lang.ArrayIndexOutOfBoundsException
Constructs an `ArrayIndexOutOfBoundsException`.

ArrayStoreException - exception java.lang.ArrayStoreException.
A JCRE owned instance of `ArrayStoreException` is thrown to indicate that an attempt has been made to store the wrong type of object into an array of objects.

ArrayStoreException() - Constructor for class java.lang.ArrayStoreException
Constructs an `ArrayStoreException`.

B

BAD_LENGTH - Static variable in class javacard.framework.APDUException
This reason code is used by the `APDU.setOutgoingLength()` method to indicate that the length parameter is greater that 256 or if non BLOCK CHAINED data transfer is requested and `len` is greater than (IFSD-2), where IFSD is the Outgoing Block Size.

beginTransaction() - Static method in class javacard.framework.JCSystem
Begins an atomic transaction.

BUFFER_BOUNDS - Static variable in class javacard.framework.APDUException
This reason code is used by the `APDU.sendBytes()` method to indicate that the sum of buffer offset parameter and the byte length parameter exceeds the APDU buffer size.

BUFFER_FULL - Static variable in class javacard.framework.TransactionException
This reason code is used during a transaction to indicate that the commit buffer is full.

buildKey(byte, short, boolean) - Static method in class javacard.security.KeyBuilder
Creates cryptographic keys for signature and cipher algorithms.

C

CardException - exception javacard.framework.CardException.
The `CardException` class defines a field `reason` and two accessor methods `getReason()` and `setReason()`.

CardException(short) - Constructor for class javacard.framework.CardException
Construct a CardException instance with the specified reason.

CardRuntimeException - exception javacard.framework.CardRuntimeException.
The `CardRuntimeException` class defines a field `reason` and two accessor methods `getReason()` and `setReason()`.

CardRuntimeException(short) - Constructor for class javacard.framework.CardRuntimeException
Construct a CardRuntimeException instance with the specified reason.

check(byte[], short, byte) - Method in class javacard.framework.OwnerPIN
Compares `pin` against the PIN value.
check(byte[], short, byte) - Method in interface javacard.framework.PIN
Compares `pin` against the PIN value.
Cipher - class javacardx.crypto.Cipher.
The `Cipher` class is the abstract base class for Cipher algorthims.
Cipher() - Constructor for class javacardx.crypto.Cipher
Protected Constructor
CLA_ISO7816 - Static variable in interface javacard.framework.ISO7816
APDU command CLA : ISO 7816 = 0x00
ClassCastException - exception java.lang.ClassCastException.
A JCRE owned instance of `ClassCastException` is thrown to indicate that the code has attempted to cast an object to a subclass of which it is not an instance.
ClassCastException() - Constructor for class java.lang.ClassCastException
Constructs a `ClassCastException`.
CLEAR_ON_DESELECT - Static variable in class javacard.framework.JCSystem
This event code indicates that the contents of the transient object are cleared to the default value on applet deselection event or in `CLEAR_ON_RESET` cases.
CLEAR_ON_RESET - Static variable in class javacard.framework.JCSystem
This event code indicates that the contents of the transient object are cleared to the default value on card reset (or power on) event.
clearKey() - Method in interface javacard.security.Key
Clears the key and sets its initialized state to false.
commitTransaction() - Static method in class javacard.framework.JCSystem
Commits an atomic transaction.
CryptoException - exception javacard.security.CryptoException.
`CryptoException` represents a cryptography-related exception.
CryptoException(short) - Constructor for class javacard.security.CryptoException
Constructs a `CryptoException` with the specified reason.

D

deselect() - Method in class javacard.framework.Applet
Called by the JCRE to inform this currently selected applet that another (or the same) applet will be selected.
DESKey - interface javacard.security.DESKey.
`DESKey` contains an 8/16/24 byte key for single/2 key triple DES/3 key triple DES operations.
doFinal(byte[], short, short, byte[], short) - Method in class javacard.security.MessageDigest
Generates a hash of all/last input data.
doFinal(byte[], short, short, byte[], short) - Method in class javacardx.crypto.Cipher
Generates encrypted/decrypted output from all/last input data.
DSAKey - interface javacard.security.DSAKey.
The DSAKey interface is the base interface for the DSA algorithms private and public key implementaions.

E

G

getExponent(byte[], short) - Method in interface javacard.security.RSAPrivateKey
Returns the private exponent value of the key in plain text.
getExponent(byte[], short) - Method in interface javacard.security.RSAPublicKey
Returns the private exponent value of the key in plain text.
getG(byte[], short) - Method in interface javacard.security.DSAKey
Returns the subprime parameter value of the key in plain text.
getInBlockSize() - Static method in class javacard.framework.APDU
Returns the configured incoming block size. In T=1 protocol, this corresponds to IFSC (information field size for ICC), the maximum size of incoming data blocks into the card. In T=0 protocol, this method returns 1.
getInstance(byte) - Static method in class javacard.security.RandomData
Creates a `RandomData` instance of the selected algorithm.
getInstance(byte, boolean) - Static method in class javacard.security.MessageDigest
Creates a `MessageDigest` object instance of the selected algorithm.
getInstance(byte, boolean) - Static method in class javacard.security.Signature
Creates a `Signature` object instance of the selected algorithm.
getInstance(byte, boolean) - Static method in class javacardx.crypto.Cipher
Creates a `Cipher` object instance of the selected algorithm.
getKey(byte[], short) - Method in interface javacard.security.DESKey
Returns the `Key` data in plain text.
getKeyCipher() - Method in interface javacardx.crypto.KeyEncryption
Returns the `Cipher` object to be used to decrypt the input key data and key parameters in the set methods. Default is `null` - no decryption performed.
getLength() - Method in class javacard.security.MessageDigest
Returns the byte length of the hash.
getLength() - Method in class javacard.security.Signature
Returns the byte length of the signature data.
getMaxCommitCapacity() - Static method in class javacard.framework.JCSystem
Returns the total number of bytes in the commit buffer.
getModulus(byte[], short) - Method in interface javacard.security.RSAPrivateKey
Returns the modulus value of the key in plain text.
getModulus(byte[], short) - Method in interface javacard.security.RSAPublicKey
Returns the modulus value of the key in plain text.
getNAD() - Method in class javacard.framework.APDU
In T=1 protocol, this method returns the Node Address byte, NAD. In T=0 protocol, this method returns 0.
getOutBlockSize() - Static method in class javacard.framework.APDU
Returns the configured outgoing block size. In T=1 protocol, this corresponds to IFSD (information field size for interface device), the maximum size of outgoing data blocks to the CAD. In T=0 protocol, this method returns 258 (accounts for 2 status bytes).
getP(byte[], short) - Method in interface javacard.security.DSAKey
Returns the base parameter value of the key in plain text.
getP(byte[], short) - Method in interface javacard.security.RSAPrivateCrtKey
Returns the value of the P parameter in plain text.
getPQ(byte[], short) - Method in interface javacard.security.RSAPrivateCrtKey
Returns the value of the PQ parameter in plain text.

getPreviousContextAID() - Static method in class javacard.framework.JCSystem
This method is called to obtain the JCRE owned instance of the `AID` object associated with the previously active applet context.
getProtocol() - Static method in class javacard.framework.APDU
Returns the ISO 7816 transport protocol type, T=1 or T=0 in progress.
getQ(byte[], short) - Method in interface javacard.security.DSAKey
Returns the prime parameter value of the key in plain text.
getQ(byte[], short) - Method in interface javacard.security.RSAPrivateCrtKey
Returns the value of the Q parameter in plain text.
getReason() - Method in class javacard.framework.CardRuntimeException
Get reason code
getReason() - Method in class javacard.framework.CardException
Get reason code
getShareableInterfaceObject(AID, byte) - Method in class javacard.framework.Applet
Called by the JCRE to obtain a shareable interface object from this server applet, on behalf of a request from a client applet.
getShort(byte[], short) - Static method in class javacard.framework.Util
Concatenates two bytes in a byte array to form a short value.
getSize() - Method in interface javacard.security.Key
Returns the key size in number of bits.
getTransactionDepth() - Static method in class javacard.framework.JCSystem
Returns the current transaction nesting depth level.
getTriesRemaining() - Method in class javacard.framework.OwnerPIN
Returns the number of times remaining that an incorrect PIN can be presented before the `PIN` is blocked.
getTriesRemaining() - Method in interface javacard.framework.PIN
Returns the number of times remaining that an incorrect PIN can be presented before the `PIN` is blocked.
getType() - Method in interface javacard.security.Key
Returns the key interface type.
getUnusedCommitCapacity() - Static method in class javacard.framework.JCSystem
Returns the number of bytes left in the commit buffer.
getValidatedFlag() - Method in class javacard.framework.OwnerPIN
This protected method returns the validated flag.
getVersion() - Static method in class javacard.framework.JCSystem
Returns the current major and minor version of the Java Card API.
getX(byte[], short) - Method in interface javacard.security.DSAPrivateKey
Returns the value of the key in plain text.
getY(byte[], short) - Method in interface javacard.security.DSAPublicKey
Returns the value of the key in plain text.

I

ILLEGAL_AID - Static variable in class javacard.framework.SystemException
This reason code is used by the `javacard.framework.Applet.register()` method to indicate that the input AID parameter is not a legal AID value.

ILLEGAL_TRANSIENT - Static variable in class javacard.framework.SystemException
This reason code is used to indicate that the request to create a transient object is not allowed in the current applet context.

ILLEGAL_USE - Static variable in class javacard.framework.APDUException
This APDUException reason code indicates that the method should not be invoked based on the current state of the APDU.

ILLEGAL_USE - Static variable in class javacard.security.CryptoException
This reason code is used to indicate that the signature or cipher algorithm does not pad the incoming message and the input message is not block aligned.

ILLEGAL_VALUE - Static variable in class javacard.framework.PINException
This reason code is used to indicate that one or more input parameters is out of allowed bounds.

ILLEGAL_VALUE - Static variable in class javacard.framework.SystemException
This reason code is used to indicate that one or more input parameters is out of allowed bounds.

ILLEGAL_VALUE - Static variable in class javacard.security.CryptoException
This reason code is used to indicate that one or more input parameters is out of allowed bounds.

IN_PROGRESS - Static variable in class javacard.framework.TransactionException
This reason code is used by the `beginTransaction` method to indicate a transaction is already in progress.

IndexOutOfBoundsException - exception java.lang.IndexOutOfBoundsException.
A JCRE owned instance of `IndexOutOfBoundsException` is thrown to indicate that an index of some sort (such as to an array) is out of range.

IndexOutOfBoundsException() - Constructor for class java.lang.IndexOutOfBoundsException
Constructs an `IndexOutOfBoundsException`.

init(Key, byte) - Method in class javacard.security.Signature
Initializes the `Signature` object with the appropriate `Key`.

init(Key, byte) - Method in class javacardx.crypto.Cipher
Initializes the `Cipher` object with the appropriate `Key`.

init(Key, byte, byte[], short, short) - Method in class javacard.security.Signature
Initializes the `Signature` object with the appropriate `Key` and algorithm specific parameters.

init(Key, byte, byte[], short, short) - Method in class javacardx.crypto.Cipher
Initializes the `Cipher` object with the appropriate Key and algorithm specific parameters.

INS_EXTERNAL_AUTHENTICATE - Static variable in interface javacard.framework.ISO7816
APDU command INS : EXTERNAL AUTHENTICATE = 0x82

INS_SELECT - Static variable in interface javacard.framework.ISO7816
APDU command INS : SELECT = 0xA4

install(byte[], short, byte) - Static method in class javacard.framework.Applet
To create an instance of the `Applet` subclass, the JCRE will call this static method first.

INTERNAL_FAILURE - Static variable in class javacard.framework.TransactionException
This reason code is used during a transaction to indicate an internal JCRE problem (fatal error).

J

K

KeyEncryption - interface javacardx.crypto.KeyEncryption.
`KeyEncryption` interface defines the methods used to enable encrypted key data access to a key implementation.

L

LENGTH_DES - Static variable in class javacard.security.KeyBuilder
DES Key Length `LENGTH_DES` = 64.
LENGTH_DES3_2KEY - Static variable in class javacard.security.KeyBuilder
DES Key Length `LENGTH_DES3_2KEY` = 128.
LENGTH_DES3_3KEY - Static variable in class javacard.security.KeyBuilder
DES Key Length `LENGTH_DES3_3KEY` = 192.
LENGTH_DSA_1024 - Static variable in class javacard.security.KeyBuilder
DSA Key Length `LENGTH_DSA_1024` = 1024.
LENGTH_DSA_512 - Static variable in class javacard.security.KeyBuilder
DSA Key Length `LENGTH_DSA_512` = 512.
LENGTH_DSA_768 - Static variable in class javacard.security.KeyBuilder
DSA Key Length `LENGTH_DSA_768` = 768.
LENGTH_RSA_1024 - Static variable in class javacard.security.KeyBuilder
RSA Key Length `LENGTH_RSA_1024` = 1024.
LENGTH_RSA_2048 - Static variable in class javacard.security.KeyBuilder
RSA Key Length `LENGTH_RSA_2048` = 2048.
LENGTH_RSA_512 - Static variable in class javacard.security.KeyBuilder
RSA Key Length `LENGTH_RSA_512` = 512.
LENGTH_RSA_768 - Static variable in class javacard.security.KeyBuilder
RSA Key Length `LENGTH_RSA_768` = 768.
lookupAID(byte[], short, byte) - Static method in class javacard.framework.JCSystem
Returns the JCRE owned instance of the `AID` object, if any, encapsulating the specified AID bytes in the `buffer` parameter if there exists a successfully installed applet on the card whose instance AID exactly matches that of the specified AID bytes.

M

makeShort(byte, byte) - Static method in class javacard.framework.Util
Concatenates the two parameter bytes to form a short value.
makeTransientBooleanArray(short, byte) - Static method in class javacard.framework.JCSystem
Create a transient boolean array with the specified array length.
makeTransientByteArray(short, byte) - Static method in class javacard.framework.JCSystem
Create a transient byte array with the specified array length.
makeTransientObjectArray(short, byte) - Static method in class javacard.framework.JCSystem
Create a transient array of `Object` with the specified array length.
makeTransientShortArray(short, byte) - Static method in class javacard.framework.JCSystem
Create a transient short array with the specified array length.

MessageDigest - class javacard.security.MessageDigest.
The `MessageDigest` class is the base class for hashing algorthims.
MessageDigest() - Constructor for class javacard.security.MessageDigest
Protected Constructor
MODE_DECRYPT - Static variable in class javacardx.crypto.Cipher
Used in `init()` methods to indicate decryption mode.
MODE_ENCRYPT - Static variable in class javacardx.crypto.Cipher
Used in `init()` methods to indicate encryption mode.
MODE_SIGN - Static variable in class javacard.security.Signature
Used in `init()` methods to indicate signature sign mode.
MODE_VERIFY - Static variable in class javacard.security.Signature
Used in `init()` methods to indicate signature verify mode.

N

NegativeArraySizeException - exception java.lang.NegativeArraySizeException.
A JCRE owned instance of `NegativeArraySizeException` is thrown if an applet tries to create an array with negative size.
NegativeArraySizeException() - Constructor for class java.lang.NegativeArraySizeException
Constructs a `NegativeArraySizeException`.
NO_RESOURCE - Static variable in class javacard.framework.SystemException
This reason code is used to indicate that there is insufficient resource in the Card for the request.
NO_SUCH_ALGORITHM - Static variable in class javacard.security.CryptoException
This reason code is used to indicate that the requested algorithm or key type is not supported.
NO_T0_GETRESPONSE - Static variable in class javacard.framework.APDUException
This reason code indicates that during T=0 protocol, the CAD did not return a GET RESPONSE command in response to a <61xx> response status to send additional data.
NO_TRANSIENT_SPACE - Static variable in class javacard.framework.SystemException
This reason code is used by the `makeTransient..()` methods to indicate that no room is available in volatile memory for the requested object.
NOT_A_TRANSIENT_OBJECT - Static variable in class javacard.framework.JCSystem
This event code indicates that the object is not transient.
NOT_IN_PROGRESS - Static variable in class javacard.framework.TransactionException
This reason code is used by the `abortTransaction` and `commintTransaction` methods when a transaction is not in progress.
NullPointerException - exception java.lang.NullPointerException.
A JCRE owned instance of `NullPointerException`is thrown when an applet attempts to use `null` in a case where an object is required.
NullPointerException() - Constructor for class java.lang.NullPointerException
Constructs a `NullPointerException`.

O

Object - class java.lang.Object.
Class `Object` is the root of the Java Card class hierarchy.
Object() - Constructor for class java.lang.Object

OFFSET_CDATA - Static variable in interface javacard.framework.ISO7816
APDU command data offset : CDATA = 5
OFFSET_CLA - Static variable in interface javacard.framework.ISO7816
APDU header offset : CLA = 0
OFFSET_INS - Static variable in interface javacard.framework.ISO7816
APDU header offset : INS = 1
OFFSET_LC - Static variable in interface javacard.framework.ISO7816
APDU header offset : LC = 4
OFFSET_P1 - Static variable in interface javacard.framework.ISO7816
APDU header offset : P1 = 2
OFFSET_P2 - Static variable in interface javacard.framework.ISO7816
APDU header offset : P2 = 3
OwnerPIN - class javacard.framework.OwnerPIN.
This class represents an Owner PIN.
OwnerPIN(byte, byte) - Constructor for class javacard.framework.OwnerPIN
Constructor.

P

partialEquals(byte[], short, byte) - Method in class javacard.framework.AID
Checks if the specified partial AID byte sequence matches the first `length` bytes of the encapsulated AID bytes within `this AID` object.
PIN - interface javacard.framework.PIN.
This interface represents a PIN.
PINException - exception javacard.framework.PINException.
`PINException` represents a `OwnerPIN` class access-related exception.
PINException(short) - Constructor for class javacard.framework.PINException
Constructs a PINException.
PrivateKey - interface javacard.security.PrivateKey.
The `PrivateKey` class is the base class for private keys used in asymmetric algorithms.
process(APDU) - Method in class javacard.framework.Applet
Called by the JCRE to process an incoming APDU command.
PROTOCOL_T0 - Static variable in class javacard.framework.APDU
ISO 7816 transport protocol type T=0
PROTOCOL_T1 - Static variable in class javacard.framework.APDU
ISO 7816 transport protocol type T=1
PublicKey - interface javacard.security.PublicKey.
The `PublicKey` class is the base class for public keys used in asymmetric algorithms.

R

RandomData - class javacard.security.RandomData.
The `RandomData` abstract class is the base class for random number generation.

RandomData() - Constructor for class javacard.security.RandomData
Protected constructor for subclassing.

receiveBytes(short) - Method in class javacard.framework.APDU
Gets as many data bytes as will fit without APDU buffer overflow, at the specified offset `bOff`. Gets all the remaining bytes if they fit.

register() - Method in class javacard.framework.Applet
This method is used by the applet to register `this` applet instance with the JCRE and to assign the `Applet` subclass AID bytes as its instance AID bytes.

register(byte[], short, byte) - Method in class javacard.framework.Applet
This method is used by the applet to register `this` applet instance with the JCRE and assign the specified AID bytes as its instance AID bytes.

reset() - Method in class javacard.framework.OwnerPIN
If the validated flag is set, this method resets it.

reset() - Method in interface javacard.framework.PIN
If the validated flag is set, this method resets it.

resetAndUnblock() - Method in class javacard.framework.OwnerPIN
This method resets the validated flag and resets the `PIN` try counter to the value of the `PIN` try limit.

RIDEquals(AID) - Method in class javacard.framework.AID
Checks if the RID (National Registered Application provider identifier) portion of the encapsulated AID bytes within the `otherAID` object matches that of `this AID` object.

RSAPrivateCrtKey - interface javacard.security.RSAPrivateCrtKey.
The `RSAPrivateCrtKey` interface is used to sign data using the RSA algorithm in its Chinese Remainder Theorem form.

RSAPrivateKey - interface javacard.security.RSAPrivateKey.
The `RSAPrivateKey` class is used to sign data using the RSA algorithm in its modulus/exponent form.

RSAPublicKey - interface javacard.security.RSAPublicKey.
The `RSAPublicKey` is used to verify signatures on signed data using the RSA algorithm.

RuntimeException - exception java.lang.RuntimeException.
`RuntimeException` is the superclass of those exceptions that can be thrown during the normal operation of the Java Card Virtual Machine. A method is not required to declare in its throws clause any subclasses of `RuntimeException` that might be thrown during the execution of the method but not caught.

RuntimeException() - Constructor for class java.lang.RuntimeException
Constructs a `RuntimeException` instance.

S

SecretKey - interface javacard.security.SecretKey.
The `SecretKey` class is the base interface for keys used in symmetric alogrightms (e.g. DES).

SecurityException - exception java.lang.SecurityException.
A JCRE owned instance of `SecurityException` is thrown by the Java Card Virtual Machine to indicate a security violation. This exception is thrown when an attempt is made to illegally access an object belonging to a another applet.

SecurityException() - Constructor for class java.lang.SecurityException
Constructs a `SecurityException`.

select() - Method in class javacard.framework.Applet
Called by the JCRE to inform this applet that it has been selected.

selectingApplet() - Method in class javacard.framework.Applet
This method is used by the applet `process()` method to distinguish the SELECT APDU command which selected `this` applet, from all other other SELECT APDU commands which may relate to file or internal applet state selection.

sendBytes(short, short) - Method in class javacard.framework.APDU
Sends `len` more bytes from APDU buffer at specified offset `bOff`.

sendBytesLong(byte[], short, short) - Method in class javacard.framework.APDU
Sends `len` more bytes from `outData` byte array starting at specified offset `bOff`.

setDP1(byte[], short, short) - Method in interface javacard.security.RSAPrivateCrtKey
Sets the value of the DP1 parameter.

setDQ1(byte[], short, short) - Method in interface javacard.security.RSAPrivateCrtKey
Sets the value of the DQ1 parameter.

setExponent(byte[], short, short) - Method in interface javacard.security.RSAPrivateKey
Sets the private exponent value of the key.

setExponent(byte[], short, short) - Method in interface javacard.security.RSAPublicKey
Sets the public exponent value of the key.

setG(byte[], short, short) - Method in interface javacard.security.DSAKey
Sets the subprime parameter value of the key.

setIncomingAndReceive() - Method in class javacard.framework.APDU
This is the primary receive method.

setKey(byte[], short) - Method in interface javacard.security.DESKey
Sets the `Key` data.

setKeyCipher(Cipher) - Method in interface javacardx.crypto.KeyEncryption
Sets the `Cipher` object to be used to decrypt the input key data and key parameters in the set methods. Default `Cipher` object is `null` - no decryption performed.

setModulus(byte[], short, short) - Method in interface javacard.security.RSAPrivateKey
Sets the modulus value of the key.

setModulus(byte[], short, short) - Method in interface javacard.security.RSAPublicKey
Sets the modulus value of the key.

setOutgoing() - Method in class javacard.framework.APDU
This method is used to set the data transfer direction to outbound and to obtain the expected length of response (Le).

setOutgoingAndSend(short, short) - Method in class javacard.framework.APDU
This is the "convenience" send method.
setOutgoingLength(short) - Method in class javacard.framework.APDU
Sets the actual length of response data.
setOutgoingNoChaining() - Method in class javacard.framework.APDU
This method is used to set the data transfer direction to outbound without using BLOCK CHAINING(See ISO 7816-3/4) and to obtain the expected length of response (Le).
setP(byte[], short, short) - Method in interface javacard.security.DSAKey
Sets the base parameter value of the key.
setP(byte[], short, short) - Method in interface javacard.security.RSAPrivateCrtKey
Sets the value of the P parameter.
setPQ(byte[], short, short) - Method in interface javacard.security.RSAPrivateCrtKey
Sets the value of the PQ parameter.
setQ(byte[], short, short) - Method in interface javacard.security.DSAKey
Sets the prime parameter value of the key.
setQ(byte[], short, short) - Method in interface javacard.security.RSAPrivateCrtKey
Sets the value of the Q parameter.
setReason(short) - Method in class javacard.framework.CardRuntimeException
Set reason code
setReason(short) - Method in class javacard.framework.CardException
Set reason code
setSeed(byte[], short, short) - Method in class javacard.security.RandomData
Seeds the random data generator.
setShort(byte[], short, short) - Static method in class javacard.framework.Util
Deposits the short value as two successive bytes at the specified offset in the byte array.
setValidatedFlag(boolean) - Method in class javacard.framework.OwnerPIN
This protected method sets the value of the validated flag.
setX(byte[], short, short) - Method in interface javacard.security.DSAPrivateKey
Sets the value of the key.
setY(byte[], short, short) - Method in interface javacard.security.DSAPublicKey
Sets the value of the key.
Shareable - interface javacard.framework.Shareable.
The Shareable interface serves to identify all shared objects.
sign(byte[], short, short, byte[], short) - Method in class javacard.security.Signature
Generates the signature of all/last input data.
Signature - class javacard.security.Signature.
The `Signature` class is the base class for Signature algorthims.
Signature() - Constructor for class javacard.security.Signature
Protected Constructor
SW_APPLET_SELECT_FAILED - Static variable in interface javacard.framework.ISO7816
Response status : Applet selection failed = 0x6999;
SW_BYTES_REMAINING_00 - Static variable in interface javacard.framework.ISO7816
Response status : Response bytes remaining = 0x6100
SW_CLA_NOT_SUPPORTED - Static variable in interface javacard.framework.ISO7816
Response status : CLA value not supported = 0x6E00

SW_COMMAND_NOT_ALLOWED - Static variable in interface javacard.framework.ISO7816
Response status : Command not allowed (no current EF) = 0x6986
SW_CONDITIONS_NOT_SATISFIED - Static variable in interface javacard.framework.ISO7816
Response status : Conditions of use not satisfied = 0x6985
SW_CORRECT_LENGTH_00 - Static variable in interface javacard.framework.ISO7816
Response status : Correct Expected Length (Le) = 0x6C00
SW_DATA_INVALID - Static variable in interface javacard.framework.ISO7816
Response status : Data invalid = 0x6984
SW_FILE_FULL - Static variable in interface javacard.framework.ISO7816
Response status : Not enough memory space in the file = 0x6A84
SW_FILE_INVALID - Static variable in interface javacard.framework.ISO7816
Response status : File invalid = 0x6983
SW_FILE_NOT_FOUND - Static variable in interface javacard.framework.ISO7816
Response status : File not found = 0x6A82
SW_FUNC_NOT_SUPPORTED - Static variable in interface javacard.framework.ISO7816
Response status : Function not supported = 0x6A81
SW_INCORRECT_P1P2 - Static variable in interface javacard.framework.ISO7816
Response status : Incorrect parameters (P1,P2) = 0x6A86
SW_INS_NOT_SUPPORTED - Static variable in interface javacard.framework.ISO7816
Response status : INS value not supported = 0x6D00
SW_NO_ERROR - Static variable in interface javacard.framework.ISO7816
Response status : No Error = (short)0x9000
SW_RECORD_NOT_FOUND - Static variable in interface javacard.framework.ISO7816
Response status : Record not found = 0x6A83
SW_SECURITY_STATUS_NOT_SATISFIED - Static variable in interface javacard.framework.ISO7816
Response status : Security condition not satisfied = 0x6982
SW_UNKNOWN - Static variable in interface javacard.framework.ISO7816
Response status : No precise diagnosis = 0x6F00
SW_WRONG_DATA - Static variable in interface javacard.framework.ISO7816
Response status : Wrong data = 0x6A80
SW_WRONG_LENGTH - Static variable in interface javacard.framework.ISO7816
Response status : Wrong length = 0x6700
SW_WRONG_P1P2 - Static variable in interface javacard.framework.ISO7816
Response status : Incorrect parameters (P1,P2) = 0x6B00
SystemException - exception javacard.framework.SystemException.
`SystemException` represents a `JCSystem` class related exception.
SystemException(short) - Constructor for class javacard.framework.SystemException
Constructs a SystemException.

T

T1_IFD_ABORT - Static variable in class javacard.framework.APDUException
This reason code indicates that during T=1 protocol, the CAD returned an ABORT S-Block command and aborted the data transfer.

Throwable - class java.lang.Throwable.
The Throwable class is the superclass of all errors and exceptions in the Java Card subset of the Java language.

Throwable() - Constructor for class java.lang.Throwable
Constructs a new `Throwable`.

throwIt(short) - Static method in class javacard.framework.CardRuntimeException
Throw the JCRE owned instance of the `CardRuntimeException` class with the specified reason.

throwIt(short) - Static method in class javacard.framework.PINException
Throws the JCRE owned instance of `PINException` with the specified reason.

throwIt(short) - Static method in class javacard.framework.ISOException
Throws the JCRE owned instance of the ISOException class with the specified status word.

throwIt(short) - Static method in class javacard.framework.CardException
Throw the JCRE owned instance of `CardException` class with the specified reason.

throwIt(short) - Static method in class javacard.framework.UserException
Throws the JCRE owned instance of `UserException` with the specified reason.

throwIt(short) - Static method in class javacard.framework.SystemException
Throws the JCRE owned instance of `SystemException` with the specified reason.

throwIt(short) - Static method in class javacard.framework.TransactionException
Throws the JCRE owned instance of `TransactionException` with the specified reason.

throwIt(short) - Static method in class javacard.framework.APDUException
Throws the JCRE owned instance of `APDUException` with the specified reason.

throwIt(short) - Static method in class javacard.security.CryptoException
Throws the JCRE owned instance of `CryptoException` with the specified reason.

TransactionException - exception javacard.framework.TransactionException.
`TransactionException` represents an exception in the transaction subsystem.

TransactionException(short) - Constructor for class javacard.framework.TransactionException
Constructs a TransactionException with the specified reason.

TYPE_DES - Static variable in class javacard.security.KeyBuilder
`Key` object which implements interface type `DESKey` with persistent key data.

TYPE_DES_TRANSIENT_DESELECT - Static variable in class javacard.security.KeyBuilder
`Key` object which implements interface type `DESKey` with CLEAR_ON_DESELECT transient key data.

TYPE_DES_TRANSIENT_RESET - Static variable in class javacard.security.KeyBuilder
`Key` object which implements interface type `DESKey` with CLEAR_ON_RESET transient key data.

TYPE_DSA_PRIVATE - Static variable in class javacard.security.KeyBuilder
`Key` object which implements the interface type `DSAPrivateKey` for the DSA algorithm.

TYPE_DSA_PUBLIC - Static variable in class javacard.security.KeyBuilder
`Key` object which implements the interface type `DSAPublicKey` for the DSA algorithm.

TYPE_RSA_CRT_PRIVATE - Static variable in class javacard.security.KeyBuilder
`Key` object which implements interface type `RSAPrivateCrtKey` which uses Chinese Remainder Theorem.

TYPE_RSA_PRIVATE - Static variable in class javacard.security.KeyBuilder
`Key` object which implements interface type `RSAPrivateKey` which uses modulus/exponent form.

TYPE_RSA_PUBLIC - Static variable in class javacard.security.KeyBuilder
`Key` object which implements interface type `RSAPublicKey`.

U

V

W

A B C D E G I J K L M N O P R S T U V W

Java Card 2.1 Application Programming Interface

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303 USA
650 960-1300

Final Revision 1.0, February 24, 1999

Appendix JCAPI02

Java Card API

Table of Contents

Java Card™ 2.1 Platform API Specification

Final Revision 1.0

This document is the specification for the Java Card 2.1 Application Programming Interface.

See:

Description

Packages	
java.lang	Provides classes that are fundamental to the design of the Java Card technology subset of the Java programming language.
javacard.framework	Provides framework of classes and interfaces for the core functionality of a Java Card applet.
javacard.security	Provides the classes and interfaces for the Java Card security framework.
javacardx.crypto	Extension package containing security classes and interfaces for export-controlled functionality.

This document is the specification for the Java Card 2.1 Application Programming Interface.

Java Card 2.1 API Notes

Referenced Standards

ISO - International Standards Organization

- Information Technology - Identification cards - integrated circuit cards with contacts: ISO 7816
- Information Technology - Security Techniques - Digital Signature Scheme Giving Message Recovery: ISO 9796
- Information Technology - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm: ISO 9797
- Information technology - Security techniques - Digital signatures with appendix : ISO 14888

RSA Data Security, Inc.

- RSA Encryption Standard: PKCS #1 Version 2.0
- Password-Based Encryption Standard: PKCS #5 Version 1.5

EMV

- The EMV ’96 ICC Specifications for Payments systems Version 3.0

IPSec

- The Internet Key Exchange (IKE) document RFC 2409 (STD 1)

Standard Names for Security and Crypto

- SHA (also SHA-1): Secure Hash Algorithm, as defined in Secure Hash Standard, NIST FIPS 180-1.
- MD5: The Message Digest algorithm RSA-MD5, as defined by RSA DSI in RFC 1321.
- RIPEMD-160 : as defined in ISO/IEC 10118-3:1998 Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions
- DSA: Digital Signature Algorithm, as defined in Digital Signature Standard, NIST FIPS 186.
- DES: The Data Encryption Standard, as defined by NIST in FIPS 46-1 and 46-2.
- RSA: The Rivest, Shamir and Adleman Asymmetric Cipher algorithm.

Parameter Checking

Policy

All Java Card API implementations must conform to the Java model of parameter checking. That is, the API code should not check for those parameter errors which the VM is expected to detect. These include all parameter errors, such as null pointers, index out of bounds, and so forth, that result in standard runtime exceptions. The runtime exceptions that are thrown by the Java Card VM are:

- ArithmeticException
- ArrayStoreException
- ClassCastException
- IllegalArgumentException
- IllegalStateException
- IndexOutOfBoundsException
- ArrayIndexOutOfBoundsException
- NegativeArraySizeException
- NullPointerException
- SecurityException

Exceptions to the Policy

In some cases, it may be necessary to explicitly check parameters. These exceptions to the policy are documented in the Java Card API specification. A Java Card API implementation must not perform parameter checking with the intent to avoid runtime exceptions, unless this is clearly specified by the Java Card API specification.

Note: If multiple erroneous input parameters exist, any one of several runtime exceptions will be thrown by the VM. Java programmers rely on this behavior, but they do not rely on getting a specific exception. It is not necessary (nor is it reasonable or practical) to document the precise error handling for all possible combinations of equivalence classes of erroneous inputs. The value of this behavior is that the logic error in the calling program is detected and exposed via the runtime exception mechanism, rather than being masked by a normal return.

Hierarchy For All Packages

Package Hierarchies:
java.lang, javacard.framework, javacard.security, javacardx.crypto

Class Hierarchy

- class java.lang.**Object**
  - class javacard.framework.**AID**
  - class javacard.framework.**APDU**
  - class javacard.framework.**Applet**
  - class javacardx.crypto.**Cipher**
  - class javacard.framework.**JCSystem**
  - class javacard.security.**KeyBuilder**
  - class javacard.security.**MessageDigest**
  - class javacard.framework.**OwnerPIN** (implements javacard.framework.PIN)
  - class javacard.security.**RandomData**
  - class javacard.security.**Signature**
  - class java.lang.**Throwable**
    - class java.lang.**Exception**
      - class javacard.framework.**CardException**
        - class javacard.framework.**UserException**
      - class java.lang.**RuntimeException**
        - class java.lang.**ArithmeticException**
        - class java.lang.**ArrayStoreException**
        - class javacard.framework.**CardRuntimeException**
          - class javacard.framework.**APDUException**
          - class javacard.security.**CryptoException**
          - class javacard.framework.**ISOException**
          - class javacard.framework.**PINException**
          - class javacard.framework.**SystemException**
          - class javacard.framework.**TransactionException**
        - class java.lang.**ClassCastException**
        - class java.lang.**IndexOutOfBoundsException**
          - class java.lang.**ArrayIndexOutOfBoundsException**
        - class java.lang.**NegativeArraySizeException**
        - class java.lang.**NullPointerException**
        - class java.lang.**SecurityException**
  - class javacard.framework.**Util**

Interface Hierarchy

- interface javacard.security.**DSAKey**
  - interface javacard.security.**DSAPrivateKey**(also extends javacard.security.PrivateKey)
  - interface javacard.security.**DSAPublicKey**(also extends javacard.security.PublicKey)
- interface javacard.framework.**ISO7816**
- interface javacard.security.**Key**
  - interface javacard.security.**PrivateKey**
    - interface javacard.security.**DSAPrivateKey**(also extends javacard.security.DSAKey)
    - interface javacard.security.**RSAPrivateCrtKey**
    - interface javacard.security.**RSAPrivateKey**
  - interface javacard.security.**PublicKey**
    - interface javacard.security.**DSAPublicKey**(also extends javacard.security.DSAKey)
    - interface javacard.security.**RSAPublicKey**
  - interface javacard.security.**SecretKey**
    - interface javacard.security.**DESKey**
- interface javacardx.crypto.**KeyEncryption**
- interface javacard.framework.**PIN**
- interface javacard.framework.**Shareable**

Package java.lang

Provides classes that are fundamental to the design of the Java Card technology subset of the Java programming language.

See:

Description

Class Summary	
Object	Class `Object` is the root of the Java Card class hierarchy.
Throwable	The Throwable class is the superclass of all errors and exceptions in the Java Card subset of the Java language.

Exception Summary	
ArithmeticException	A JCRE owned instance of `ArithmethicException` is thrown when an exceptional arithmetic condition has occurred.
ArrayIndexOutOfBoundsException	A JCRE owned instance of `IndexOutOfBoundsException` is thrown to indicate that an array has been accessed with an illegal index.
ArrayStoreException	A JCRE owned instance of `ArrayStoreException` is thrown to indicate that an attempt has been made to store the wrong type of object into an array of objects.
ClassCastException	A JCRE owned instance of `ClassCastException` is thrown to indicate that the code has attempted to cast an object to a subclass of which it is not an instance.
Exception	The class `Exception` and its subclasses are a form of `Throwable` that indicates conditions that a reasonable applet might want to catch.
IndexOutOfBoundsException	A JCRE owned instance of `IndexOutOfBoundsException` is thrown to indicate that an index of some sort (such as to an array) is out of range.
NegativeArraySizeException	A JCRE owned instance of `NegativeArraySizeException` is thrown if an applet tries to create an array with negative size.
NullPointerException	A JCRE owned instance of `NullPointerException`is thrown when an applet attempts to use `null` in a case where an object is required.
RuntimeException	`RuntimeException` is the superclass of those exceptions that can be thrown during the normal operation of the Java Card Virtual Machine. A method is not required to declare in its throws clause any subclasses of `RuntimeException` that might be thrown during the execution of the method but not caught.
SecurityException	A JCRE owned instance of `SecurityException` is thrown by the Java Card Virtual Machine to indicate a security violation. This exception is thrown when an attempt is made to illegally access an object belonging to a another applet.

Package java.lang Description

Provides classes that are fundamental to the design of the Java Card technology subset of the Java programming language.

---

java.lang
Class ArithmeticException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--java.lang.ArithmeticException
```

public class **ArithmeticException**
extends RuntimeException

A JCRE owned instance of `ArithmethicException` is thrown when an exceptional arithmetic condition has occurred. For example, a "divide by zero" is an exceptional arithmentic condition.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`ArithmeticException``()` Constructs an `ArithmeticException`.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

ArithmeticException

`public` **`ArithmeticException`**`()`

Constructs an `ArithmeticException`.

---

java.lang
Class ArrayIndexOutOfBoundsException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--java.lang.IndexOutOfBoundsException
                          |
                          +--java.lang.ArrayIndexOutOfBoundsException
```

public class **ArrayIndexOutOfBoundsException**
extends IndexOutOfBoundsException

A JCRE owned instance of `IndexOutOfBoundsException` is thrown to indicate that an array has been accessed with an illegal index. The index is either negative or greater than or equal to the size of the array.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`ArrayIndexOutOfBoundsException``()` Constructs an `ArrayIndexOutOfBoundsException`.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

ArrayIndexOutOfBoundsException

`public` **`ArrayIndexOutOfBoundsException`**`()`

Constructs an `ArrayIndexOutOfBoundsException`.

---

java.lang
Class ArrayStoreException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--java.lang.ArrayStoreException
```

public class **ArrayStoreException**
extends RuntimeException

A JCRE owned instance of `ArrayStoreException` is thrown to indicate that an attempt has been made to store the wrong type of object into an array of objects. For example, the following code generates an `ArrayStoreException`:

```
Object x[] = new AID[3];
x[0] = new OwnerPIN( (byte) 3, (byte) 8);
```

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`ArrayStoreException``()` Constructs an `ArrayStoreException`.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

ArrayStoreException

`public` **`ArrayStoreException`**`()`

Constructs an `ArrayStoreException`.

---

java.lang
Class ClassCastException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--java.lang.ClassCastException
```

public class **ClassCastException**
extends RuntimeException

A JCRE owned instance of `ClassCastException` is thrown to indicate that the code has attempted to cast an object to a subclass of which it is not an instance. For example, the following code generates a `ClassCastException`:

```
Object x = new OwnerPIN( (byte)3, (byte)8);
JCSystem.getAppletShareableInterfaceObject( (AID)x, (byte)5 );
```

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`ClassCastException``()` Constructs a `ClassCastException`.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

ClassCastException

`public` **`ClassCastException`**`()`

Constructs a `ClassCastException`.

---

java.lang
Class Exception

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
```

Direct Known Subclasses:
CardException, RuntimeException

public class **Exception**
extends Throwable

The class `Exception` and its subclasses are a form of `Throwable` that indicates conditions that a reasonable applet might want to catch.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`Exception``()` Constructs an `Exception` instance.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

Exception

`public` **`Exception`**`()`

Constructs an `Exception` instance.

java.lang
Class IndexOutOfBoundsException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--java.lang.IndexOutOfBoundsException
```

Direct Known Subclasses:
ArrayIndexOutOfBoundsException

---

public class **IndexOutOfBoundsException**
extends RuntimeException

A JCRE owned instance of `IndexOutOfBoundsException` is thrown to indicate that an index of some sort (such as to an array) is out of range.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`IndexOutOfBoundsException``()` Constructs an `IndexOutOfBoundsException`.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

IndexOutOfBoundsException

`public` **`IndexOutOfBoundsException`**`()`

Constructs an `IndexOutOfBoundsException`.

---

java.lang
Class NegativeArraySizeException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--java.lang.NegativeArraySizeException
```

public class **NegativeArraySizeException**
extends RuntimeException

A JCRE owned instance of `NegativeArraySizeException` is thrown if an applet tries to create an array with negative size.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`NegativeArraySizeException``()` Constructs a `NegativeArraySizeException`.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

NegativeArraySizeException

```
public NegativeArraySizeException()
```

Constructs a `NegativeArraySizeException`.

---

java.lang
Class NullPointerException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--java.lang.NullPointerException
```

public class **NullPointerException**
extends RuntimeException

A JCRE owned instance of `NullPointerException`is thrown when an applet attempts to use `null` in a case where an object is required. These include:

- Calling the instance method of a `null` object.
- Accessing or modifying the field of a `null` object.
- Taking the length of `null` as if it were an array.
- Accessing or modifying the slots of `null` as if it were an array.
- Throwing `null` as if it were a `Throwable` value.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`NullPointerException``()` Constructs a `NullPointerException`.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

NullPointerException

```
public NullPointerException()
```

Constructs a `NullPointerException`.

---

java.lang
Class Object

java.lang.Object

public class **Object**

Class `Object` is the root of the Java Card class hierarchy. Every class has `Object` as a superclass. All objects, including arrays, implement the methods of this class.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

Object()	

Method Summary

boolean	**equals**(Object obj) Compares two Objects for equality.

Constructor Detail

Object

public **Object**()

Method Detail

equals

public boolean **equals**(Object obj)

Compares two Objects for equality.

The `equals` method implements an equivalence relation:

- It is *reflexive*: for any reference value `x`, `x.equals(x)` should return `true`.
- It is *symmetric*: for any reference values `x` and `y`, `x.equals(y)` should return `true` if and only if `y.equals(x)` returns `true`.
- It is *transitive*: for any reference values `x`, `y`, and `z`, if `x.equals(y)` returns `true` and `y.equals(z)` returns `true`, then `x.equals(z)` should return `true`.
- It is *consistent*: for any reference values `x` and `y`, multiple invocations of `x.equals(y)` consistently return `true` or consistently return `false`.
- For any reference value `x`, `x.equals(null)` should return `false`.

The equals method for class `Object` implements the most discriminating possible equivalence relation on objects; that is, for any reference values `x` and `y`, this method returns `true` if and only if `x` and `y` refer to the same object (`x==y` has the value `true`).

Parameters:

`obj` - the reference object with which to compare.

Returns:

`true` if this object is the same as the obj argument; `false` otherwise.

---

java.lang
Class RuntimeException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
```

Direct Known Subclasses:
ArithmeticException, ArrayStoreException, CardRuntimeException, ClassCastException, IndexOutOfBoundsException, NegativeArraySizeException, NullPointerException, SecurityException

---

public class **RuntimeException**
extends Exception

`RuntimeException` is the superclass of those exceptions that can be thrown during the normal operation of the Java Card Virtual Machine.

A method is not required to declare in its throws clause any subclasses of `RuntimeException` that might be thrown during the execution of the method but not caught.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`RuntimeException``()` Constructs a `RuntimeException` instance.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

RuntimeException

`public` **`RuntimeException`**`()`

Constructs a `RuntimeException` instance.

---

java.lang
Class SecurityException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--java.lang.SecurityException
```

public class **SecurityException**
extends RuntimeException

A JCRE owned instance of `SecurityException` is thrown by the Java Card Virtual Machine to indicate a security violation.

This exception is thrown when an attempt is made to illegally access an object belonging to a another applet. It may optionally be thrown by a Java Card VM implementation to indicate fundamental language restrictions, such as attempting to invoke a private method in another class.

For security reasons, the JCRE implementation may mute the card instead of throwing this exception.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`SecurityException``()` Constructs a `SecurityException`.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

SecurityException

```
public SecurityException()
```

Constructs a `SecurityException`.

java.lang
Class Throwable

```
java.lang.Object
  |
  +--java.lang.Throwable
```

Direct Known Subclasses:
Exception

public class **Throwable**
extends Object

The Throwable class is the superclass of all errors and exceptions in the Java Card subset of the Java language. Only objects that are instances of this class (or of one of its subclasses) are thrown by the Java Card Virtual Machine or can be thrown by the Java `throw` statement. Similarly, only this class or one of its subclasses can be the argument type in a `catch` clause.

This Java Card class's functionality is a strict subset of the definition in the *Java Platform Core API Specification*.

Constructor Summary

`Throwable``()` Constructs a new `Throwable`.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

Throwable

```
public Throwable()
```

Constructs a new `Throwable`.

Package javacard.framework

Provides framework of classes and interfaces for the core functionality of a Java Card applet.

See:

Description

Interface Summary	
ISO7816	`ISO7816` encapsulates constants related to ISO 7816-3 and ISO 7816-4.
PIN	This interface represents a PIN.
Shareable	The Shareable interface serves to identify all shared objects.

Class Summary	
AID	This class encapsulates the Application Identifier(AID) associated with an applet.
APDU	Application Protocol Data Unit (APDU) is the communication format between the card and the off-card applications.
Applet	This abstract class defines an applet in Java Card.
JCSystem	The `JCSystem` class includes a collection of methods to control applet execution, resource management, atomic transaction management and inter-applet object sharing in Java Card.
OwnerPIN	This class represents an Owner PIN.
Util	The `Util` class contains common utility functions.

Exception Summary	
APDUException	`APDUException` represents an `APDU` related exception.
CardException	The `CardException` class defines a field `reason` and two accessor methods `getReason()` and `setReason()`.
CardRuntimeException	The `CardRuntimeException` class defines a field `reason` and two accessor methods `getReason()` and `setReason()`.
ISOException	`ISOException` class encapsulates an ISO 7816-4 response status word as its `reason` code.
PINException	`PINException` represents a `OwnerPIN` class access-related exception.
SystemException	`SystemException` represents a `JCSystem` class related exception.
TransactionException	`TransactionException` represents an exception in the transaction subsystem.
UserException	`UserException` represents a User exception.

Package javacard.framework Description

Provides framework of classes and interfaces for the core functionality of a Java Card applet.

javacard.framework
Class AID

```
java.lang.Object
  |
  +--javacard.framework.AID
```

public final class **AID**
extends Object

This class encapsulates the Application Identifier(AID) associated with an applet. An AID is defined in ISO 7816-5 to be a sequence of bytes between 5 and 16 bytes in length.

The JCRE creates instances of `AID` class to identify and manage every applet on the card. Applets need not create instances of this class. An applet may request and use the JCRE owned instances to identify itself and other applet instances.

JCRE owned instances of `AID` are permanent JCRE Entry Point Objects and can be accessed from any applet context. References to these permanent objects can be stored and re-used.

An applet instance can obtain a reference to JCRE owned instances of its own `AID` object by using the `JCSystem.getAID()` method and another applet's `AID` object via the `JCSystem.lookupAID()` method.

An applet uses `AID` instances to request to share another applet's object or to control access to its own shared object from another applet. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

See Also:
`JCSystem`, `SystemException`

Constructor Summary

`AID``(byte[] bArray, short offset, byte length)` The JCRE uses this constructor to create a new `AID` instance encapsulating the specified AID bytes.

Method Summary	
boolean	**equals**(byte[] bArray, short offset, byte length) Checks if the specified AID bytes in bArray are the same as those encapsulated in this AID object.
boolean	**equals**(Object anObject) Compares the AID bytes in this AID instance to the AID bytes in the specified object.
byte	**getBytes**(byte[] dest, short offset) Called to get the AID bytes encapsulated within AID object.
boolean	**partialEquals**(byte[] bArray, short offset, byte length) Checks if the specified partial AID byte sequence matches the first length bytes of the encapsulated AID bytes within this AID object.
boolean	**RIDEquals**(AID otherAID) Checks if the RID (National Registered Application provider identifier) portion of the encapsulated AID bytes within the otherAID object matches that of this AID object.

Constructor Detail

AID

```
public AID(byte[] bArray,
           short offset,
           byte length)
    throws SystemException
```

The JCRE uses this constructor to create a new AID instance encapsulating the specified AID bytes.

Parameters:

bArray - the byte array containing the AID bytes.
offset - the start of AID bytes in bArray.
length - the length of the AID bytes in bArray.

Throws:

SystemException - with the following reason code:

- SystemException.ILLEGAL_VALUE if the length parameter is less than 5 or greater than 16.

Method Detail

getBytes

```
public byte getBytes(byte[] dest,
                     short offset)
```

Called to get the AID bytes encapsulated within `AID` object.

Parameters:

`dest` - byte array to copy the AID bytes.

`offset` - within dest where the AID bytes begin.

Returns:

the length of the AID bytes.

---

equals

```
public boolean equals(Object anObject)
```

Compares the AID bytes in `this AID` instance to the AID bytes in the specified object. The result is `true` if and only if the argument is not `null` and is an `AID` object that encapsulates the same AID bytes as `this` object.

This method does not throw `NullPointerException`.

Parameters:

`anObject` - the object to compare `this AID` against.

Returns:

`true` if the AID byte values are equal, `false` otherwise.

Overrides:

equals in class Object

---

equals

```
public boolean equals(byte[] bArray,
                      short offset,
                      byte length)
```

Checks if the specified AID bytes in `bArray` are the same as those encapsulated in `this AID` object. The result is `true` if and only if the `bArray` argument is not `null` and the AID bytes encapsulated in `this AID` object are equal to the specified AID bytes in `bArray`.

This method does not throw `NullPointerException`.

Parameters:

`bArray` - containing the AID bytes

`offset` - within bArray to begin

`length` - of AID bytes in bArray

Returns:

`true` if equal, `false` otherwise.

partialEquals

```
public boolean partialEquals(byte[] bArray,
                             short offset,
                             byte length)
```

Checks if the specified partial AID byte sequence matches the first `length` bytes of the encapsulated AID bytes within `this AID` object. The result is `true` if and only if the `bArray` argument is not `null` and the input `length` is less than or equal to the length of the encapsulated AID bytes within `this AID` object and the specified bytes match.

This method does not throw `NullPointerException`.

Parameters:

`bArray` - containing the partial AID byte sequence
`offset` - within bArray to begin
`length` - of partial AID bytes in bArray

Returns:

`true` if equal, `false` otherwise.

RIDEquals

```
public boolean RIDEquals(AID otherAID)
```

Checks if the RID (National Registered Application provider identifier) portion of the encapsulated AID bytes within the `otherAID` object matches that of `this AID` object. The first 5 bytes of an AID byte sequence is the RID. See ISO 7816-5 for details. The result is `true` if and only if the argument is not `null` and is an `AID` object that encapsulates the same RID bytes as `this` object.

This method does not throw `NullPointerException`.

Parameters:

`otherAID` - the `AID` to compare against.

Returns:

`true` if the RID bytes match, `false` otherwise.

javacard.framework
Class APDU

```
java.lang.Object
  |
  +--javacard.framework.APDU
```

public final class **APDU**
extends Object

Application Protocol Data Unit (APDU) is the communication format between the card and the off-card applications. The format of the APDU is defined in ISO specification 7816-4.

This class only supports messages which conform to the structure of command and response defined in ISO 7816-4. The behavior of messages which use proprietary structure of messages (for example with header CLA byte in range 0xD0-0xFE) is undefined. This class does not support extended length fields.

The APDU object is owned by the JCRE. The APDU class maintains a byte array buffer which is used to transfer incoming APDU header and data bytes as well as outgoing data. The buffer length must be at least 37 bytes (5 bytes of header and 32 bytes of data). The JCRE must zero out the APDU buffer before each new message received from the CAD.

The JCRE designates the APDU object as a temporary JCRE Entry Point Object (See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details). A temporary JCRE Entry Point Object can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components.

The JCRE similarly marks the APDU buffer as a global array (See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details). A global array can be accessed from any applet context. References to global arrays cannot be stored in class variables or instance variables or array components.

The applet receives the APDU instance to process from the JCRE in the `Applet.process(APDU)` method, and the first five bytes [CLA, INS, P1, P2, P3] are available in the APDU buffer.

The APDU class API is designed to be transport protocol independent. In other words, applets can use the same APDU methods regardless of whether the underlying protocol in use is T=0 or T=1 (as defined in ISO 7816-3).

The incoming APDU data size may be bigger than the APDU buffer size and may therefore need to be read in portions by the applet. Similarly, the outgoing response APDU data size may be bigger than the APDU buffer size and may need to be written in portions by the applet. The APDU class has methods to facilitate this.

For sending large byte arrays as response data, the APDU class provides a special method `sendBytesLong()` which manages the APDU buffer.

```
 // The purpose of this example is to show most of the methods
 // in use and not to depict any particular APDU processing

public void process(APDU apdu){
  // ...
  byte[] buffer = apdu.getBuffer();
  byte cla = buffer[ISO7816.OFFSET_CLA];
  byte ins = buffer[ISO7816.OFFSET_INS];
  ...
  // assume this command has incoming data
  // Lc tells us the incoming apdu command length
  short bytesLeft = (short) (buffer[ISO7816.OFFSET_LC] & 0x00FF);
  if (bytesLeft < (short)55) ISOException.throwIt( ISO7816.SW_WRONG_LENGTH );

  short readCount = apdu.setIncomingAndReceive();
  while ( bytesLeft > 0){
      // process bytes in buffer[5] to buffer[readCount+4];
      bytesLeft -= readCount;
      readCount = apdu.receiveBytes ( ISO7816.OFFSET_CDATA );
      }
  //
  //...
  //
  // Note that for a short response as in the case illustrated here
  // the three APDU method calls shown : setOutgoing(),setOutgoingLength() & sendBytes()
  // could be replaced by one APDU method call : setOutgoingAndSend().

  // construct the reply APDU
  short le = apdu.setOutgoing();
  if (le < (short)2) ISOException.throwIt( ISO7816.SW_WRONG_LENGTH );
  apdu.setOutgoingLength( (short)3 );

  // build response data in apdu.buffer[ 0.. outCount-1 ];
  buffer[0] = (byte)1; buffer[1] = (byte)2; buffer[3] = (byte)3;
  apdu.sendBytes ( (short)0 , (short)3 );
  // return good complete status 90 00
  }
```

See Also:

`APDUException`, `ISOException`

Field Summary

static byte	**PROTOCOL_T0** ISO 7816 transport protocol type T=0
static byte	**PROTOCOL_T1** ISO 7816 transport protocol type T=1

Method Summary

byte[]	**getBuffer**() Returns the APDU buffer byte array.
static short	**getInBlockSize**() Returns the configured incoming block size. In T=1 protocol, this corresponds to IFSC (information field size for ICC), the maximum size of incoming data blocks into the card. In T=0 protocol, this method returns 1.
byte	**getNAD**() In T=1 protocol, this method returns the Node Address byte, NAD. In T=0 protocol, this method returns 0.
static short	**getOutBlockSize**() Returns the configured outgoing block size. In T=1 protocol, this corresponds to IFSD (information field size for interface device), the maximum size of outgoing data blocks to the CAD. In T=0 protocol, this method returns 258 (accounts for 2 status bytes).
static byte	**getProtocol**() Returns the ISO 7816 transport protocol type, T=1 or T=0 in progress.
short	**receiveBytes**(short bOff) Gets as many data bytes as will fit without APDU buffer overflow, at the specified offset `bOff`. Gets all the remaining bytes if they fit.
void	**sendBytes**(short bOff, short len) Sends `len` more bytes from APDU buffer at specified offset `bOff`.
void	**sendBytesLong**(byte[] outData, short bOff, short len) Sends `len` more bytes from `outData` byte array starting at specified offset `bOff`.
short	**setIncomingAndReceive**() This is the primary receive method.
short	**setOutgoing**() This method is used to set the data transfer direction to outbound and to obtain the expected length of response (Le).
void	**setOutgoingAndSend**(short bOff, short len) This is the "convenience" send method.
void	**setOutgoingLength**(short len) Sets the actual length of response data.
short	**setOutgoingNoChaining**() This method is used to set the data transfer direction to outbound without using BLOCK CHAINING(See ISO 7816-3/4) and to obtain the expected length of response (Le).
void	**waitExtension**() Requests additional processsing time from CAD.

Methods inherited from class java.lang.Object
equals

Field Detail

PROTOCOL_T0

```
public static final byte PROTOCOL_T0
```

ISO 7816 transport protocol type T=0

PROTOCOL_T1

```
public static final byte PROTOCOL_T1
```

ISO 7816 transport protocol type T=1

Method Detail

getBuffer

```
public byte[] getBuffer()
```

Returns the APDU buffer byte array.

Notes:

- *References to the APDU buffer byte array cannot be stored in class variables or instance variables or array components. See* Java Card Runtime Environment (JCRE) 2.1 Specification *for details.*

Returns:

byte array containing the APDU buffer

---

getInBlockSize

```
public static short getInBlockSize()
```

Returns the configured incoming block size. In T=1 protocol, this corresponds to IFSC (information field size for ICC), the maximum size of incoming data blocks into the card. In T=0 protocol, this method returns 1. IFSC is defined in ISO 7816-3.

This information may be used to ensure that there is enough space remaining in the APDU buffer when `receiveBytes()` is invoked.

Notes:

- *On* `receiveBytes()` *the* `bOff` *param should account for this potential blocksize.*

Returns:

incoming block size setting.

See Also:

`receiveBytes(short)`

---

getOutBlockSize

```
public static short getOutBlockSize()
```

Returns the configured outgoing block size. In T=1 protocol, this corresponds to IFSD (information field size for interface device), the maximum size of outgoing data blocks to the CAD. In T=0 protocol, this method returns 258 (accounts for 2 status bytes). IFSD is defined in ISO 7816-3.

This information may be used prior to invoking the `setOutgoingLength()` method, to limit the length of outgoing messages when BLOCK CHAINING is not allowed.

Notes:

- *On* `setOutgoingLength()` *the* `len` *param should account for this potential blocksize.*

Returns:

outgoing block size setting.

See Also:

`setOutgoingLength(short)`

---

getProtocol

```
public static byte getProtocol()
```

Returns the ISO 7816 transport protocol type, T=1 or T=0 in progress.

Returns:

the protocol type in progress. One of `PROTOCOL_T0`, `PROTOCOL_T1` listed above.

---

getNAD

```
public byte getNAD()
```

In T=1 protocol, this method returns the Node Address byte, NAD. In T=0 protocol, this method returns 0. This may be used as additional information to maintain multiple contexts.

Returns:

NAD transport byte as defined in ISO 7816-3.

setOutgoing

```
public short setOutgoing()
                  throws APDUException
```

This method is used to set the data transfer direction to outbound and to obtain the expected length of response (Le).

Notes.

- *Any remaining incoming data will be discarded.*
- *In T=0 (Case 4) protocol, this method will return 256.*

Returns:

Le, the expected length of response.

Throws:

APDUException - with the following reason codes:

- `APDUException.ILLEGAL_USE` if this method or `setOutgoingNoChaining()` method already invoked.
- `APDUException.IO_ERROR` on I/O error.

setOutgoingNoChaining

```
public short setOutgoingNoChaining()
                           throws APDUException
```

This method is used to set the data transfer direction to outbound without using BLOCK CHAINING(See ISO 7816-3/4) and to obtain the expected length of response (Le). This method should be used in place of the `setOutgoing()` method by applets which need to be compatible with legacy CAD/terminals which do not support ISO 7816-3/4 defined block chaining. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Notes.

- *Any remaining incoming data will be discarded.*
- *In T=0 (Case 4) protocol, this method will return 256.*
- *When this method is used, the* `waitExtension()` *method cannot be used.*
- *In T=1 protocol, retransmission on error may be restricted.*
- *In T=0 protocol, the outbound transfer must be performed without using response status chaining.*
- *In T=1 protocol, the outbound transfer must not set the More(M) Bit in the PCB of the I block. See ISO 7816-3.*

Returns:

Le, the expected length of response data.

Throws:

APDUException - with the following reason codes:

- `APDUException.ILLEGAL_USE` if this method or `setOutgoing()` method already invoked.

- `APDUException.IO_ERROR` on I/O error.

---

setOutgoingLength

```
public void setOutgoingLength(short len)
                      throws APDUException
```

Sets the actual length of response data. Default is 0.

Note:

- *In T=0 (Case 2&4) protocol, the length is used by the JCRE to prompt the CAD for GET RESPONSE commands.*

Parameters:

`len` - the length of response data.

Throws:

APDUException - with the following reason codes:

- `APDUException.ILLEGAL_USE` if `setOutgoing()` not called or this method already invoked.
- `APDUException.BAD_LENGTH` if `len` is greater than 256 or if non BLOCK CHAINED data transfer is requested and `len` is greater than (IFSD-2), where IFSD is the Outgoing Block Size. The -2 accounts for the status bytes in T=1.
- `APDUException.IO_ERROR` on I/O error.

See Also:

`getOutBlockSize()`

---

receiveBytes

```
public short receiveBytes(short bOff)
                  throws APDUException
```

Gets as many data bytes as will fit without APDU buffer overflow, at the specified offset `bOff`. Gets all the remaining bytes if they fit.

Notes:

- *The space in the buffer must allow for incoming block size.*
- *In T=1 protocol, if all the remaining bytes do not fit in the buffer, this method may return less bytes than the maximum incoming block size (IFSC).*
- *In T=0 protocol, if all the remaining bytes do not fit in the buffer, this method may return less than a full buffer of bytes to optimize and reduce protocol overhead.*
- *In T=1 protocol, if this method throws an* `APDUException` *with* `T1_IFD_ABORT` *reason code, the JCRE will restart APDU command processing using the newly received command. No more input data can be received. No output data can be transmitted. No error status response can be returned.*

Parameters:

`bOff` - the offset into APDU buffer.

Returns:
number of bytes read. Returns 0 if no bytes are available.

Throws:
APDUException - with the following reason codes:

- `APDUException.ILLEGAL_USE` if `setIncomingAndReceive()` not called or if `setOutgoing()` or `setOutgoingNoChaining()` previously invoked.
- `APDUException.BUFFER_BOUNDS` if not enough buffer space for incoming block size.
- `APDUException.IO_ERROR` on I/O error.
- `APDUException.T1_IFD_ABORT` if T=1 protocol is in use and the CAD sends in an ABORT S-Block command to abort the data transfer.

See Also:
`getInBlockSize()`

---

setIncomingAndReceive

```
public short setIncomingAndReceive()
                          throws APDUException
```

This is the primary receive method. Calling this method indicates that this APDU has incoming data. This method gets as many bytes as will fit without buffer overflow in the APDU buffer following the header. It gets all the incoming bytes if they fit.

Notes:

- *In T=0 (Case 3&4) protocol, the P3 param is assumed to be Lc.*
- *Data is read into the buffer at offset 5.*
- *In T=1 protocol, if all the incoming bytes do not fit in the buffer, this method may return less bytes than the maximum incoming block size (IFSC).*
- *In T=0 protocol, if all the incoming bytes do not fit in the buffer, this method may return less than a full buffer of bytes to optimize and reduce protocol overhead.*
- *This method sets the transfer direction to be inbound and calls* `receiveBytes(5)`.
- *This method may only be called once in a* `Applet.process()` *method.*

Returns:
number of bytes read. Returns 0 if no bytes are available.

Throws:
APDUException - with the following reason codes:

- `APDUException.ILLEGAL_USE` if `setIncomingAndReceive()` already invoked or if `setOutgoing()` or `setOutgoingNoChaining()` previously invoked.
- `APDUException.IO_ERROR` on I/O error.
- `APDUException.T1_IFD_ABORT` if T=1 protocol is in use and the CAD sends in an ABORT S-Block command to abort the data transfer.

---

sendBytes

```
public void sendBytes(short bOff,
                      short len)
               throws APDUException
```

Sends `len` more bytes from APDU buffer at specified offset `bOff`.

If the last part of the response is being sent by the invocation of this method, the APDU buffer must not be altered. If the data is altered, incorrect output may be sent to the CAD. Requiring that the buffer not be altered allows the implementation to reduce protocol overhead by transmitting the last part of the response along with the status bytes.

Notes:

- *If* `setOutgoingNoChaining()` *was invoked, output block chaining must not be used.*
- *In T=0 protocol, if* `setOutgoingNoChaining()` *was invoked, Le bytes must be transmitted before response status is returned.*
- *In T=0 protocol, if this method throws an* `APDUException` *with* `NO_T0_GETRESPONSE` *reason code, the JCRE will restart APDU command processing using the newly received command. No more output data can be transmitted. No error status response can be returned.*
- *In T=1 protocol, if this method throws an* `APDUException` *with* `T1_IFD_ABORT` *reason code, the JCRE will restart APDU command processing using the newly received command. No more output data can be transmitted. No error status response can be returned.*

Parameters:

`bOff` - the offset into APDU buffer.
`len` - the length of the data in bytes to send.

Throws:

APDUException - with the following reason codes:

- `APDUException.ILLEGAL_USE` if `setOutgoingLen()` not called or `setOutgoingAndSend()` previously invoked or response byte count exeeded or if `APDUException.NO_T0_GETRESPONSE` previously thrown.
- `APDUException.BUFFER_BOUNDS` if the sum of `bOff` and `len` exceeds the buffer size.
- `APDUException.IO_ERROR` on I/O error.
- `APDUException.NO_T0_GETRESPONSE` if T=0 protocol is in use and the CAD does not respond to response status with GET RESPONSE command.
- `APDUException.T1_IFD_ABORT` if T=1 protocol is in use and the CAD sends in an ABORT S-Block command to abort the data transfer.

See Also:

`setOutgoing()`, `setOutgoingNoChaining()`

---

sendBytesLong

```
public void sendBytesLong(byte[] outData,
                          short bOff,
                          short len)
                   throws APDUException
```

Sends `len` more bytes from `outData` byte array starting at specified offset `bOff`.

If the last of the response is being sent by the invocation of this method, the APDU buffer must not be altered. If the data is altered, incorrect output may be sent to the CAD. Requiring that the buffer not be altered allows the implementation to reduce protocol overhead by transmitting the last part of the response along with the status bytes.

The JCRE may use the APDU buffer to send data to the CAD.

Notes:

- *If* `setOutgoingNoChaining()` *was invoked, output block chaining must not be used.*
- *In T=0 protocol, if* `setOutgoingNoChaining()` *was invoked, Le bytes must be transmitted before response status is returned.*
- *In T=0 protocol, if this method throws an* `APDUException` *with NO_T0_GETRESPONSE reason code, the JCRE will restart APDU command processing using the newly received command. No more output data can be transmitted. No error status response can be returned.*
- *In T=1 protocol, if this method throws an* `APDUException` *with* `T1_IFD_ABORT` *reason code, the JCRE will restart APDU command processing using the newly received command. No more output data can be transmitted. No error status response can be returned.*

Parameters:

`outData` - the source data byte array.
`bOff` - the offset into OutData array.
`len` - the bytelength of the data to send.

Throws:

APDUException - with the following reason codes:

- `APDUException.ILLEGAL_USE` if `setOutgoingLen()` not called or `setOutgoingAndSend()` previously invoked or response byte count exeeded or if `APDUException.NO_T0_GETRESPONSE` previously thrown.
- `APDUException.IO_ERROR` on I/O error.
- `APDUException.NO_T0_GETRESPONSE` if T=0 protocol is in use and CAD does not respond to response status with GET RESPONSE command.
- `APDUException.T1_IFD_ABORT` if T=1 protocol is in use and the CAD sends in an ABORT S-Block command to abort the data transfer.

See Also:

`setOutgoing()`, `setOutgoingNoChaining()`

setOutgoingAndSend

```
public void setOutgoingAndSend(short bOff,
                               short len)
                        throws APDUException
```

This is the "convenience" send method. It provides for the most efficient way to send a short response which fits in the buffer and needs the least protocol overhead. This method is a combination of `setOutgoing(), setOutgoingLength( len )` followed by `sendBytes ( bOff, len )`. In addition, once this method is invoked, `sendBytes()` and `sendBytesLong()` methods cannot be invoked and the APDU buffer must not be altered.

Sends `len` byte response from the APDU buffer at starting specified offset `bOff`.

Notes:

- *No other* `APDU` *send methods can be invoked.*
- *The APDU buffer must not be altered. If the data is altered, incorrect output may be sent to the CAD.*
- *The actual data transmission may only take place on return from* `Applet.process()`

Parameters:

`bOff` - the offset into APDU buffer.
`len` - the bytelength of the data to send.

Throws:

APDUException - with the following reason codes:

- `APDUException.ILLEGAL_USE` if `setOutgoing()` or `setOutgoingAndSend()` previously invoked or response byte count exeeded.
- `APDUException.IO_ERROR` on I/O error.

---

waitExtension

```
public void waitExtension()
                  throws APDUException
```

Requests additional processsing time from CAD. The implementation should ensure that this method needs to be invoked only under unusual conditions requiring excessive processing times.

Notes:

- *In T=0 protocol, a NULL procedure byte is sent to reset the work waiting time (see ISO 7816-3).*
- *In T=1 protocol, the implementation needs to request the same T=0 protocol work waiting time quantum by sending a T=1 protocol request for wait time extension(see ISO 7816-3).*
- *If the implementation uses an automatic timer mechanism instead, this method may do nothing.*

Throws:

APDUException - with the following reason codes:

- `APDUException.ILLEGAL_USE` if `setOutgoingNoChaining()` previously

invoked.

- `APDUException.IO_ERROR` on I/O error.

---

javacard.framework
Class APDUException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--javacard.framework.CardRuntimeException
                          |
                          +--javacard.framework.APDUException
```

public class **APDUException**
extends CardRuntimeException

`APDUException` represents an `APDU` related exception.

The `APDU` class throws JCRE owned instances of `APDUException`.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

See Also:
`APDU`

Field Summary

static short	**BAD_LENGTH** This reason code is used by the APDU.setOutgoingLength() method to indicate that the length parameter is greater that 256 or if non BLOCK CHAINED data transfer is requested and len is greater than (IFSD-2), where IFSD is the Outgoing Block Size.
static short	**BUFFER_BOUNDS** This reason code is used by the APDU.sendBytes() method to indicate that the sum of buffer offset parameter and the byte length parameter exceeds the APDU buffer size.
static short	**ILLEGAL_USE** This APDUException reason code indicates that the method should not be invoked based on the current state of the APDU.
static short	**IO_ERROR** This reason code indicates that an unrecoverable error occurred in the I/O transmission layer.
static short	**NO_T0_GETRESPONSE** This reason code indicates that during T=0 protocol, the CAD did not return a GET RESPONSE command in response to a <61xx> response status to send additional data.
static short	**T1_IFD_ABORT** This reason code indicates that during T=1 protocol, the CAD returned an ABORT S-Block command and aborted the data transfer.

Constructor Summary

APDUException(short reason) Constructs an APDUException.	

Method Summary

static void	**throwIt**(short reason) Throws the JCRE owned instance of APDUException with the specified reason.

Methods inherited from class javacard.framework.CardRuntimeException
`getReason, setReason`

Methods inherited from class java.lang.Object
`equals`

Field Detail

ILLEGAL_USE

```
public static final short ILLEGAL_USE
```

This APDUException reason code indicates that the method should not be invoked based on the current state of the APDU.

BUFFER_BOUNDS

```
public static final short BUFFER_BOUNDS
```

This reason code is used by the `APDU.sendBytes()` method to indicate that the sum of buffer offset parameter and the byte length parameter exceeds the APDU buffer size.

BAD_LENGTH

```
public static final short BAD_LENGTH
```

This reason code is used by the `APDU.setOutgoingLength()` method to indicate that the length parameter is greater that 256 or if non BLOCK CHAINED data transfer is requested and `len` is greater than (IFSD-2), where IFSD is the Outgoing Block Size.

IO_ERROR

```
public static final short IO_ERROR
```

This reason code indicates that an unrecoverable error occurred in the I/O transmission layer.

NO_T0_GETRESPONSE

```
public static final short NO_T0_GETRESPONSE
```

This reason code indicates that during T=0 protocol, the CAD did not return a GET RESPONSE command in response to a <61xx> response status to send additional data. The outgoing transfer has been aborted. No more data or status can be sent to the CAD in this `APDU.process()` method.

T1_IFD_ABORT

```
public static final short T1_IFD_ABORT
```

This reason code indicates that during T=1 protocol, the CAD returned an ABORT S-Block command and aborted the data transfer. The incoming or outgoing transfer has been aborted. No more data can be received from the CAD. No more data or status can be sent to the CAD in this `APDU.process()` method.

Constructor Detail

APDUException

```
public APDUException(short reason)
```

Constructs an APDUException. To conserve on resources use `throwIt()` to use the JCRE owned instance of this class.

Parameters:

`reason` - the reason for the exception.

Method Detail

throwIt

```
public static void throwIt(short reason)
```

Throws the JCRE owned instance of `APDUException` with the specified reason.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Parameters:

`reason` - the reason for the exception.

Throws:

APDUException - always.

javacard.framework
Class Applet

```
java.lang.Object
  |
  +--javacard.framework.Applet
```

public abstract class **Applet**
extends Object

This abstract class defines an applet in Java Card.

The `Applet` class should be extended by any applet that is intended to be loaded onto, installed into and executed on a Java Card compliant smart card.

Example usage of `Applet`

```
public class MyApplet extends javacard.framework.Applet{
static byte someByteArray[];

public static void install( byte[] bArray, short bOffset, byte bLength  ) throws ISOException {
  // make all my allocations here, so I do not run
  // out of memory later
  MyApplet theApplet = new MyApplet();

  // check incoming parameter
  byte bLen = bArray[bOffset];
  if ( bLen!=0 ) { someByteArray = new byte[bLen]; theApplet.register(); return; }
  else ISOException.throwIt(ISO7816.SW_FUNC_NOT_SUPPORTED);
  }

public boolean select(){
  // selection initialization
  someByteArray[17] = 42; // set selection state
  return true;
  }

public void process(APDU apdu) throws ISOException{
 byte[] buffer = apdu.getBuffer();
 // .. process the incoming data and reply
 if ( buffer[ISO7816.OFFSET_CLA] == (byte)0 ) {
    switch ( buffer[ISO7816.OFFSET_INS] ) {
        case ISO.INS_SELECT:
            ...
            // send response data to select command
            short Le =  apdu.setOutgoing();
            // assume data containing response bytes in replyData[] array.
            if ( Le < ..) ISOException.throwIt( ISO7816.SW_WRONG_LENGTH);
            apdu.setOutgoingLength( (short)replyData.length );
            apdu.sendBytesLong(replyData, (short) 0, (short)replyData.length);
            break;
        case ...
        }
     }
```

```
  }
}
```

See Also:
`SystemException`, `JCSystem`

Constructor Summary

protected	**`Applet`**`()` Only this class's `install()` method should create the applet object.

Method Summary

void	**`deselect`**`()` Called by the JCRE to inform this currently selected applet that another (or the same) applet will be selected.
Shareable	**`getShareableInterfaceObject`**`(AID clientAID, byte parameter)` Called by the JCRE to obtain a shareable interface object from this server applet, on behalf of a request from a client applet.
static void	**`install`**`(byte[] bArray, short bOffset, byte bLength)` To create an instance of the `Applet` subclass, the JCRE will call this static method first.
abstract void	**`process`**`(APDU apdu)` Called by the JCRE to process an incoming APDU command.
protected void	**`register`**`()` This method is used by the applet to register `this` applet instance with the JCRE and to assign the `Applet` subclass AID bytes as its instance AID bytes.
protected void	**`register`**`(byte[] bArray, short bOffset, byte bLength)` This method is used by the applet to register `this` applet instance with the JCRE and assign the specified AID bytes as its instance AID bytes.
boolean	**`select`**`()` Called by the JCRE to inform this applet that it has been selected.
protected boolean	**`selectingApplet`**`()` This method is used by the applet `process()` method to distinguish the SELECT APDU command which selected `this` applet, from all other other SELECT APDU commands which may relate to file or internal applet state selection.

Methods inherited from class java.lang.Object
`equals`

Constructor Detail

Applet

```
protected Applet()
```

Only this class's `install()` method should create the applet object.

Method Detail

install

```
public static void install(byte[] bArray,
                           short bOffset,
                           byte bLength)
                    throws ISOException
```

To create an instance of the `Applet` subclass, the JCRE will call this static method first.

The applet should perform any necessary initializations and must call one of the `register()` methods. The installation is considered successful when the call to `register()` completes without an exception. The installation is deemed unsuccessful if the `install` method does not call a `register()` method, or if an exception is thrown from within the `install` method prior to the call to a `register()` method, or if the `register()` method throws an exception. If the installation is unsuccessful, the JCRE must perform all the necessary clean up when it receives control. Successful installation makes the applet instance capable of being selected via a SELECT APDU command.

Installation parameters are supplied in the byte array parameter and must be in a format defined by the applet. The `bArray` object is a global array. If the applet desires to preserve any of this data, it should copy the data into its own object.

`bArray` is zeroed by the JCRE after the return from the `install()` method.

References to the `bArray` object cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

The implementation of this method provided by `Applet` class throws an `ISOException` with reason code = `ISO7816.SW_FUNC_NOT_SUPPORTED`.

Note:

- *Exceptions thrown by this method after successful installation are caught by the JCRE and processed by the Installer.*

Parameters:

`bArray` - the array containing installation parameters.
`bOffset` - the starting offset in bArray.
`bLength` - the length in bytes of the parameter data in bArray. The maximum value of bLength is 32.

---

process

```
public abstract void process(APDU apdu)
                     throws ISOException
```

Called by the JCRE to process an incoming APDU command. An applet is expected to perform the action requested and return response data if any to the terminal.

Upon normal return from this method the JCRE sends the ISO 7816-4 defined success status (90 00) in APDU response. If this method throws an `ISOException` the JCRE sends the associated reason code as the response status instead.

The JCRE zeroes out the APDU buffer before receiving a new APDU command from the CAD. The five header bytes of the APDU command are available in APDU buffer[0..4] at the time this method is called.

The `APDU` object parameter is a temporary JCRE Entry Point Object. A temporary JCRE Entry Point Object can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components.

Notes:

- *APDU buffer[5..] is undefined and should not be read or written prior to invoking the* `APDU.setIncomingAndReceive()` *method if incoming data is expected. Altering the APDU buffer[5..] could corrupt incoming data.*

Parameters:

`apdu` - the incoming `APDU` object

Throws:

ISOException - with the response bytes per ISO 7816-4

See Also:

`APDU`

---

select

```
public boolean select()
```

Called by the JCRE to inform this applet that it has been selected.

It is called when a SELECT APDU command is received and before the applet is selected. SELECT APDU commands use instance AID bytes for applet selection. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

A subclass of `Applet` should override this method if it should perform any initialization that may be required to process APDU commands that may follow. This method returns a boolean to indicate that it is ready to accept incoming APDU commands via its `process()` method. If this method returns false, it indicates to the JCRE that this Applet declines to be selected.

The implementation of this method provided by `Applet` class returns `true`.

Returns:
`true` to indicate success, `false` otherwise.

---

deselect

```
public void deselect()
```

Called by the JCRE to inform this currently selected applet that another (or the same) applet will be selected. It is called when a SELECT APDU command is received by the JCRE. This method is invoked prior to another applets or this very applets `select()` method being invoked.

A subclass of `Applet` should override this method if it has any cleanup or bookkeeping work to be performed before another applet is selected.

The default implementation of this method provided by `Applet` class does nothing.

Notes:

- *Unchecked exceptions thrown by this method are caught by the JCRE but the applet is deselected.*
- *Transient objects of* `JCSystem.CLEAR_ON_DESELECT` *clear event type are cleared to their default value by the JCRE after this method.*
- *This method is NOT called on reset or power loss.*

---

getShareableInterfaceObject

```
public Shareable getShareableInterfaceObject(AID clientAID,
                                             byte parameter)
```

Called by the JCRE to obtain a shareable interface object from this server applet, on behalf of a request from a client applet. This method executes in the applet context of `this` applet instance. The client applet initiated this request by calling the `JCSystem.getAppletShareableInterfaceObject()` method. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Parameters:

`clientAID` - the `AID` object of the client applet.

`parameter` - optional parameter byte. The parameter byte may be used by the client to specify which shareable interface object is being requested.

Returns:

the shareable interface object or `null`. Note:

- *The* `clientAID` *parameter is a JCRE owned* `AID` *instance. JCRE owned instances of* `AID` *are permanent JCRE Entry Point Objects and can be accessed from any applet context. References to these permanent objects can be stored and re-used.*

See Also:

`JCSystem.getAppletShareableInterfaceObject(AID, byte)`

---

register

```
protected final void register()
                      throws SystemException
```

This method is used by the applet to register `this` applet instance with the JCRE and to assign the `Applet` subclass AID bytes as its instance AID bytes. One of the `register()` methods must be called from within `install()` to be registered with the JCRE. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Throws:

SystemException - with the following reason codes:

- `SystemException.ILLEGAL_AID` if the `Applet` subclass AID bytes are in use or if the applet instance has previously called one of the `register()` methods.

---

register

```
protected final void register(byte[] bArray,
                              short bOffset,
                              byte bLength)
                      throws SystemException
```

This method is used by the applet to register `this` applet instance with the JCRE and assign the specified AID bytes as its instance AID bytes. One of the `register()` methods must be called from within `install()` to be registered with the JCRE. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Parameters:

`bArray` - the byte array containing the AID bytes.

`bOffset` - the start of AID bytes in bArray.

`bLength` - the length of the AID bytes in bArray.

Throws:

APDUException - with the following reason codes:

SystemException - with the following reason code:

- `SystemException.ILLEGAL_VALUE` if the `bLength` parameter is less than `5` or greater than `16`.
- `SystemException.ILLEGAL_AID` if the specified instance AID bytes are in use or if the RID portion of the AID bytes in the `bArray` parameter does not match the RID portion of the `Applet` subclass AID bytes or if the applet instance has previously called one of the `register()` methods.

---

selectingApplet

```
protected final boolean selectingApplet()
```

This method is used by the applet `process()` method to distinguish the SELECT APDU command which selected `this` applet, from all other other SELECT APDU commands which may relate to file or internal applet state selection.

Returns:

`true` if `this` applet is being selected.

---

javacard.framework
Class CardException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--javacard.framework.CardException
```

Direct Known Subclasses:
UserException

public class **CardException**
extends Exception

The `CardException` class defines a field `reason` and two accessor methods `getReason()` and `setReason()`. The `reason` field encapsulates exception cause identifier in Java Card. All Java Card checked Exception classes should extend `CardException`. This class also provides a resource-saving mechanism (`throwIt()` method) for using a JCRE owned instance of this class.

Constructor Summary

`CardException``(short reason)` Construct a CardException instance with the specified reason.

Method Summary

`short`	**`getReason`**`()` Get reason code
`void`	**`setReason`**`(short reason)` Set reason code
`static void`	**`throwIt`**`(short reason)` Throw the JCRE owned instance of `CardException` class with the specified reason.

Methods inherited from class java.lang.Object
equals

Constructor Detail

CardException

```
public CardException(short reason)
```

Construct a CardException instance with the specified reason. To conserve on resources, use the `throwIt()` method to use the JCRE owned instance of this class.

Parameters:

`reason` - the reason for the exception

Method Detail

getReason

```
public short getReason()
```

Get reason code

Returns:

the reason for the exception

---

setReason

```
public void setReason(short reason)
```

Set reason code

Parameters:

`reason` - the reason for the exception

---

throwIt

```
public static void throwIt(short reason)
                    throws CardException
```

Throw the JCRE owned instance of `CardException` class with the specified reason.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1*

Specification for details.

Parameters:

`reason` - the reason for the exception

Throws:

CardException - always.

---

javacard.framework
Class CardRuntimeException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--javacard.framework.CardRuntimeException
```

Direct Known Subclasses:
APDUException, CryptoException, ISOException, PINException, SystemException, TransactionException

---

public class **CardRuntimeException**
extends RuntimeException

The `CardRuntimeException` class defines a field `reason` and two accessor methods `getReason()` and `setReason()`. The `reason` field encapulates exception cause identifier in Java Card. All Java Card unchecked Exception classes should extend `CardRuntimeException`. This class also provides a resource-saving mechanism (`throwIt()` method) for using a JCRE owned instance of this class.

Constructor Summary

`CardRuntimeException``(short reason)` Construct a CardRuntimeException instance with the specified reason.

Method Summary

`short`	**`getReason`**`()` Get reason code
`void`	**`setReason`**`(short reason)` Set reason code
`static void`	**`throwIt`**`(short reason)` Throw the JCRE owned instance of the `CardRuntimeException` class with the specified reason.

Methods inherited from class java.lang.Object
equals

Constructor Detail

CardRuntimeException

```
public CardRuntimeException(short reason)
```

Construct a CardRuntimeException instance with the specified reason. To conserve on resources, use `throwIt()` method to use the JCRE owned instance of this class.

Parameters:

`reason` - the reason for the exception

Method Detail

getReason

```
public short getReason()
```

Get reason code

Returns:

the reason for the exception

---

setReason

```
public void setReason(short reason)
```

Set reason code

Parameters:

`reason` - the reason for the exception

---

throwIt

```
public static void throwIt(short reason)
                    throws CardRuntimeException
```

Throw the JCRE owned instance of the `CardRuntimeException` class with the specified reason.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Parameters:

`reason` - the reason for the exception

Throws:

CardRuntimeException - always.

---

javacard.framework
Interface ISO7816

public abstract interface **ISO7816**

`ISO7816` encapsulates constants related to ISO 7816-3 and ISO 7816-4. `ISO7816` interface contains only static fields.

The static fields with `SW_` prefixes define constants for the ISO 7816-4 defined response status word. The fields which use the `_00` suffix require the low order byte to be customized appropriately e.g (ISO7816.SW_CORRECT_LENGTH_00 + (0x0025 & 0xFF)).

The static fields with `OFFSET_` prefixes define constants to be used to index into the APDU buffer byte array to access ISO 7816-4 defined header information.

Field Summary

static byte	**CLA_ISO7816** APDU command CLA : ISO 7816 = 0x00
static byte	**INS_EXTERNAL_AUTHENTICATE** APDU command INS : EXTERNAL AUTHENTICATE = 0x82
static byte	**INS_SELECT** APDU command INS : SELECT = 0xA4
static byte	**OFFSET_CDATA** APDU command data offset : CDATA = 5
static byte	**OFFSET_CLA** APDU header offset : CLA = 0
static byte	**OFFSET_INS** APDU header offset : INS = 1
static byte	**OFFSET_LC** APDU header offset : LC = 4
static byte	**OFFSET_P1** APDU header offset : P1 = 2
static byte	**OFFSET_P2** APDU header offset : P2 = 3
static short	**SW_APPLET_SELECT_FAILED** Response status : Applet selection failed = 0x6999;

static short	**SW_BYTES_REMAINING_00** Response status : Response bytes remaining = 0x6100
static short	**SW_CLA_NOT_SUPPORTED** Response status : CLA value not supported = 0x6E00
static short	**SW_COMMAND_NOT_ALLOWED** Response status : Command not allowed (no current EF) = 0x6986
static short	**SW_CONDITIONS_NOT_SATISFIED** Response status : Conditions of use not satisfied = 0x6985
static short	**SW_CORRECT_LENGTH_00** Response status : Correct Expected Length (Le) = 0x6C00
static short	**SW_DATA_INVALID** Response status : Data invalid = 0x6984
static short	**SW_FILE_FULL** Response status : Not enough memory space in the file = 0x6A84
static short	**SW_FILE_INVALID** Response status : File invalid = 0x6983
static short	**SW_FILE_NOT_FOUND** Response status : File not found = 0x6A82
static short	**SW_FUNC_NOT_SUPPORTED** Response status : Function not supported = 0x6A81
static short	**SW_INCORRECT_P1P2** Response status : Incorrect parameters (P1,P2) = 0x6A86
static short	**SW_INS_NOT_SUPPORTED** Response status : INS value not supported = 0x6D00
static short	**SW_NO_ERROR** Response status : No Error = (short)0x9000
static short	**SW_RECORD_NOT_FOUND** Response status : Record not found = 0x6A83
static short	**SW_SECURITY_STATUS_NOT_SATISFIED** Response status : Security condition not satisfied = 0x6982
static short	**SW_UNKNOWN** Response status : No precise diagnosis = 0x6F00
static short	**SW_WRONG_DATA** Response status : Wrong data = 0x6A80
static short	**SW_WRONG_LENGTH** Response status : Wrong length = 0x6700

static short	**SW_WRONG_P1P2** Response status : Incorrect parameters (P1,P2) = 0x6B00

Field Detail

SW_NO_ERROR

```
public static final short SW_NO_ERROR
```

Response status : No Error = (short)0x9000

SW_BYTES_REMAINING_00

```
public static final short SW_BYTES_REMAINING_00
```

Response status : Response bytes remaining = 0x6100

SW_WRONG_LENGTH

```
public static final short SW_WRONG_LENGTH
```

Response status : Wrong length = 0x6700

SW_SECURITY_STATUS_NOT_SATISFIED

```
public static final short SW_SECURITY_STATUS_NOT_SATISFIED
```

Response status : Security condition not satisfied = 0x6982

SW_FILE_INVALID

```
public static final short SW_FILE_INVALID
```

Response status : File invalid = 0x6983

SW_DATA_INVALID

```
public static final short SW_DATA_INVALID
```

Response status : Data invalid = 0x6984

SW_CONDITIONS_NOT_SATISFIED

```
public static final short SW_CONDITIONS_NOT_SATISFIED
```

Response status : Conditions of use not satisfied = 0x6985

SW_COMMAND_NOT_ALLOWED

```
public static final short SW_COMMAND_NOT_ALLOWED
```

Response status : Command not allowed (no current EF) = 0x6986

SW_APPLET_SELECT_FAILED

```
public static final short SW_APPLET_SELECT_FAILED
```

Response status : Applet selection failed = 0x6999;

SW_WRONG_DATA

```
public static final short SW_WRONG_DATA
```

Response status : Wrong data = 0x6A80

SW_FUNC_NOT_SUPPORTED

```
public static final short SW_FUNC_NOT_SUPPORTED
```

Response status : Function not supported = 0x6A81

SW_FILE_NOT_FOUND

```
public static final short SW_FILE_NOT_FOUND
```

Response status : File not found = 0x6A82

SW_RECORD_NOT_FOUND

```
public static final short SW_RECORD_NOT_FOUND
```

Response status : Record not found = 0x6A83

SW_INCORRECT_P1P2

```
public static final short SW_INCORRECT_P1P2
```

Response status : Incorrect parameters (P1,P2) = 0x6A86

SW_WRONG_P1P2

```
public static final short SW_WRONG_P1P2
```

Response status : Incorrect parameters (P1,P2) = 0x6B00

SW_CORRECT_LENGTH_00

```
public static final short SW_CORRECT_LENGTH_00
```

Response status : Correct Expected Length (Le) = 0x6C00

SW_INS_NOT_SUPPORTED

```
public static final short SW_INS_NOT_SUPPORTED
```

Response status : INS value not supported = 0x6D00

SW_CLA_NOT_SUPPORTED

```
public static final short SW_CLA_NOT_SUPPORTED
```

Response status : CLA value not supported = 0x6E00

SW_UNKNOWN

```
public static final short SW_UNKNOWN
```

Response status : No precise diagnosis = 0x6F00

SW_FILE_FULL

```
public static final short SW_FILE_FULL
```

Response status : Not enough memory space in the file = 0x6A84

OFFSET_CLA

```
public static final byte OFFSET_CLA
```

APDU header offset : CLA = 0

OFFSET_INS

```
public static final byte OFFSET_INS
```

APDU header offset : INS = 1

OFFSET_P1

```
public static final byte OFFSET_P1
```

APDU header offset : P1 = 2

OFFSET_P2

```
public static final byte OFFSET_P2
```

APDU header offset : P2 = 3

OFFSET_LC

```
public static final byte OFFSET_LC
```

APDU header offset : LC = 4

OFFSET_CDATA

```
public static final byte OFFSET_CDATA
```

APDU command data offset : CDATA = 5

CLA_ISO7816

```
public static final byte CLA_ISO7816
```

APDU command CLA : ISO 7816 = 0x00

INS_SELECT

```
public static final byte INS_SELECT
```

APDU command INS : SELECT = 0xA4

INS_EXTERNAL_AUTHENTICATE

```
public static final byte INS_EXTERNAL_AUTHENTICATE
```

APDU command INS : EXTERNAL AUTHENTICATE = 0x82

javacard.framework
Class ISOException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--javacard.framework.CardRuntimeException
                          |
                          +--javacard.framework.ISOException
```

public class **ISOException**
extends CardRuntimeException

`ISOException` class encapsulates an ISO 7816-4 response status word as its `reason` code.

The `APDU` class throws JCRE owned instances of `ISOException`.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Constructor Summary

`ISOException``(short sw)` Constructs an ISOException instance with the specified status word.	

Method Summary

`static void`	**`throwIt`**`(short sw)` Throws the JCRE owned instance of the ISOException class with the specified status word.

Methods inherited from class javacard.framework.CardRuntimeException
`getReason, setReason`

Methods inherited from class java.lang.Object
equals

Constructor Detail

ISOException

```
public ISOException(short sw)
```

Constructs an ISOException instance with the specified status word. To conserve on resources use `throwIt()` to use the JCRE owned instance of this class.

Parameters:

`sw` - the ISO 7816-4 defined status word

Method Detail

throwIt

```
public static void throwIt(short sw)
```

Throws the JCRE owned instance of the ISOException class with the specified status word.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Parameters:

`sw` - ISO 7816-4 defined status word

Throws:

ISOException - always.

javacard.framework
Class JCSystem

```
java.lang.Object
  |
  +--javacard.framework.JCSystem
```

public final class **JCSystem**
extends Object

The `JCSystem` class includes a collection of methods to control applet execution, resource management, atomic transaction management and inter-applet object sharing in Java Card. All methods in `JCSystem` class are static methods.

The JCSystem class also includes methods to control the persistence and transience of objects. The term *persistent* means that objects and their values persist from one CAD session to the next, indefinitely. Persistent object values are updated atomically using transactions.

The `makeTransient...Array()` methods can be used to create *transient* arrays with primitive data components. Transient array data is lost (in an undefined state, but the real data is unavailable) immediately upon power loss, and is reset to the default value at the occurrence of certain events such as card reset or deselect. Updates to the values of transient arrays are not atomic and are not affected by transactions.

The JCRE maintains an atomic transaction commit buffer which is initialized on card reset (or power on). When a transaction is in progress, the JCRE journals all updates to persistent data space into this buffer so that it can always guarantee, at commit time, that everything in the buffer is written or nothing at all is written. The `JCSystem` includes methods to control an atomic transaction. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

See Also:
`SystemException`, `TransactionException`, `Applet`

Field Summary

`static byte`	**`CLEAR_ON_DESELECT`** This event code indicates that the contents of the transient object are cleared to the default value on applet deselection event or in `CLEAR_ON_RESET` cases.
`static byte`	**`CLEAR_ON_RESET`** This event code indicates that the contents of the transient object are cleared to the default value on card reset (or power on) event.
`static byte`	**`NOT_A_TRANSIENT_OBJECT`** This event code indicates that the object is not transient.

Method Summary	
static void	**abortTransaction**() Aborts the atomic transaction.
static void	**beginTransaction**() Begins an atomic transaction.
static void	**commitTransaction**() Commits an atomic transaction.
static AID	**getAID**() Returns the JCRE owned instance of the AID object associated with the current applet context.
static Shareable	**getAppletShareableInterfaceObject**(AID serverAID, byte parameter) This method is called by a client applet to get a server applet's shareable interface object.
static short	**getMaxCommitCapacity**() Returns the total number of bytes in the commit buffer.
static AID	**getPreviousContextAID**() This method is called to obtain the JCRE owned instance of the AID object associated with the previously active applet context.
static byte	**getTransactionDepth**() Returns the current transaction nesting depth level.
static short	**getUnusedCommitCapacity**() Returns the number of bytes left in the commit buffer.
static short	**getVersion**() Returns the current major and minor version of the Java Card API.
static byte	**isTransient**(Object theObj) Used to check if the specified object is transient.
static AID	**lookupAID**(byte[] buffer, short offset, byte length) Returns the JCRE owned instance of the AID object, if any, encapsulating the specified AID bytes in the buffer parameter if there exists a successfully installed applet on the card whose instance AID exactly matches that of the specified AID bytes.
static boolean[]	**makeTransientBooleanArray**(short length, byte event) Create a transient boolean array with the specified array length.
static byte[]	**makeTransientByteArray**(short length, byte event) Create a transient byte array with the specified array length.

`static Object[]`	**`makeTransientObjectArray`**`(short length, byte event)` Create a transient array of `Object` with the specified array length.
`static short[]`	**`makeTransientShortArray`**`(short length, byte event)` Create a transient short array with the specified array length.

Methods inherited from class java.lang.Object
`equals`

Field Detail

NOT_A_TRANSIENT_OBJECT

`public static final byte` **`NOT_A_TRANSIENT_OBJECT`**

This event code indicates that the object is not transient.

CLEAR_ON_RESET

`public static final byte` **`CLEAR_ON_RESET`**

This event code indicates that the contents of the transient object are cleared to the default value on card reset (or power on) event.

CLEAR_ON_DESELECT

`public static final byte` **`CLEAR_ON_DESELECT`**

This event code indicates that the contents of the transient object are cleared to the default value on applet deselection event or in `CLEAR_ON_RESET` cases.

Notes:

- `CLEAR_ON_DESELECT` *transient objects can be accessed only when the applet which created the object is the currently the selected applet.*
- *The JCRE will throw a* `SecurityException` *if a* `CLEAR_ON_DESELECT` *transient object is accessed when the currently selected applet is not the applet which created the object.*

Method Detail

isTransient

```
public static byte isTransient(Object theObj)
```

Used to check if the specified object is transient.

Notes:

This method returns `NOT_A_TRANSIENT_OBJECT` *if the specified object is* `null` *or is not an array type.*

Parameters:

`theObj` - the object being queried.

Returns:

`NOT_A_TRANSIENT_OBJECT`, `CLEAR_ON_RESET`, or `CLEAR_ON_DESELECT`.

See Also:

`makeTransientBooleanArray(short, byte)`,
`makeTransientByteArray(short, byte)`,
`makeTransientShortArray(short, byte)`,
`makeTransientObjectArray(short, byte)`

---

makeTransientBooleanArray

```
public static boolean[] makeTransientBooleanArray(short length,
                                                  byte event)
                                           throws SystemException
```

Create a transient boolean array with the specified array length.

Parameters:

`length` - the length of the boolean array.

`event` - the `CLEAR_ON...` event which causes the array elements to be cleared.

Throws:

SystemException - with the following reason codes:

- `SystemException.ILLEGAL_VALUE` if event is not a valid event code.
- `SystemException.NO_TRANSIENT_SPACE` if sufficient transient space is not available.
- `SystemException.ILLEGAL_TRANSIENT` if the current applet context is not the currently selected applet context and `CLEAR_ON_DESELECT` is specified.

---

makeTransientByteArray

```
public static byte[] makeTransientByteArray(short length,
                                            byte event)
                                     throws SystemException
```

Create a transient byte array with the specified array length.

Parameters:

`length` - the length of the byte array.

`event` - the `CLEAR_ON...` event which causes the array elements to be cleared.

Throws:

SystemException - with the following reason codes:

- `SystemException.ILLEGAL_VALUE` if event is not a valid event code.
- `SystemException.NO_TRANSIENT_SPACE` if sufficient transient space is not available.
- `SystemException.ILLEGAL_TRANSIENT` if the current applet context is not the currently selected applet context and `CLEAR_ON_DESELECT` is specified.

---

makeTransientShortArray

```
public static short[] makeTransientShortArray(short length,
                                               byte event)
                                        throws SystemException
```

Create a transient short array with the specified array length.

Parameters:

`length` - the length of the short array.

`event` - the `CLEAR_ON...` event which causes the array elements to be cleared.

Throws:

SystemException - with the following reason codes:

- `SystemException.ILLEGAL_VALUE` if event is not a valid event code.
- `SystemException.NO_TRANSIENT_SPACE` if sufficient transient space is not available.
- `SystemException.ILLEGAL_TRANSIENT` if the current applet context is not the currently selected applet context and `CLEAR_ON_DESELECT` is specified.

---

makeTransientObjectArray

```
public static Object[] makeTransientObjectArray(short length,
                                                 byte event)
                                          throws SystemException
```

Create a transient array of `Object` with the specified array length.

Parameters:

`length` - the length of the `Object` array.

`event` - the `CLEAR_ON...` event which causes the array elements to be cleared.

Throws:

SystemException - with the following reason codes:

- `SystemException.ILLEGAL_VALUE` if event is not a valid event code.
- `SystemException.NO_TRANSIENT_SPACE` if sufficient transient space is not available.
- `SystemException.ILLEGAL_TRANSIENT` if the current applet context is not the currently selected applet context and `CLEAR_ON_DESELECT` is specified.

getVersion

```
public static short getVersion()
```

Returns the current major and minor version of the Java Card API.

Returns:

version number as byte.byte (major.minor)

getAID

```
public static AID getAID()
```

Returns the JCRE owned instance of the `AID` object associated with the current applet context. Returns `null` if the `Applet.register()` method has not yet been invoked.

JCRE owned instances of `AID` are permanent JCRE Entry Point Objects and can be accessed from any applet context. References to these permanent objects can be stored and re-used.

See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Returns:

the `AID` object.

lookupAID

```
public static AID lookupAID(byte[] buffer,
                            short offset,
                            byte length)
```

Returns the JCRE owned instance of the `AID` object, if any, encapsulating the specified AID bytes in the `buffer` parameter if there exists a successfully installed applet on the card whose instance AID exactly matches that of the specified AID bytes.

JCRE owned instances of `AID` are permanent JCRE Entry Point Objects and can be accessed from any applet context. References to these permanent objects can be stored and re-used.

See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Parameters:

`buffer` - byte array containing the AID bytes.
`offset` - offset within buffer where AID bytes begin.
`length` - length of AID bytes in buffer.

Returns:

the `AID` object, if any; `null` otherwise. A VM exception is thrown if `buffer` is `null`, or if `offset` or `length` are out of range.

beginTransaction

```
public static void beginTransaction()
                            throws TransactionException
```

Begins an atomic transaction. If a transaction is already in progress (transactionDepth != 0), a TransactionException is thrown.

Throws:

TransactionException - with the following reason codes:

- `TransactionException.IN_PROGRESS` if a transaction is already in progress.

See Also:

`commitTransaction()`, `abortTransaction()`

---

abortTransaction

```
public static void abortTransaction()
                            throws TransactionException
```

Aborts the atomic transaction. The contents of the commit buffer is discarded.

Notes:

- *Do not call this method from within a transaction which creates new objects because the JCRE may not recover the heap space used by the new object instances.*
- *The JCRE ensures that any variable of reference type which references an object instantiated from within this aborted transaction is equivalent to a* `null` *reference.*

Throws:

TransactionException - with the following reason codes:

- `TransactionException.NOT_IN_PROGRESS` if a transaction is not in progress.

See Also:

`beginTransaction()`, `commitTransaction()`

---

commitTransaction

```
public static void commitTransaction()
                             throws TransactionException
```

Commits an atomic transaction. The contents of commit buffer is atomically commited. If a transaction is not in progress (transactionDepth == 0) then a TransactionException is thrown.

Throws:

TransactionException - with the following reason codes:

- `TransactionException.NOT_IN_PROGRESS` if a transaction is not in progress.

See Also:

`beginTransaction()`, `abortTransaction()`

getTransactionDepth

```
public static byte getTransactionDepth()
```

Returns the current transaction nesting depth level. At present, only 1 transaction can be in progress at a time.

Returns:

1 if transaction in progress, 0 if not.

getUnusedCommitCapacity

```
public static short getUnusedCommitCapacity()
```

Returns the number of bytes left in the commit buffer.

Returns:

the number of bytes left in the commit buffer

See Also:

`getMaxCommitCapacity()`

getMaxCommitCapacity

```
public static short getMaxCommitCapacity()
```

Returns the total number of bytes in the commit buffer. This is approximately the maximum number of bytes of persistent data which can be modified during a transaction. However, the transaction subsystem requires additional bytes of overhead data to be included in the commit buffer, and this depends on the number of fields modified and the implementation of the transaction subsystem. The application cannot determine the actual maximum amount of data which can be modified during a transaction without taking these overhead bytes into consideration.

Returns:

the total number of bytes in the commit buffer

See Also:

`getUnusedCommitCapacity()`

getPreviousContextAID

```
public static AID getPreviousContextAID()
```

This method is called to obtain the JCRE owned instance of the `AID` object associated with the previously active applet context. This method is typically used by a server applet, while executing a shareable interface method to determine the identity of its client and thereby control access privileges.

JCRE owned instances of `AID` are permanent JCRE Entry Point Objects and can be accessed from any applet context. References to these permanent objects can be stored and re-used.

See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Returns:

the `AID` object of the previous context, or `null` if JCRE.

---

getAppletShareableInterfaceObject

```
public static Shareable getAppletShareableInterfaceObject(AID serverAID,
                                                          byte parameter)
```

This method is called by a client applet to get a server applet's shareable interface object.

This method returns `null` if the `Applet.register()` has not yet been invoked or if the server does not exist or if the server returns `null`.

Parameters:

`serverAID` - the AID of the server applet.

`parameter` - optional parameter data.

Returns:

the shareable interface object or `null`.

See Also:

`Applet.getShareableInterfaceObject(AID, byte)`

---

javacard.framework
Class OwnerPIN

```
java.lang.Object
  |
  +--javacard.framework.OwnerPIN
```

public class **OwnerPIN**
extends Object
implements PIN

This class represents an Owner PIN. It implements Personal Identification Number functionality as defined in the `PIN` interface. It provides the ability to update the PIN and thus owner functionality.

The implementation of this class must protect against attacks based on program flow prediction.Even if a transaction is in progress, internal state such as the try counter, the validated flag and the blocking state must not be conditionally updated during PIN presentation.

If an implementation of this class creates transient arrays, it must ensure that they are `CLEAR_ON_RESET` transient objects.

The protected methods `getValidatedFlag` and `setValidatedFlag` allow a subclass of this class to optimize the storage for the validated boolean state.

Some methods of instances of this class are only suitable for sharing when there exists a trust relationship among the applets. A typical shared usage would use a proxy PIN interface which implements both the `PIN` interface and the `Shareable` interface.

Any of the methods of the `OwnerPIN` may be called with a transaction in progress. None of the methods of `OwnerPIN` class initiate or alter the state of the transaction if one is in progress.

See Also:
`PINException`, `PIN`, `Shareable`, `JCSystem`

Constructor Summary

`OwnerPIN``(byte tryLimit, byte maxPINSize)` Constructor.

Method Summary

boolean	**check**(byte[] pin, short offset, byte length) Compares pin against the PIN value.
byte	**getTriesRemaining**() Returns the number of times remaining that an incorrect PIN can be presented before the PIN is blocked.
protected boolean	**getValidatedFlag**() This protected method returns the validated flag.
boolean	**isValidated**() Returns true if a valid PIN has been presented since the last card reset or last call to reset().
void	**reset**() If the validated flag is set, this method resets it.
void	**resetAndUnblock**() This method resets the validated flag and resets the PIN try counter to the value of the PIN try limit.
protected void	**setValidatedFlag**(boolean value) This protected method sets the value of the validated flag.
void	**update**(byte[] pin, short offset, byte length) This method sets a new value for the PIN and resets the PIN try counter to the value of the PIN try limit.

Methods inherited from class java.lang.Object
equals

Constructor Detail

OwnerPIN

```
public OwnerPIN(byte tryLimit,
                byte maxPINSize)
         throws PINException
```

Constructor. Allocates a new PIN instance.

Parameters:

tryLimit - the maximum number of times an incorrect PIN can be presented.

maxPINSize - the maximum allowed PIN size. maxPINSize must be >=1.

Throws:

PINException - with the following reason codes:

- `PINException.ILLEGAL_VALUE` if `maxPINSize` parameter is less than 1.

Method Detail

getValidatedFlag

```
protected boolean getValidatedFlag()
```

This protected method returns the validated flag. This method is intended for subclass of this `OwnerPIN` to access or override the internal PIN state of the `OwnerPIN`.

Returns:

the boolean state of the PIN validated flag.

---

setValidatedFlag

```
protected void setValidatedFlag(boolean value)
```

This protected method sets the value of the validated flag. This method is intended for subclass of this `OwnerPIN` to control or override the internal PIN state of the `OwnerPIN`.

Parameters:

`value` - the new value for the validated flag.

---

getTriesRemaining

```
public byte getTriesRemaining()
```

Returns the number of times remaining that an incorrect PIN can be presented before the `PIN` is blocked.

Specified by:

getTriesRemaining in interface PIN

Returns:

the number of times remaining

---

check

```
public boolean check(byte[] pin,
                     short offset,
                     byte length)
```

Compares `pin` against the PIN value. If they match and the `PIN` is not blocked, it sets the validated flag and resets the try counter to its maximum. If it does not match, it decrements the try counter, and if the counter has reached zero, blocks the `PIN`. Even if a transaction is in progress, internal state such as the try counter, the validated flag and the blocking state must not be conditionally updated.

Specified by:
check in interface PIN
Parameters:
`pin` - the byte array containing the PIN value being checked
`offset` - the starting offset in the pin array
`length` - the length of pin.
Returns:
`true` if the PIN value matches; `false` otherwise

---

isValidated

```
public boolean isValidated()
```

Returns `true` if a valid PIN has been presented since the last card reset or last call to `reset()`.
Specified by:
isValidated in interface PIN
Returns:
`true` if validated; `false` otherwise

---

reset

```
public void reset()
```

If the validated flag is set, this method resets it. If the validated flag is not set, this method does nothing.
Specified by:
reset in interface PIN

---

update

```
public void update(byte[] pin,
                   short offset,
                   byte length)
            throws PINException
```

This method sets a new value for the PIN and resets the `PIN` try counter to the value of the `PIN` try limit. It also resets the validated flag.

This method copies the input pin parameter into an internal representation. If a transaction is in progress, the new pin and try counter update must be conditional i.e the copy operation must use the transaction facility.
Parameters:
`pin` - the byte array containing the new PIN value
`offset` - the starting offset in the pin array
`length` - the length of the new PIN.

Throws:

PINException - with the following reason codes:

- `PINException.ILLEGAL_VALUE` if length is greater than configured maximum PIN size.

See Also:

`JCSystem.beginTransaction()`

---

resetAndUnblock

```
public void resetAndUnblock()
```

This method resets the validated flag and resets the `PIN` try counter to the value of the `PIN` try limit. This method is used by the owner to re-enable the blocked `PIN`.

---

javacard.framework
Interface PIN

All Known Implementing Classes:
OwnerPIN

public abstract interface **PIN**

This interface represents a PIN. An implementation must maintain these internal values:

- PIN value
- try limit, the maximum number of times an incorrect PIN can be presented before the PIN is blocked. When the PIN is blocked, it cannot be validated even on valid PIN presentation.
- max PIN size, the maximum length of PIN allowed
- try counter, the remaining number of times an incorrect PIN presentation is permitted before the `PIN` becomes blocked.
- validated flag, true if a valid PIN has been presented. This flag is reset on every card reset.

This interface does not make any assumptions about where the data for the PIN value comparison is stored.

An owner implementation of this interface must provide a way to initialize/update the PIN value.The owner implemention of the interface must protect against attacks based on program flow prediction. Even if a transaction is in progress, internal state such as the try counter, the validated flag and the blocking state must not be conditionally updated during PIN presentation.

A typical card global PIN usage will combine an instance of `OwnerPIN` class and a a Proxy PIN interface which implements both the `PIN` and the `Shareable` interfaces. The `OwnerPIN` instance would be manipulated only by the owner who has update privilege. All others would access the global PIN functionality via the proxy PIN interface.

See Also:
`OwnerPIN`, `Shareable`

Method Summary	
boolean	**check**(byte[] pin, short offset, byte length) Compares pin against the PIN value.
byte	**getTriesRemaining**() Returns the number of times remaining that an incorrect PIN can be presented before the PIN is blocked.
boolean	**isValidated**() Returns true if a valid PIN value has been presented since the last card reset or last call to reset().
void	**reset**() If the validated flag is set, this method resets it.

Method Detail

getTriesRemaining

```
public byte getTriesRemaining()
```

Returns the number of times remaining that an incorrect PIN can be presented before the PIN is blocked.

Returns:

the number of times remaining

---

check

```
public boolean check(byte[] pin,
                     short offset,
                     byte length)
```

Compares pin against the PIN value. If they match and the PIN is not blocked, it sets the validated flag and resets the try counter to its maximum. If it does not match, it decrements the try counter, and if the counter has reached zero, blocks the PIN. Even if a transaction is in progress, internal state such as the try counter, the validated flag and the blocking state must not be conditionally updated.

Parameters:

pin - the byte array containing the PIN value being checked
offset - the starting offset in the pin array
length - the length of the PIN value.

Returns:

true if the PIN value matches; false otherwise

isValidated

```
public boolean isValidated()
```

Returns `true` if a valid PIN value has been presented since the last card reset or last call to `reset()`.

Returns:

`true` if validated; `false` otherwise

reset

```
public void reset()
```

If the validated flag is set, this method resets it. If the validated flag is not set, this method does nothing.

javacard.framework
Class PINException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--javacard.framework.CardRuntimeException
                          |
                          +--javacard.framework.PINException
```

public class **PINException**
extends CardRuntimeException

`PINException` represents a `OwnerPIN` class access-related exception.

The `OwnerPIN` class throws JCRE owned instances of `PINException`.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

See Also:
`OwnerPIN`

Field Summary

`static short`	**`ILLEGAL_VALUE`** This reason code is used to indicate that one or more input parameters is out of allowed bounds.

Constructor Summary

`PINException``(short reason)` Constructs a PINException.	

Method Summary

`static void`	**`throwIt`**`(short reason)` Throws the JCRE owned instance of `PINException` with the specified reason.

Methods inherited from class javacard.framework.CardRuntimeException

`getReason, setReason`

Methods inherited from class java.lang.Object

`equals`

Field Detail

ILLEGAL_VALUE

```
public static final short ILLEGAL_VALUE
```

This reason code is used to indicate that one or more input parameters is out of allowed bounds.

Constructor Detail

PINException

```
public PINException(short reason)
```

Constructs a PINException. To conserve on resources use `throwIt()` to use the JCRE owned instance of this class.

Parameters:

`reason` - the reason for the exception.

Method Detail

throwIt

```
public static void throwIt(short reason)
```

Throws the JCRE owned instance of `PINException` with the specified reason.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Parameters:

`reason` - the reason for the exception.

Throws:

PINException - always.

---

javacard.framework
Interface Shareable

public abstract interface **Shareable**

The Shareable interface serves to identify all shared objects. Any object that needs to be shared through the applet firewall must directly or indirectly implement this interface. Only those methods specified in a shareable interface are available through the firewall. Implementation classes can implement any number of shareable interfaces and can extend other shareable implementation classes.

javacard.framework
Class SystemException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--javacard.framework.CardRuntimeException
                          |
                          +--javacard.framework.SystemException
```

public class **SystemException**
extends CardRuntimeException

`SystemException` represents a `JCSystem` class related exception. It is also thrown by the `javacard.framework.Applet.register()` methods and by the `AID` class constructor.

These API classes throw JCRE owned instances of `SystemException`.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

See Also:
`JCSystem`, `Applet`, `AID`

Field Summary

static short	**ILLEGAL_AID** This reason code is used by the `javacard.framework.Applet.register()` method to indicate that the input AID parameter is not a legal AID value.
static short	**ILLEGAL_TRANSIENT** This reason code is used to indicate that the request to create a transient object is not allowed in the current applet context.
static short	**ILLEGAL_VALUE** This reason code is used to indicate that one or more input parameters is out of allowed bounds.
static short	**NO_RESOURCE** This reason code is used to indicate that there is insufficient resource in the Card for the request.
static short	**NO_TRANSIENT_SPACE** This reason code is used by the `makeTransient..()` methods to indicate that no room is available in volatile memory for the requested object.

Constructor Summary

SystemException(short reason) Constructs a SystemException.	

Method Summary

static void	**throwIt**(short reason) Throws the JCRE owned instance of `SystemException` with the specified reason.

Methods inherited from class javacard.framework.CardRuntimeException
`getReason, setReason`

Methods inherited from class java.lang.Object
equals

Field Detail

ILLEGAL_VALUE

```
public static final short ILLEGAL_VALUE
```

This reason code is used to indicate that one or more input parameters is out of allowed bounds.

NO_TRANSIENT_SPACE

```
public static final short NO_TRANSIENT_SPACE
```

This reason code is used by the `makeTransient..()` methods to indicate that no room is available in volatile memory for the requested object.

ILLEGAL_TRANSIENT

```
public static final short ILLEGAL_TRANSIENT
```

This reason code is used to indicate that the request to create a transient object is not allowed in the current applet context. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

ILLEGAL_AID

```
public static final short ILLEGAL_AID
```

This reason code is used by the `javacard.framework.Applet.register()` method to indicate that the input AID parameter is not a legal AID value.

NO_RESOURCE

```
public static final short NO_RESOURCE
```

This reason code is used to indicate that there is insufficient resource in the Card for the request.

For example, the Java Card Virtual Machine may `throw` this exception reason when there is insufficient heap space to create a new instance.

Constructor Detail

SystemException

```
public SystemException(short reason)
```

Constructs a SystemException. To conserve on resources use `throwIt()` to use the JCRE owned instance of this class.

Parameters:

`reason` - the reason for the exception.

Method Detail

throwIt

```
public static void throwIt(short reason)
```

Throws the JCRE owned instance of `SystemException` with the specified reason.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Parameters:

`reason` - the reason for the exception.

Throws:

SystemException - always.

javacard.framework
Class TransactionException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--javacard.framework.CardRuntimeException
                          |
                          +--javacard.framework.TransactionException
```

public class **TransactionException**
extends CardRuntimeException

`TransactionException` represents an exception in the transaction subsystem. The methods referred to in this class are in the `JCSystem` class.

The `JCSystem` class and the transaction facility throw JCRE owned instances of `TransactionException`.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

See Also:
`JCSystem`

Field Summary

static short	**BUFFER_FULL** This reason code is used during a transaction to indicate that the commit buffer is full.
static short	**IN_PROGRESS** This reason code is used by the `beginTransaction` method to indicate a transaction is already in progress.
static short	**INTERNAL_FAILURE** This reason code is used during a transaction to indicate an internal JCRE problem (fatal error).
static short	**NOT_IN_PROGRESS** This reason code is used by the `abortTransaction` and `commintTransaction` methods when a transaction is not in progress.

Constructor Summary

TransactionException(short reason) Constructs a TransactionException with the specified reason.

Method Summary

static void	**throwIt**(short reason) Throws the JCRE owned instance of `TransactionException` with the specified reason.

Methods inherited from class javacard.framework.CardRuntimeException
`getReason, setReason`

Methods inherited from class java.lang.Object
`equals`

Field Detail

IN_PROGRESS

```
public static final short IN_PROGRESS
```

This reason code is used by the `beginTransaction` method to indicate a transaction is already in progress.

NOT_IN_PROGRESS

```
public static final short NOT_IN_PROGRESS
```

This reason code is used by the `abortTransaction` and `commintTransaction` methods when a transaction is not in progress.

BUFFER_FULL

```
public static final short BUFFER_FULL
```

This reason code is used during a transaction to indicate that the commit buffer is full.

INTERNAL_FAILURE

```
public static final short INTERNAL_FAILURE
```

This reason code is used during a transaction to indicate an internal JCRE problem (fatal error).

Constructor Detail

TransactionException

```
public TransactionException(short reason)
```

Constructs a TransactionException with the specified reason. To conserve on resources use `throwIt()` to use the JCRE owned instance of this class.

Method Detail

throwIt

```
public static void throwIt(short reason)
```

Throws the JCRE owned instance of `TransactionException` with the specified reason.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Throws:

TransactionException - always.

---

javacard.framework
Class UserException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--javacard.framework.CardException
                    |
                    +--javacard.framework.UserException
```

public class **UserException**
extends CardException

`UserException` represents a User exception. This class also provides a resource-saving mechanism (the `throwIt()` method) for user exceptions by using a JCRE owned instance.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Constructor Summary

`UserException``()` Constructs a `UserException` with reason = 0.
`UserException``(short reason)` Constructs a `UserException` with the specified reason.

Method Summary

`static void`	**`throwIt`**`(short reason)` Throws the JCRE owned instance of `UserException` with the specified reason.

Methods inherited from class javacard.framework.CardException
`getReason, setReason`

Methods inherited from class java.lang.Object
equals

Constructor Detail

UserException

```
public UserException()
```

Constructs a `UserException` with reason = 0. To conserve on resources use `throwIt()` to use the JCRE owned instance of this class.

UserException

```
public UserException(short reason)
```

Constructs a `UserException` with the specified reason. To conserve on resources use `throwIt()` to use the JCRE owned instance of this class.

Parameters:

`reason` - the reason for the exception.

Method Detail

throwIt

```
public static void throwIt(short reason)
                    throws UserException
```

Throws the JCRE owned instance of `UserException` with the specified reason.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Parameters:

`reason` - the reason for the exception.

Throws:

UserException - always.

javacard.framework
Class Util

```
java.lang.Object
  |
  +--javacard.framework.Util
```

public class **Util**
extends Object

The `Util` class contains common utility functions. Some of the methods may be implemented as native functions for performance reasons. All methods in `Util`, class are static methods.

Some methods of `Util` namely `arrayCopy()`, `arrayCopyNonAtomic()`, `arrayFillNonAtomic()` and `setShort()`, refer to the persistence of array objects. The term *persistent* means that arrays and their values persist from one CAD session to the next, indefinitely. The `JCSystem` class is used to control the persistence and transience of objects.

See Also:
`JCSystem`

Method Summary

static byte	**arrayCompare**(byte[] src, short srcOff, byte[] dest, short destOff, short length) Compares an array from the specified source array, beginning at the specified position, with the specified position of the destination array from left to right.
static short	**arrayCopy**(byte[] src, short srcOff, byte[] dest, short destOff, short length) Copies an array from the specified source array, beginning at the specified position, to the specified position of the destination array.
static short	**arrayCopyNonAtomic**(byte[] src, short srcOff, byte[] dest, short destOff, short length) Copies an array from the specified source array, beginning at the specified position, to the specified position of the destination array (non-atomically).
static short	**arrayFillNonAtomic**(byte[] bArray, short bOff, short bLen, byte bValue) Fills the byte array (non-atomically) beginning at the specified position, for the specified length with the specified byte value.
static short	**getShort**(byte[] bArray, short bOff) Concatenates two bytes in a byte array to form a short value.
static short	**makeShort**(byte b1, byte b2) Concatenates the two parameter bytes to form a short value.
static short	**setShort**(byte[] bArray, short bOff, short sValue) Deposits the short value as two successive bytes at the specified offset in the byte array.

Methods inherited from class java.lang.Object
equals

Method Detail

arrayCopy

```
public static final short arrayCopy(byte[] src,
                                    short srcOff,
                                    byte[] dest,
                                    short destOff,
```

```
                short length)
        throws IndexOutOfBoundsException,
                NullPointerException,
                TransactionException
```

Copies an array from the specified source array, beginning at the specified position, to the specified position of the destination array.

Notes:

- *If* `srcOff` *or* `destOff` *or* `length` *parameter is negative an* `IndexOutOfBoundsException` *exception is thrown.*
- *If* `srcOff+length` *is greater than* `src.length`*, the length of the* `src` *array a* `IndexOutOfBoundsException` *exception is thrown and no copy is performed.*
- *If* `destOff+length` *is greater than* `dest.length`*, the length of the* `dest` *array an* `IndexOutOfBoundsException` *exception is thrown and no copy is performed.*
- *If* `src` *or* `dest` *parameter is* `null` *a* `NullPointerException` *exception is thrown.*
- *If the* `src` *and* `dest` *arguments refer to the same array object, then the copying is performed as if the components at positions* `srcOff` *through* `srcOff+length-1` *were first copied to a temporary array with length components and then the contents of the temporary array were copied into positions* `destOff` *through* `destOff+length-1` *of the argument array.*
- *If the destination array is persistent, the entire copy is performed atomically.*
- *The copy operation is subject to atomic commit capacity limitations. If the commit capacity is exceeded, no copy is performed and a* `TransactionException` *exception is thrown.*

Parameters:

`src` - source byte array.
`srcOff` - offset within source byte array to start copy from.
`dest` - destination byte array.
`destOff` - offset within destination byte array to start copy into.
`length` - byte length to be copied.

Returns:

`destOff+length`

Throws:

IndexOutOfBoundsException - - if copying would cause access of data outside array bounds.
NullPointerException - - if either `src` or `dest` is `null`.
TransactionException - - if copying would cause the commit capacity to be exceeded.

See Also:

`JCSystem.getUnusedCommitCapacity()`

---

arrayCopyNonAtomic

```
public static final short arrayCopyNonAtomic(byte[] src,
                                             short srcOff,
                                             byte[] dest,
                                             short destOff,
                                             short length)
                                      throws IndexOutOfBoundsException,
                                             NullPointerException
```

Copies an array from the specified source array, beginning at the specified position, to the specified position of the destination array (non-atomically).

This method does not use the transaction facility during the copy operation even if a transaction is in progress. Thus, this method is suitable for use only when the contents of the destination array can be left in a partially modified state in the event of a power loss in the middle of the copy operation.

Notes:

- *If* `srcOff` *or* `destOff` *or* `length` *parameter is negative an* `IndexOutOfBoundsException` *exception is thrown.*
- *If* `srcOff+length` *is greater than* `src.length`*, the length of the* `src` *array a* `IndexOutOfBoundsException` *exception is thrown and no copy is performed.*
- *If* `destOff+length` *is greater than* `dest.length`*, the length of the* `dest` *array an* `IndexOutOfBoundsException` *exception is thrown and no copy is performed.*
- *If* `src` *or* `dest` *parameter is* `null` *a* `NullPointerException` *exception is thrown.*
- *If the* `src` *and* `dest` *arguments refer to the same array object, then the copying is performed as if the components at positions* `srcOff` *through* `srcOff+length-1` *were first copied to a temporary array with length components and then the contents of the temporary array were copied into positions* `destOff` *through* `destOff+length-1` *of the argument array.*
- *If power is lost during the copy operation and the destination array is persistent, a partially changed destination array could result.*
- *The copy* `length` *parameter is not constrained by the atomic commit capacity limitations.*

Parameters:

`src` - source byte array.
`srcOff` - offset within source byte array to start copy from.
`dest` - destination byte array.
`destOff` - offset within destination byte array to start copy into.
`length` - byte length to be copied.

Returns:

`destOff+length`

Throws:

IndexOutOfBoundsException - - if copying would cause access of data outside array bounds.
NullPointerException - - if either `src` or `dest` is `null`.

See Also:

`JCSystem.getUnusedCommitCapacity()`

---

arrayFillNonAtomic

```
public static final short arrayFillNonAtomic(byte[] bArray,
                                              short bOff,
                                              short bLen,
                                              byte bValue)
                                       throws IndexOutOfBoundsException,
                                              NullPointerException
```

Fills the byte array (non-atomically) beginning at the specified position, for the specified length with the specified byte value.

This method does not use the transaction facility during the fill operation even if a transaction is in progress. Thus, this method is suitable for use only when the contents of the byte array can be left in a partially filled state in the event of a power loss in the middle of the fill operation.

Notes:

- *If* `bOff` *or* `bLen` *parameter is negative an* `IndexOutOfBoundsException` *exception is thrown.*
- *If* `bOff+bLen` *is greater than* `bArray.length`*, the length of the* `bArray` *array an* `IndexOutOfBoundsException` *exception is thrown.*
- *If* `bArray` *parameter is* `null` *a* `NullPointerException` *exception is thrown.*
- *If power is lost during the copy operation and the byte array is persistent, a partially changed byte array could result.*
- *The* `bLen` *parameter is not constrained by the atomic commit capacity limitations.*

Parameters:

`bArray` - the byte array.
`bOff` - offset within byte array to start filling bValue into.
`bLen` - byte length to be filled.
`bValue` - the value to fill the byte array with.

Returns:

`bOff+bLen`

Throws:

IndexOutOfBoundsException - - if the fill operation would cause access of data outside array bounds.
NullPointerException - - if bArray is `null`

See Also:

`JCSystem.getUnusedCommitCapacity()`

---

arrayCompare

```
public static final byte arrayCompare(byte[] src,
                                       short srcOff,
                                       byte[] dest,
                                       short destOff,
                                       short length)
                                throws IndexOutOfBoundsException,
                                       NullPointerException
```

Compares an array from the specified source array, beginning at the specified position, with the specified position of the destination array from left to right. Returns the ternary result of the comparison : less than(-1), equal(0) or greater than(1).

Notes:

- *If* `srcOff` *or* `destOff` *or* `length` *parameter is negative an* `IndexOutOfBoundsException` *exception is thrown.*

- *If* `srcOff+length` *is greater than* `src.length`*, the length of the* `src` *array a* `IndexOutOfBoundsException` *exception is thrown.*
- *If* `destOff+length` *is greater than* `dest.length`*, the length of the* `dest` *array an* `IndexOutOfBoundsException` *exception is thrown.*
- *If* `src` *or* `dest` *parameter is* `null` *a* `NullPointerException` *exception is thrown.*

Parameters:

`src` - source byte array.
`srcOff` - offset within source byte array to start compare.
`dest` - destination byte array.
`destOff` - offset within destination byte array to start compare.
`length` - byte length to be compared.

Returns:

the result of the comparison as follows:

- `0` if identical
- `-1` if the first miscomparing byte in source array is less than that in destination array,
- `1` if the first miscomparing byte in source array is greater that that in destination array.

Throws:

IndexOutOfBoundsException - - if comparing all bytes would cause access of data outside array bounds.
NullPointerException - - if either `src` or `dest` is `null`.

---

makeShort

```
public static final short makeShort(byte b1,
                                    byte b2)
```

Concatenates the two parameter bytes to form a short value.

Parameters:

`b1` - the first byte (high order byte).
`b2` - the second byte (low order byte).

Returns:

the short value - the concatenated result

---

getShort

```
public static final short getShort(byte[] bArray,
                                   short bOff)
```

Concatenates two bytes in a byte array to form a short value.

Parameters:

`bArray` - byte array.
`bOff` - offset within byte array containing first byte (the high order byte).

Returns:

the short value - the concatenated result

setShort

```
public static final short setShort(byte[] bArray,
                                   short bOff,
                                   short sValue)
                            throws TransactionException
```

Deposits the short value as two successive bytes at the specified offset in the byte array.

Parameters:

`bArray` - byte array.

`bOff` - offset within byte array to deposit the first byte (the high order byte).

`sValue` - the short value to set into array.

Returns:

`bOff+2`

Note:

- *If the byte array is persistent, this operation is performed atomically. If the commit capacity is exceeded, no operation is performed and a* `TransactionException` *exception is thrown.*

Throws:

TransactionException - - if the operation would cause the commit capacity to be exceeded.

See Also:

`JCSystem.getUnusedCommitCapacity()`

Package javacard.security

Provides the classes and interfaces for the Java Card security framework.

See:

Description

Interface Summary	
DESKey	`DESKey` contains an 8/16/24 byte key for single/2 key triple DES/3 key triple DES operations.
DSAKey	The DSAKey interface is the base interface for the DSA algorithms private and public key implementaions.
DSAPrivateKey	The `DSAPrivateKey` interface is used to sign data using the DSA algorithm.
DSAPublicKey	The `DSAPublicKey` interface is used to verify signatures on signed data using the DSA algorithm.
Key	The `Key` interface is the base interface for all keys.
PrivateKey	The `PrivateKey` class is the base class for private keys used in asymmetric algorithms.
PublicKey	The `PublicKey` class is the base class for public keys used in asymmetric algorithms.
RSAPrivateCrtKey	The `RSAPrivateCrtKey` interface is used to sign data using the RSA algorithm in its Chinese Remainder Theorem form.
RSAPrivateKey	The `RSAPrivateKey` class is used to sign data using the RSA algorithm in its modulus/exponent form.
RSAPublicKey	The `RSAPublicKey` is used to verify signatures on signed data using the RSA algorithm.
SecretKey	The `SecretKey` class is the base interface for keys used in symmetric alogrightms (e.g. DES).

Class Summary	
KeyBuilder	The `KeyBuilder` class is a key object factory.
MessageDigest	The `MessageDigest` class is the base class for hashing algorthims.
RandomData	The `RandomData` abstract class is the base class for random number generation.
Signature	The `Signature` class is the base class for Signature algorthims.

Exception Summary	
CryptoException	`CryptoException` represents a cryptography-related exception.

Package javacard.security Description

Provides the classes and interfaces for the Java Card security framework.

javacard.security
Class CryptoException

```
java.lang.Object
  |
  +--java.lang.Throwable
        |
        +--java.lang.Exception
              |
              +--java.lang.RuntimeException
                    |
                    +--javacard.framework.CardRuntimeException
                          |
                          +--javacard.security.CryptoException
```

public class **CryptoException**
extends CardRuntimeException

`CryptoException` represents a cryptography-related exception.

The API classes throw JCRE owned instances of `SystemException`.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components.

See Also:
`KeyBuilder`, `MessageDigest`, `Signature`, `RandomData`, `Cipher`

Field Summary

static short	**ILLEGAL_USE** This reason code is used to indicate that the signature or cipher algorithm does not pad the incoming message and the input message is not block aligned.
static short	**ILLEGAL_VALUE** This reason code is used to indicate that one or more input parameters is out of allowed bounds.
static short	**INVALID_INIT** This reason code is used to indicate that the signature or cipher object has not been correctly initialized for the requested operation.
static short	**NO_SUCH_ALGORITHM** This reason code is used to indicate that the requested algorithm or key type is not supported.
static short	**UNINITIALIZED_KEY** This reason code is used to indicate that the key is uninitialized.

Constructor Summary

CryptoException(short reason) Constructs a CryptoException with the specified reason.

Method Summary

static void	**throwIt**(short reason) Throws the JCRE owned instance of CryptoException with the specified reason.

Methods inherited from class javacard.framework.CardRuntimeException
getReason, setReason

Methods inherited from class java.lang.Object
equals

Field Detail

ILLEGAL_VALUE

```
public static final short ILLEGAL_VALUE
```

This reason code is used to indicate that one or more input parameters is out of allowed bounds.

UNINITIALIZED_KEY

```
public static final short UNINITIALIZED_KEY
```

This reason code is used to indicate that the key is uninitialized.

NO_SUCH_ALGORITHM

```
public static final short NO_SUCH_ALGORITHM
```

This reason code is used to indicate that the requested algorithm or key type is not supported.

INVALID_INIT

```
public static final short INVALID_INIT
```

This reason code is used to indicate that the signature or cipher object has not been correctly initialized for the requested operation.

ILLEGAL_USE

```
public static final short ILLEGAL_USE
```

This reason code is used to indicate that the signature or cipher algorithm does not pad the incoming message and the input message is not block aligned.

Constructor Detail

CryptoException

```
public CryptoException(short reason)
```

Constructs a `CryptoException` with the specified reason. To conserve on resources use `throwIt()` to use the JCRE owned instance of this class.

Parameters:

`reason` - the reason for the exception.

Method Detail

throwIt

```
public static void throwIt(short reason)
```

Throws the JCRE owned instance of `CryptoException` with the specified reason.

JCRE owned instances of exception classes are temporary JCRE Entry Point Objects and can be accessed from any applet context. References to these temporary objects cannot be stored in class variables or instance variables or array components. See *Java Card Runtime Environment (JCRE) 2.1 Specification* for details.

Parameters:

`reason` - the reason for the exception.

Throws:

CryptoException - always.

javacard.security
Interface DESKey

public abstract interface **DESKey**
extends SecretKey

`DESKey` contains an 8/16/24 byte key for single/2 key triple DES/3 key triple DES operations.

When the key data is set, the key is initialized and ready for use.

See Also:
`KeyBuilder`, `Signature`, `Cipher`, `KeyEncryption`

Method Summary

byte	**`getKey`**`(byte[] keyData, short kOff)` Returns the `Key` data in plain text.
void	**`setKey`**`(byte[] keyData, short kOff)` Sets the `Key` data.

Methods inherited from interface javacard.security.Key
`clearKey, getSize, getType, isInitialized`

Method Detail

setKey

```
public void setKey(byte[] keyData,
                   short kOff)
            throws CryptoException
```

Sets the `Key` data. The plaintext length of input key data is 8 bytes for DES, 16 bytes for 2 key triple DES and 24 bytes for 3 key triple DES. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input key data is copied into the internal representation.

Parameters:

`keyData` - byte array containing key initialization data
`kOff` - offset within keyData to start

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input key data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`, `keyData` *is decrypted using the* `Cipher` *object.*

---

getKey

```
public byte getKey(byte[] keyData,
                   short kOff)
```

Returns the `Key` data in plain text. The length of output key data is 8 bytes for DES, 16 bytes for 2 key triple DES and 24 bytes for 3 key triple DES. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`keyData` - byte array to return key data

`kOff` - offset within `keyData` to start.

Returns:

the byte length of the key data returned.

---

javacard.security
Interface DSAKey

All Known Subinterfaces:
DSAPrivateKey, DSAPublicKey

public abstract interface **DSAKey**

The DSAKey interface is the base interface for the DSA algorithms private and public key implementaions. A DSA private key implementation must also implement the `DSAPrivateKey` interface methods. A DSA public key implementation must also implement the `DSAPublicKey` interface methods.

When all four components of the key (X or Y,P,Q,G) are set, the key is initialized and ready for use.

See Also:
`DSAPublicKey`, `DSAPrivateKey`, `KeyBuilder`, `Signature`, `KeyEncryption`

Method Summary

`short`	**`getG`**`(byte[] buffer, short offset)` Returns the subprime parameter value of the key in plain text.
`short`	**`getP`**`(byte[] buffer, short offset)` Returns the base parameter value of the key in plain text.
`short`	**`getQ`**`(byte[] buffer, short offset)` Returns the prime parameter value of the key in plain text.
`void`	**`setG`**`(byte[] buffer, short offset, short length)` Sets the subprime parameter value of the key.
`void`	**`setP`**`(byte[] buffer, short offset, short length)` Sets the base parameter value of the key.
`void`	**`setQ`**`(byte[] buffer, short offset, short length)` Sets the prime parameter value of the key.

Method Detail

setP

```
public void setP(byte[] buffer,
                 short offset,
                 short length)
          throws CryptoException
```

Sets the base parameter value of the key. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input base parameter data is copied into the internal representation.

Parameters:

`buffer` - the input buffer

`offset` - the offset into the input buffer at which the base parameter value begins

`length` - the length of the base parameter value

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input parameter data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the base parameter value is decrypted using the* `Cipher` *object.*

---

setQ

```
public void setQ(byte[] buffer,
                 short offset,
                 short length)
          throws CryptoException
```

Sets the prime parameter value of the key. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input prime parameter data is copied into the internal representation.

Parameters:

`buffer` - the input buffer

`offset` - the offset into the input buffer at which the prime parameter value begins

`length` - the length of the prime parameter value

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input parameter data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the prime parameter value is decrypted using the* `Cipher` *object.*

setG

```
public void setG(byte[] buffer,
                 short offset,
                 short length)
          throws CryptoException
```

Sets the subprime parameter value of the key. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input subprime parameter data is copied into the internal representation.

Parameters:

`buffer` - the input buffer

`offset` - the offset into the input buffer at which the subprime parameter value begins

`length` - the length of the subprime parameter value

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input parameter data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the subprime parameter value is decrypted using the* `Cipher` *object.*

---

getP

```
public short getP(byte[] buffer,
                  short offset)
```

Returns the base parameter value of the key in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer

`offset` - the offset into the output buffer at which the base parameter value starts

Returns:

the byte length of the base parameter value returned

---

getQ

```
public short getQ(byte[] buffer,
                  short offset)
```

Returns the prime parameter value of the key in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer

`offset` - the offset into the output buffer at which the prime parameter value begins

Returns:

the byte length of the prime parameter value returned

---

getG

```
public short getG(byte[] buffer,
                  short offset)
```

Returns the subprime parameter value of the key in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer

`offset` - the offset into the output buffer at which the subprime parameter value begins

Returns:

the byte length of the subprime parameter value returned

---

javacard.security
Interface DSAPrivateKey

public abstract interface **DSAPrivateKey**
extends PrivateKey, DSAKey

The `DSAPrivateKey` interface is used to sign data using the DSA algorithm. An implementation of `DSAPrivateKey` interface must also implement the `DSAKey` interface methods.

When all four components of the key (X,P,Q,G) are set, the key is initialized and ready for use.

See Also:
`DSAPublicKey`, `KeyBuilder`, `Signature`, `KeyEncryption`

Method Summary

short	**getX**(byte[] buffer, short offset) Returns the value of the key in plain text.
void	**setX**(byte[] buffer, short offset, short length) Sets the value of the key.

Methods inherited from interface javacard.security.DSAKey

`getG, getP, getQ, setG, setP, setQ`

Methods inherited from interface javacard.security.Key

`clearKey, getSize, getType, isInitialized`

Method Detail

setX

```
public void setX(byte[] buffer,
                 short offset,
                 short length)
          throws CryptoException
```

Sets the value of the key. When the base, prime and subprime parameters are intialized and the key value is set, the key is ready for use. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input key data is copied into the internal representation.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer at which the modulus value begins
`length` - the length of the modulus

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input key data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the key value is decrypted using the* `Cipher` *object.*

---

getX

```
public short getX(byte[] buffer,
                  short offset)
```

Returns the value of the key in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer
`offset` - the offset into the output buffer at which the key value starts

Returns:

the byte length of the key value returned

---

javacard.security
Interface DSAPublicKey

public abstract interface **DSAPublicKey**
extends PublicKey, DSAKey

The `DSAPublicKey` interface is used to verify signatures on signed data using the DSA algorithm. An implementation of `DSAPublicKey` interface must also implement the `DSAKey` interface methods.

When all four components of the key (Y,P,Q,G) are set, the key is initialized and ready for use.

See Also:
`DSAPrivateKey`, `KeyBuilder`, `Signature`, `KeyEncryption`

Method Summary

`short`	**`getY`**`(byte[] buffer, short offset)` Returns the value of the key in plain text.
`void`	**`setY`**`(byte[] buffer, short offset, short length)` Sets the value of the key.

Methods inherited from interface javacard.security.DSAKey
`getG, getP, getQ, setG, setP, setQ`

Methods inherited from interface javacard.security.Key
`clearKey, getSize, getType, isInitialized`

Method Detail

setY

```
public void setY(byte[] buffer,
                 short offset,
                 short length)
          throws CryptoException
```

Sets the value of the key. When the base, prime and subprime parameters are intialized and the key value is set, the key is ready for use. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input key data is copied into the internal representation.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer at which the key value begins
`length` - the length of the key value

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input key data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the key value is decrypted using the* `Cipher` *object.*

---

getY

```
public short getY(byte[] buffer,
                  short offset)
```

Returns the value of the key in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer
`offset` - the offset into the input buffer at which the key value starts

Returns:

the byte length of the key value returned

---

javacard.security
Interface Key

All Known Subinterfaces:
DESKey, DSAPrivateKey, DSAPublicKey, PrivateKey, PublicKey, RSAPrivateCrtKey, RSAPrivateKey, RSAPublicKey, SecretKey

public abstract interface **Key**

The `Key` interface is the base interface for all keys.

See Also:
`KeyBuilder`

Method Summary

`void`	**`clearKey`**`()` Clears the key and sets its initialized state to false.
`short`	**`getSize`**`()` Returns the key size in number of bits.
`byte`	**`getType`**`()` Returns the key interface type.
`boolean`	**`isInitialized`**`()` Reports the initialized state of the key.

Method Detail

isInitialized

`public boolean` **`isInitialized`**`()`

Reports the initialized state of the key. Keys must be initialized before being used.

A `Key` object sets its initialized state to true only when all the associated set methods have been invoked at least once since the time the initialized state was set to false.

A newly created `Key` object sets its initialized state to false. Invocation of the `clearKey()` method sets the initialized state to false. A key with transient key data sets its initialized state to false on the associated clear events.

Returns:
`true` if the key has been initialized.

---

clearKey

```
public void clearKey()
```

Clears the key and sets its initialized state to false.

---

getType

```
public byte getType()
```

Returns the key interface type.
Returns:
the key interface type.

See Also:
`KeyBuilder`

---

getSize

```
public short getSize()
```

Returns the key size in number of bits.
Returns:
the key size in number of bits.

---

javacard.security
Class KeyBuilder

```
java.lang.Object
  |
  +--javacard.security.KeyBuilder
```

public class **KeyBuilder**
extends Object

The `KeyBuilder` class is a key object factory.

Field Summary

static short	**LENGTH_DES** DES Key Length `LENGTH_DES` = 64.
static short	**LENGTH_DES3_2KEY** DES Key Length `LENGTH_DES3_2KEY` = 128.
static short	**LENGTH_DES3_3KEY** DES Key Length `LENGTH_DES3_3KEY` = 192.
static short	**LENGTH_DSA_1024** DSA Key Length `LENGTH_DSA_1024` = 1024.
static short	**LENGTH_DSA_512** DSA Key Length `LENGTH_DSA_512` = 512.
static short	**LENGTH_DSA_768** DSA Key Length `LENGTH_DSA_768` = 768.
static short	**LENGTH_RSA_1024** RSA Key Length `LENGTH_RSA_1024` = 1024.
static short	**LENGTH_RSA_2048** RSA Key Length `LENGTH_RSA_2048` = 2048.
static short	**LENGTH_RSA_512** RSA Key Length `LENGTH_RSA_512` = 512.
static short	**LENGTH_RSA_768** RSA Key Length `LENGTH_RSA_768` = 768.
static byte	**TYPE_DES** `Key` object which implements interface type `DESKey` with persistent key data.

static byte	**TYPE_DES_TRANSIENT_DESELECT** Key object which implements interface type DESKey with CLEAR_ON_DESELECT transient key data.
static byte	**TYPE_DES_TRANSIENT_RESET** Key object which implements interface type DESKey with CLEAR_ON_RESET transient key data.
static byte	**TYPE_DSA_PRIVATE** Key object which implements the interface type DSAPrivateKey for the DSA algorithm.
static byte	**TYPE_DSA_PUBLIC** Key object which implements the interface type DSAPublicKey for the DSA algorithm.
static byte	**TYPE_RSA_CRT_PRIVATE** Key object which implements interface type RSAPrivateCrtKey which uses Chinese Remainder Theorem.
static byte	**TYPE_RSA_PRIVATE** Key object which implements interface type RSAPrivateKey which uses modulus/exponent form.
static byte	**TYPE_RSA_PUBLIC** Key object which implements interface type RSAPublicKey.

Method Summary

static Key	**buildKey**(byte keyType, short keyLength, boolean keyEncryption) Creates cryptographic keys for signature and cipher algorithms.

Methods inherited from class java.lang.Object
equals

Field Detail

TYPE_DES_TRANSIENT_RESET

`public static final byte` **`TYPE_DES_TRANSIENT_RESET`**

`Key` object which implements interface type `DESKey` with CLEAR_ON_RESET transient key data.

This `Key` object implicitly performs a `clearKey()` on power on or card reset.

TYPE_DES_TRANSIENT_DESELECT

`public static final byte` **`TYPE_DES_TRANSIENT_DESELECT`**

`Key` object which implements interface type `DESKey` with CLEAR_ON_DESELECT transient key data.

This `Key` object implicitly performs a `clearKey()` on power on, card reset and applet deselection.

TYPE_DES

`public static final byte` **`TYPE_DES`**

`Key` object which implements interface type `DESKey` with persistent key data.

TYPE_RSA_PUBLIC

`public static final byte` **`TYPE_RSA_PUBLIC`**

`Key` object which implements interface type `RSAPublicKey`.

TYPE_RSA_PRIVATE

`public static final byte` **`TYPE_RSA_PRIVATE`**

`Key` object which implements interface type `RSAPrivateKey` which uses modulus/exponent form.

TYPE_RSA_CRT_PRIVATE

`public static final byte` **`TYPE_RSA_CRT_PRIVATE`**

`Key` object which implements interface type `RSAPrivateCrtKey` which uses Chinese Remainder Theorem.

TYPE_DSA_PUBLIC

`public static final byte` **`TYPE_DSA_PUBLIC`**

`Key` object which implements the interface type `DSAPublicKey` for the DSA algorithm.

TYPE_DSA_PRIVATE

`public static final byte` **`TYPE_DSA_PRIVATE`**

`Key` object which implements the interface type `DSAPrivateKey` for the DSA algorithm.

LENGTH_DES

`public static final short` **`LENGTH_DES`**

DES Key Length `LENGTH_DES` = 64.

LENGTH_DES3_2KEY

`public static final short` **`LENGTH_DES3_2KEY`**

DES Key Length `LENGTH_DES3_2KEY` = 128.

LENGTH_DES3_3KEY

`public static final short` **`LENGTH_DES3_3KEY`**

DES Key Length `LENGTH_DES3_3KEY` = 192.

LENGTH_RSA_512

`public static final short` **`LENGTH_RSA_512`**

RSA Key Length `LENGTH_RSA_512` = 512.

LENGTH_RSA_768

`public static final short` **`LENGTH_RSA_768`**

RSA Key Length `LENGTH_RSA_768` = 768.

LENGTH_RSA_1024

```
public static final short LENGTH_RSA_1024
```

RSA Key Length `LENGTH_RSA_1024` = 1024.

LENGTH_RSA_2048

```
public static final short LENGTH_RSA_2048
```

RSA Key Length `LENGTH_RSA_2048` = 2048.

LENGTH_DSA_512

```
public static final short LENGTH_DSA_512
```

DSA Key Length `LENGTH_DSA_512` = 512.

LENGTH_DSA_768

```
public static final short LENGTH_DSA_768
```

DSA Key Length `LENGTH_DSA_768` = 768.

LENGTH_DSA_1024

```
public static final short LENGTH_DSA_1024
```

DSA Key Length `LENGTH_DSA_1024` = 1024.

Method Detail

buildKey

```
public static Key buildKey(byte keyType,
                           short keyLength,
                           boolean keyEncryption)
                    throws CryptoException
```

Creates cryptographic keys for signature and cipher algorithms. Instances created by this method may be the only key objects used to initialize instances of `Signature` and `Cipher`. Note that the object returned must be cast to their appropriate key type interface.

Parameters:

`keyType` - the type of key to be generated. Valid codes listed in TYPE.. constants.
`keyLength` - the key size in bits. The valid key bit lengths are key type dependent. See above.
`keyEncryption` - if `true` this boolean requests a key implementation which implements the `javacardx.cipher.KeyEncryption` interface.

Returns:

the key object instance of the requested key type, length and encrypted access.

Throws:

CryptoException - with the following reason codes:

- `CryptoException.NO_SUCH_ALGORITHM` if the requested algorithm associated with the specified type, size of key and key encryption interface is not supported.

---

javacard.security
Class MessageDigest

```
java.lang.Object
  |
  +--javacard.security.MessageDigest
```

public abstract class **MessageDigest**
extends Object

The `MessageDigest` class is the base class for hashing algorthims. Implementations of MessageDigest algorithms must extend this class and implement all the abstract methods.

Field Summary

static byte	**ALG_MD5** Message Digest algorithm MD5.
static byte	**ALG_RIPEMD160** Message Digest algorithm RIPE MD-160.
static byte	**ALG_SHA** Message Digest algorithm SHA.

Constructor Summary

protected	**MessageDigest**() Protected Constructor

Method Summary	
abstract short	**doFinal**(byte[] inBuff, short inOffset, short inLength, byte[] outBuff, short outOffset) Generates a hash of all/last input data.
abstract byte	**getAlgorithm**() Gets the Message digest algorithm.
static MessageDigest	**getInstance**(byte algorithm, boolean externalAccess) Creates a MessageDigest object instance of the selected algorithm.
abstract byte	**getLength**() Returns the byte length of the hash.
abstract void	**update**(byte[] inBuff, short inOffset, short inLength) Accumulates a hash of the input data.

Methods inherited from class java.lang.Object
equals

Field Detail

ALG_SHA

```
public static final byte ALG_SHA
```

Message Digest algorithm SHA.

ALG_MD5

```
public static final byte ALG_MD5
```

Message Digest algorithm MD5.

ALG_RIPEMD160

```
public static final byte ALG_RIPEMD160
```

Message Digest algorithm RIPE MD-160.

Constructor Detail

MessageDigest

```
protected MessageDigest()
```

Protected Constructor

Method Detail

getInstance

```
public static final MessageDigest getInstance(byte algorithm,
                                               boolean externalAccess)
                                        throws CryptoException
```

Creates a `MessageDigest` object instance of the selected algorithm.

Parameters:

`algorithm` - the desired message digest algorithm. Valid codes listed in ALG_.. constants. See above.

`externalAccess` - if `true` indicates that the instance will be shared among multiple applet instances and that the `MessageDigest` instance will also be accessed (via a `Shareable` interface) when the owner of the `MessageDigest` instance is not the currently selected applet.

Returns:

the `MessageDigest` object instance of the requested algorithm.

Throws:

CryptoException - with the following reason codes:

- `CryptoException.NO_SUCH_ALGORITHM` if the requested algorithm is not supported.

---

getAlgorithm

```
public abstract byte getAlgorithm()
```

Gets the Message digest algorithm.

Returns:

the algorithm code defined above.

---

getLength

```
public abstract byte getLength()
```

Returns the byte length of the hash.

Returns:

hash length

---

doFinal

```
public abstract short doFinal(byte[] inBuff,
                              short inOffset,
                              short inLength,
                              byte[] outBuff,
                              short outOffset)
```

Generates a hash of all/last input data. Completes and returns the hash computation after performing final operations such as padding. The `MessageDigest` object is reset after this call is made.

The input and output buffer data may overlap.

Parameters:

`inBuff` - the input buffer of data to be hashed
`inOffset` - the offset into the input buffer at which to begin hash generation
`inLength` - the byte length to hash
`outBuff` - the output buffer, may be the same as the input buffer
`outOffset` - the offset into the output buffer where the resulting hash value begins

Returns:

number of bytes of hash output in `outBuff`

---

update

```
public abstract void update(byte[] inBuff,
                            short inOffset,
                            short inLength)
```

Accumulates a hash of the input data. When this method is used temporary storage of intermediate results is required. This method should only be used if all the input data required for the hash is not available in one byte array. The doFinal() method is recommended whenever possible.

Parameters:

`inBuff` - the input buffer of data to be hashed
`inOffset` - the offset into the input buffer at which to begin hash generation
`inLength` - the byte length to hash

See Also:

`doFinal(byte[], short, short, byte[], short)`

javacard.security
Interface PrivateKey

All Known Subinterfaces:
DSAPrivateKey, RSAPrivateCrtKey, RSAPrivateKey

public abstract interface **PrivateKey**
extends Key

The `PrivateKey` class is the base class for private keys used in asymmetric algorithms.

Methods inherited from interface javacard.security.Key
`clearKey, getSize, getType, isInitialized`

javacard.security
Interface PublicKey

All Known Subinterfaces:
DSAPublicKey, RSAPublicKey

public abstract interface **PublicKey**
extends Key

The `PublicKey` class is the base class for public keys used in asymmetric algorithms.

Methods inherited from interface javacard.security.Key
`clearKey, getSize, getType, isInitialized`

javacard.security
Interface RSAPrivateCrtKey

public abstract interface **RSAPrivateCrtKey**
extends PrivateKey

The `RSAPrivateCrtKey` interface is used to sign data using the RSA algorithm in its Chinese Remainder Theorem form. It may also be used by the `javacardx.crypto.Cipher` class to encrypt/decrypt messages.

Let $S = m^d \bmod n$, where m is the data to be signed, d is the private key exponent, and n is private key modulus composed of two prime numbers p and q. The following names are used in the initializer methods in this interface:

P, the prime factor p
Q, the prime factor q.
PQ = $q^{-1} \bmod p$
DP1 = $d \bmod (p - 1)$
DQ1 = $d \bmod (q - 1)$

When all five components (P,Q,PQ,DP1,DQ1) of the key are set, the key is initialized and ready for use.

See Also:
`RSAPrivateKey`, `RSAPublicKey`, `KeyBuilder`, `Signature`, `Cipher`, `KeyEncryption`

Method Summary

short	**getDP1**(byte[] buffer, short offset) Returns the value of the DP1 parameter in plain text.
short	**getDQ1**(byte[] buffer, short offset) Returns the value of the DQ1 parameter in plain text.
short	**getP**(byte[] buffer, short offset) Returns the value of the P parameter in plain text.
short	**getPQ**(byte[] buffer, short offset) Returns the value of the PQ parameter in plain text.
short	**getQ**(byte[] buffer, short offset) Returns the value of the Q parameter in plain text.
void	**setDP1**(byte[] buffer, short offset, short length) Sets the value of the DP1 parameter.
void	**setDQ1**(byte[] buffer, short offset, short length) Sets the value of the DQ1 parameter.
void	**setP**(byte[] buffer, short offset, short length) Sets the value of the P parameter.
void	**setPQ**(byte[] buffer, short offset, short length) Sets the value of the PQ parameter.
void	**setQ**(byte[] buffer, short offset, short length) Sets the value of the Q parameter.

Methods inherited from interface javacard.security.Key

clearKey, getSize, getType, isInitialized

Method Detail

setP

```
public void setP(byte[] buffer,
                 short offset,
                 short length)
          throws CryptoException
```

Sets the value of the P parameter. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input P parameter data is copied into the internal representation.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer at which the parameter value begins
`length` - the length of the parameter

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input parameter data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the P parameter value is decrypted using the* `Cipher` *object.*

---

setQ

```
public void setQ(byte[] buffer,
                 short offset,
                 short length)
          throws CryptoException
```

Sets the value of the Q parameter. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input Q parameter data is copied into the internal representation.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer at which the parameter value begins
`length` - the length of the parameter

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input parameter data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the Q parameter value is decrypted using the* `Cipher` *object.*

---

setDP1

```
public void setDP1(byte[] buffer,
                   short offset,
                   short length)
            throws CryptoException
```

Sets the value of the DP1 parameter. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input DP1 parameter data is copied into the internal representation.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer at which the parameter value begins
`length` - the length of the parameter

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input parameter data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the DP1 parameter value is decrypted using the* `Cipher` *object.*

---

setDQ1

```
public void setDQ1(byte[] buffer,
                   short offset,
                   short length)
            throws CryptoException
```

Sets the value of the DQ1 parameter. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input DQ1 parameter data is copied into the internal representation.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer at which the parameter value begins
`length` - the length of the parameter

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input parameter data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the DQ1 parameter value is decrypted using the* `Cipher` *object.*

setPQ

```
public void setPQ(byte[] buffer,
                  short offset,
                  short length)
           throws CryptoException
```

Sets the value of the PQ parameter. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input PQ parameter data is copied into the internal representation.

Parameters:

`buffer` - the input buffer

`offset` - the offset into the input buffer at which the parameter value begins

`length` - the length of the parameter

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input parameter data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the PQ parameter value is decrypted using the* `Cipher` *object.*

---

getP

```
public short getP(byte[] buffer,
                  short offset)
```

Returns the value of the P parameter in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer

`offset` - the offset into the output buffer at which the parameter value begins

Returns:

the byte length of the P parameter value returned

---

getQ

```
public short getQ(byte[] buffer,
                  short offset)
```

Returns the value of the Q parameter in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer

`offset` - the offset into the output buffer at which the parameter value begins

Returns:

the byte length of the Q parameter value returned

---

getDP1

```
public short getDP1(byte[] buffer,
                    short offset)
```

Returns the value of the DP1 parameter in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer

`offset` - the offset into the output buffer at which the parameter value begins

Returns:

the byte length of the DP1 parameter value returned

---

getDQ1

```
public short getDQ1(byte[] buffer,
                    short offset)
```

Returns the value of the DQ1 parameter in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer

`offset` - the offset into the output buffer at which the parameter value begins

Returns:

the byte length of the DQ1 parameter value returned

---

getPQ

```
public short getPQ(byte[] buffer,
                   short offset)
```

Returns the value of the PQ parameter in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer

`offset` - the offset into the output buffer at which the parameter value begins

Returns:

the byte length of the PQ parameter value returned

javacard.security
Interface RSAPrivateKey

public abstract interface **RSAPrivateKey**
extends PrivateKey

The `RSAPrivateKey` class is used to sign data using the RSA algorithm in its modulus/exponent form. It may also be used by the `javacardx.crypto.Cipher` class to encrypt/decrypt messages.

When both the modulus and exponent of the key are set, the key is initialized and ready for use.

See Also:
`RSAPublicKey`, `RSAPrivateCrtKey`, `KeyBuilder`, `Signature`, `Cipher`, `KeyEncryption`

Method Summary

`short`	**`getExponent`**`(byte[] buffer, short offset)` Returns the private exponent value of the key in plain text.
`short`	**`getModulus`**`(byte[] buffer, short offset)` Returns the modulus value of the key in plain text.
`void`	**`setExponent`**`(byte[] buffer, short offset, short length)` Sets the private exponent value of the key.
`void`	**`setModulus`**`(byte[] buffer, short offset, short length)` Sets the modulus value of the key.

Methods inherited from interface javacard.security.Key
`clearKey, getSize, getType, isInitialized`

Method Detail

setModulus

```
public void setModulus(byte[] buffer,
                       short offset,
                       short length)
                throws CryptoException
```

Sets the modulus value of the key. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input modulus data is copied into the internal representation.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer at which the modulus value begins
`length` - the length of the modulus

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input modulus data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the modulus value is decrypted using the* `Cipher` *object.*

---

setExponent

```
public void setExponent(byte[] buffer,
                        short offset,
                        short length)
                 throws CryptoException
```

Sets the private exponent value of the key. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input exponent data is copied into the internal representation.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer at which the exponent value begins
`length` - the length of the exponent

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input exponent data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the exponent value is decrypted using the* `Cipher` *object.*

getModulus

```
public short getModulus(byte[] buffer,
                        short offset)
```

Returns the modulus value of the key in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer

`offset` - the offset into the output buffer at which the modulus value starts

Returns:

the byte length of the modulus value returned

getExponent

```
public short getExponent(byte[] buffer,
                         short offset)
```

Returns the private exponent value of the key in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer

`offset` - the offset into the output buffer at which the exponent value begins

Returns:

the byte length of the private exponent value returned

javacard.security
Interface RSAPublicKey

public abstract interface **RSAPublicKey**
extends PublicKey

The `RSAPublicKey` is used to verify signatures on signed data using the RSA algorithm. It may also used by the `javacardx.crypto.Cipher` class to encrypt/decrypt messages.

When both the modulus and exponent of the key are set, the key is initialized and ready for use.

See Also:
`RSAPrivateKey`, `RSAPrivateCrtKey`, `KeyBuilder`, `Signature`, `Cipher`, `KeyEncryption`

Method Summary

`short`	**`getExponent`**`(byte[] buffer, short offset)` Returns the private exponent value of the key in plain text.
`short`	**`getModulus`**`(byte[] buffer, short offset)` Returns the modulus value of the key in plain text.
`void`	**`setExponent`**`(byte[] buffer, short offset, short length)` Sets the public exponent value of the key.
`void`	**`setModulus`**`(byte[] buffer, short offset, short length)` Sets the modulus value of the key.

Methods inherited from interface javacard.security.Key
`clearKey, getSize, getType, isInitialized`

Method Detail

setModulus

```
public void setModulus(byte[] buffer,
                       short offset,
                       short length)
                throws CryptoException
```

Sets the modulus value of the key. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input modulus data is copied into the internal representation.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer at which the modulus value begins
`length` - the byte length of the modulus

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input modulus data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the modulus value is decrypted using the* `Cipher` *object.*

---

setExponent

```
public void setExponent(byte[] buffer,
                        short offset,
                        short length)
                 throws CryptoException
```

Sets the public exponent value of the key. The plaintext data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte). Input exponent data is copied into the internal representation.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer at which the exponent value begins
`length` - the byte length of the exponent

Throws:

CryptoException - with the following reason code:

- `CryptoException.ILLEGAL_VALUE` if the input exponent data length is inconsistent with the implementation or if input data decryption is required and fails.

Note:

- *If the key object implements the* `javacardx.crypto.KeyEncryption` *interface and the* `Cipher` *object specified via* `setKeyCipher()` *is not* `null`*, the exponent value is decrypted using the* `Cipher` *object.*

getModulus

```
public short getModulus(byte[] buffer,
                        short offset)
```

Returns the modulus value of the key in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer

`offset` - the offset into the input buffer at which the modulus value starts

Returns:

the byte length of the modulus value returned

getExponent

```
public short getExponent(byte[] buffer,
                         short offset)
```

Returns the private exponent value of the key in plain text. The data format is big-endian and right-aligned (the least significant bit is the least significant bit of last byte).

Parameters:

`buffer` - the output buffer

`offset` - the offset into the output buffer at which the exponent value begins

Returns:

the byte length of the public exponent returned

javacard.security
Class RandomData

```
java.lang.Object
  |
  +--javacard.security.RandomData
```

public abstract class **RandomData**
extends Object

The `RandomData` abstract class is the base class for random number generation. Implementations of RandomData algorithms must extend this class and implement all the abstract methods.

Field Summary

static byte	**ALG_PSEUDO_RANDOM** Utility pseudo random number generation algorithms.
static byte	**ALG_SECURE_RANDOM** Cryptographically secure random number generation algorithms.

Constructor Summary

protected	**RandomData**() Protected constructor for subclassing.

Method Summary

abstract void	**generateData**(byte[] buffer, short offset, short length) Generates random data.
static RandomData	**getInstance**(byte algorithm) Creates a `RandomData` instance of the selected algorithm.
abstract void	**setSeed**(byte[] buffer, short offset, short length) Seeds the random data generator.

Methods inherited from class java.lang.Object
equals

Field Detail

ALG_PSEUDO_RANDOM

```
public static final byte ALG_PSEUDO_RANDOM
```

Utility pseudo random number generation algorithms.

ALG_SECURE_RANDOM

```
public static final byte ALG_SECURE_RANDOM
```

Cryptographically secure random number generation algorithms.

Constructor Detail

RandomData

```
protected RandomData()
```

Protected constructor for subclassing.

Method Detail

getInstance

```
public static final RandomData getInstance(byte algorithm)
                                    throws CryptoException
```

Creates a `RandomData` instance of the selected algorithm. The pseudo random `RandomData` instance's seed is initialized to a internal default value.

Parameters:

`algorithm` - the desired random number algorithm. Valid codes listed in ALG_.. constants. See above.

Returns:

the `RandomData` object instance of the requested algorithm.

Throws:

CryptoException - with the following reason codes:

- `CryptoException.NO_SUCH_ALGORITHM` if the requested algorithm is not supported.

---

generateData

```
public abstract void generateData(byte[] buffer,
                                  short offset,
                                  short length)
```

Generates random data.

Parameters:

`buffer` - the output buffer
`offset` - the offset into the output buffer
`length` - the length of random data to generate

---

setSeed

```
public abstract void setSeed(byte[] buffer,
                             short offset,
                             short length)
```

Seeds the random data generator.

Parameters:

`buffer` - the input buffer
`offset` - the offset into the input buffer
`length` - the length of the seed data

---

javacard.security
Interface SecretKey

All Known Subinterfaces:
DESKey

public abstract interface **SecretKey**
extends Key

The `SecretKey` class is the base interface for keys used in symmetric alogrightms (e.g. DES).

Methods inherited from interface javacard.security.Key
`clearKey, getSize, getType, isInitialized`

javacard.security
Class Signature

```
java.lang.Object
  |
  +--javacard.security.Signature
```

public abstract class **Signature**
extends Object

The `Signature` class is the base class for Signature algorthims. Implementations of Signature algorithms must extend this class and implement all the abstract methods.

The term "pad" is used in the public key signature algorithms below to refer to all the operations specified in the referenced scheme to transform the message digest into the encryption block size.

Field Summary

`static byte`	**`ALG_DES_MAC4_ISO9797_M1`** Signature algorithm `ALG_DES_MAC4_ISO9797_M1` generates a 4 byte MAC (most significant 4 bytes of encrypted block) using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 1 scheme.
`static byte`	**`ALG_DES_MAC4_ISO9797_M2`** Signature algorithm `ALG_DES_MAC4_ISO9797_M2` generates a 4 byte MAC (most significant 4 bytes of encrypted block) using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 2 (ISO 7816-4, EMV'96) scheme.
`static byte`	**`ALG_DES_MAC4_NOPAD`** Signature algorithm `ALG_DES_MAC4_NOPAD` generates a 4 byte MAC (most significant 4 bytes of encrypted block) using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. This algorithm does not pad input data.
`static byte`	**`ALG_DES_MAC4_PKCS5`** Signature algorithm `ALG_DES_MAC4_PKCS5` generates a 4 byte MAC (most significant 4 bytes of encrypted block) using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the PKCS#5 scheme.
`static byte`	**`ALG_DES_MAC8_ISO9797_M1`** Signature algorithm `ALG_DES_MAC8_ISO9797_M1` generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 1 scheme.

static byte	**ALG_DES_MAC8_ISO9797_M2** Signature algorithm ALG_DES_MAC8_ISO9797_M2 generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 2 (ISO 7816-4, EMV'96) scheme.
static byte	**ALG_DES_MAC8_NOPAD** Signature algorithm ALG_DES_MAC_8_NOPAD generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. This algorithm does not pad input data.
static byte	**ALG_DES_MAC8_PKCS5** Signature algorithm ALG_DES_MAC8_PKCS5 generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the PKCS#5 scheme.
static byte	**ALG_DSA_SHA** Signature algorithm ALG_DSA_SHA signs/verifies the 20 byte SHA digest using DSA.
static byte	**ALG_RSA_MD5_PKCS1** Signature algorithm ALG_RSA_MD5_PKCS1 encrypts the 16 byte MD5 digest using RSA. The digest is padded according to the PKCS#1 (v1.5) scheme.
static byte	**ALG_RSA_MD5_RFC2409** Signature algorithm ALG_RSA_MD5_RFC2409 encrypts the 16 byte MD5 digest using RSA. The digest is padded according to the RFC2409 scheme.
static byte	**ALG_RSA_RIPEMD160_ISO9796** Signature algorithm ALG_RSA_RIPEMD160_ISO9796 encrypts the 20 byte RIPE MD-160 digest using RSA. The digest is padded according to the ISO 9796 scheme.
static byte	**ALG_RSA_RIPEMD160_PKCS1** Signature algorithm ALG_RSA_RIPEMD160_PKCS1 encrypts the 20 byte RIPE MD-160 digest using RSA. The digest is padded according to the PKCS#1 (v1.5) scheme.
static byte	**ALG_RSA_SHA_ISO9796** Signature algorithm ALG_RSA_SHA_ISO9796 encrypts the 20 byte SHA digest using RSA. The digest is padded according to the ISO 9796 (EMV'96) scheme.
static byte	**ALG_RSA_SHA_PKCS1** Signature algorithm ALG_RSA_SHA_PKCS1 encrypts the 20 byte SHA digest using RSA. The digest is padded according to the PKCS#1 (v1.5) scheme.
static byte	**ALG_RSA_SHA_RFC2409** Signature algorithm ALG_RSA_SHA_RFC2409 encrypts the 20 byte SHA digest using RSA. The digest is padded according to the RFC2409 scheme.
static byte	**MODE_SIGN** Used in init() methods to indicate signature sign mode.

static byte	**MODE_VERIFY** Used in `init()` methods to indicate signature verify mode.

Constructor Summary

protected	**Signature**() Protected Constructor

Method Summary

abstract byte	**getAlgorithm**() Gets the Signature algorithm.
static Signature	**getInstance**(byte algorithm, boolean externalAccess) Creates a `Signature` object instance of the selected algorithm.
abstract short	**getLength**() Returns the byte length of the signature data.
abstract void	**init**(Key theKey, byte theMode) Initializes the `Signature` object with the appropriate `Key`.
abstract void	**init**(Key theKey, byte theMode, byte[] bArray, short bOff, short bLen) Initializes the `Signature` object with the appropriate `Key` and algorithm specific parameters.
abstract short	**sign**(byte[] inBuff, short inOffset, short inLength, byte[] sigBuff, short sigOffset) Generates the signature of all/last input data.
abstract void	**update**(byte[] inBuff, short inOffset, short inLength) Accumulates a signature of the input data.
abstract boolean	**verify**(byte[] inBuff, short inOffset, short inLength, byte[] sigBuff, short sigOffset, short sigLength) Verifies the signature of all/last input data against the passed in signature.

Methods inherited from class java.lang.Object
equals

Field Detail

ALG_DES_MAC4_NOPAD

```
public static final byte ALG_DES_MAC4_NOPAD
```

Signature algorithm `ALG_DES_MAC4_NOPAD` generates a 4 byte MAC (most significant 4 bytes of encrypted block) using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. This algorithm does not pad input data. If the input data is not (8 byte) block aligned it throws `CryptoExeption` with the reason code `ILLEGAL_USE`.

ALG_DES_MAC8_NOPAD

```
public static final byte ALG_DES_MAC8_NOPAD
```

Signature algorithm `ALG_DES_MAC_8_NOPAD` generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. This algorithm does not pad input data. If the input data is not (8 byte) block aligned it throws `CryptoExeption` with the reason code `ILLEGAL_USE`.

Note:

- *This algorithm must not be implemented if export restrictions apply.*

ALG_DES_MAC4_ISO9797_M1

```
public static final byte ALG_DES_MAC4_ISO9797_M1
```

Signature algorithm `ALG_DES_MAC4_ISO9797_M1` generates a 4 byte MAC (most significant 4 bytes of encrypted block) using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 1 scheme.

ALG_DES_MAC8_ISO9797_M1

```
public static final byte ALG_DES_MAC8_ISO9797_M1
```

Signature algorithm `ALG_DES_MAC8_ISO9797_M1` generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 1 scheme.

Note:

- *This algorithm must not be implemented if export restrictions apply.*

ALG_DES_MAC4_ISO9797_M2

```
public static final byte ALG_DES_MAC4_ISO9797_M2
```

Signature algorithm ALG_DES_MAC4_ISO9797_M2 generates a 4 byte MAC (most significant 4 bytes of encrypted block) using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 2 (ISO 7816-4, EMV'96) scheme.

ALG_DES_MAC8_ISO9797_M2

```
public static final byte ALG_DES_MAC8_ISO9797_M2
```

Signature algorithm ALG_DES_MAC8_ISO9797_M2 generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 2 (ISO 7816-4, EMV'96) scheme.

Note:

- *This algorithm must not be implemented if export restrictions apply.*

ALG_DES_MAC4_PKCS5

```
public static final byte ALG_DES_MAC4_PKCS5
```

Signature algorithm ALG_DES_MAC4_PKCS5 generates a 4 byte MAC (most significant 4 bytes of encrypted block) using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the PKCS#5 scheme.

ALG_DES_MAC8_PKCS5

```
public static final byte ALG_DES_MAC8_PKCS5
```

Signature algorithm ALG_DES_MAC8_PKCS5 generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the PKCS#5 scheme.

Note:

- *This algorithm must not be implemented if export restrictions apply.*

ALG_RSA_SHA_ISO9796

```
public static final byte ALG_RSA_SHA_ISO9796
```

Signature algorithm ALG_RSA_SHA_ISO9796 encrypts the 20 byte SHA digest using RSA. The digest is padded according to the ISO 9796 (EMV'96) scheme.

ALG_RSA_SHA_PKCS1

```
public static final byte ALG_RSA_SHA_PKCS1
```

Signature algorithm ALG_RSA_SHA_PKCS1 encrypts the 20 byte SHA digest using RSA. The digest is padded according to the PKCS#1 (v1.5) scheme.

ALG_RSA_MD5_PKCS1

```
public static final byte ALG_RSA_MD5_PKCS1
```

Signature algorithm ALG_RSA_MD5_PKCS1 encrypts the 16 byte MD5 digest using RSA. The digest is padded according to the PKCS#1 (v1.5) scheme.

ALG_RSA_RIPEMD160_ISO9796

```
public static final byte ALG_RSA_RIPEMD160_ISO9796
```

Signature algorithm ALG_RSA_RIPEMD160_ISO9796 encrypts the 20 byte RIPE MD-160 digest using RSA. The digest is padded according to the ISO 9796 scheme.

ALG_RSA_RIPEMD160_PKCS1

```
public static final byte ALG_RSA_RIPEMD160_PKCS1
```

Signature algorithm ALG_RSA_RIPEMD160_PKCS1 encrypts the 20 byte RIPE MD-160 digest using RSA. The digest is padded according to the PKCS#1 (v1.5) scheme.

ALG_DSA_SHA

```
public static final byte ALG_DSA_SHA
```

Signature algorithm ALG_DSA_SHA signs/verifies the 20 byte SHA digest using DSA.

ALG_RSA_SHA_RFC2409

```
public static final byte ALG_RSA_SHA_RFC2409
```

Signature algorithm `ALG_RSA_SHA_RFC2409` encrypts the 20 byte SHA digest using RSA. The digest is padded according to the RFC2409 scheme.

ALG_RSA_MD5_RFC2409

```
public static final byte ALG_RSA_MD5_RFC2409
```

Signature algorithm `ALG_RSA_MD5_RFC2409` encrypts the 16 byte MD5 digest using RSA. The digest is padded according to the RFC2409 scheme.

MODE_SIGN

```
public static final byte MODE_SIGN
```

Used in `init()` methods to indicate signature sign mode.

MODE_VERIFY

```
public static final byte MODE_VERIFY
```

Used in `init()` methods to indicate signature verify mode.

Constructor Detail

Signature

```
protected Signature()
```

Protected Constructor

Method Detail

getInstance

```
public static final Signature getInstance(byte algorithm,
                                          boolean externalAccess)
                                   throws CryptoException
```

Creates a `Signature` object instance of the selected algorithm.

Parameters:

`algorithm` - the desired Signature algorithm. See above.

`externalAccess` - if `true` indicates that the instance will be shared among multiple applet instances and that the `Signature` instance will also be accessed (via a `Shareable` interface) when the owner of the `Signature` instance is not the currently selected applet.

Returns:

the `Signature` object instance of the requested algorithm.

Throws:

CryptoException - with the following reason codes:

- `CryptoException.NO_SUCH_ALGORITHM` if the requested algorithm is not supported.

---

init

```
public abstract void init(Key theKey,
                          byte theMode)
                   throws CryptoException
```

Initializes the `Signature` object with the appropriate `Key`. This method should be used for algorithms which do not need initialization parameters or use default parameter values.

Note:

- *DES and triple DES algorithms in CBC mode will use 0 for initial vector(IV) if this method is used.*

Parameters:

`theKey` - the key object to use for signing or verifying

`theMode` - one of `MODE_SIGN` or `MODE_VERIFY`

Throws:

CryptoException - with the following reason codes:

- `CryptoException.ILLEGAL_VALUE` if `theMode` option is an undefined value or if the `Key` is inconsistent with `theMode` or with the `Signature` implementation.

---

init

```
public abstract void init(Key theKey,
                          byte theMode,
                          byte[] bArray,
                          short bOff,
                          short bLen)
                   throws CryptoException
```

Initializes the `Signature` object with the appropriate `Key` and algorithm specific parameters.

Note:

- *DES and triple DES algorithms in outer CBC mode expect an 8 byte parameter value for the initial vector(IV) in* `bArray`.

- *RSA and DSA algorithms throw* `CryptoException.ILLEGAL_VALUE`.

Parameters:

`theKey` - the key object to use for signing
`theMode` - one of `MODE_SIGN` or `MODE_VERIFY`
`bArray` - byte array containing algorithm specific initialization info.
`bOff` - offset withing `bArray` where the algorithm specific data begins.
`bLen` - byte length of algorithm specific parameter data

Throws:

CryptoException - with the following reason codes:

- `CryptoException.ILLEGAL_VALUE` if `theMode` option is an undefined value or if a byte array parameter option is not supported by the algorithm or if the `bLen` is an incorrect byte length for the algorithm specific data or if the `Key` is inconsistent with `theMode` or with the `Signature` implementation.

---

getAlgorithm

```
public abstract byte getAlgorithm()
```

Gets the Signature algorithm.

Returns:

the algorithm code defined above.

---

getLength

```
public abstract short getLength()
```

Returns the byte length of the signature data.

Returns:

the byte length of the signature data.

---

update

```
public abstract void update(byte[] inBuff,
                            short inOffset,
                            short inLength)
                     throws CryptoException
```

Accumulates a signature of the input data. When this method is used temporary storage of intermediate results is required. This method should only be used if all the input data required for the signature is not available in one byte array. The `sign()` or `verify()` method is recommended whenever possible.

Parameters:

`inBuff` - the input buffer of data to be signed
`inOffset` - the offset into the input buffer at which to begin signature generation
`inLength` - the byte length to sign

Throws:

CryptoException - with the following reason codes:

- `CryptoException.UNINITIALIZED_KEY` if key not initialized.

See Also:

`sign(byte[], short, short, byte[], short)`, `verify(byte[], short, short, byte[], short, short)`

---

sign

```
public abstract short sign(byte[] inBuff,
                           short inOffset,
                           short inLength,
                           byte[] sigBuff,
                           short sigOffset)
                    throws CryptoException
```

Generates the signature of all/last input data. A call to this method also resets this `Signature` object to the state it was in when previously initialized via a call to `init()`. That is, the object is reset and available to sign another message.

The input and output buffer data may overlap.

Parameters:

`inBuff` - the input buffer of data to be signed
`inOffset` - the offset into the input buffer at which to begin signature generation
`inLength` - the byte length to sign
`sigBuff` - the output buffer to store signature data
`sigOffset` - the offset into sigBuff at which to begin signature data

Returns:

number of bytes of signature output in sigBuff

Throws:

CryptoException - with the following reason codes:

- `CryptoException.UNINITIALIZED_KEY` if key not initialized.
- `CryptoException.INVALID_INIT` if this `Signature` object is not initialized or initialized for signature verify mode.
- `CryptoException.ILLEGAL_USE` if this `Signature` algorithm does not pad the message and the message is not block aligned.

---

verify

```
public abstract boolean verify(byte[] inBuff,
                               short inOffset,
                               short inLength,
                               byte[] sigBuff,
                               short sigOffset,
                               short sigLength)
                        throws CryptoException
```

Verifies the signature of all/last input data against the passed in signature. A call to this method also resets this `Signature` object to the state it was in when previously initialized via a call to `init()`. That is, the object is reset and available to verify another message.

Parameters:

`inBuff` - the input buffer of data to be verified
`inOffset` - the offset into the input buffer at which to begin signature generation
`inLength` - the byte length to sign
`sigBuff` - the input buffer containing signature data
`sigOffset` - the offset into sigBuff where signature data begins.
`sigLength` - the byte length of the signature data

Returns:

`true` if signature verifies `false` otherwise.

Throws:

CryptoException - with the following reason codes:

- `CryptoException.UNINITIALIZED_KEY` if key not initialized.
- `CryptoException.INVALID_INIT` if this `Signature` object is not initialized or initialized for signature sign mode.
- `CryptoException.ILLEGAL_USE` if this `Signature` algorithm does not pad the message and the message is not block aligned.

Package javacardx.crypto

Extension package containing security classes and interfaces for export-controlled functionality.

See:

Description

Interface Summary	
KeyEncryption	`KeyEncryption` interface defines the methods used to enable encrypted key data access to a key implementation.

Class Summary	
Cipher	The `Cipher` class is the abstract base class for Cipher algorthims.

Package javacardx.crypto Description

Extension package containing security classes and interfaces for export-controlled functionality.

javacardx.crypto
Class Cipher

```
java.lang.Object
  |
  +--javacardx.crypto.Cipher
```

public abstract class **Cipher**
extends Object

The `Cipher` class is the abstract base class for Cipher algorthims. Implementations of Cipher algorithms must extend this class and implement all the abstract methods.

The term "pad" is used in the public key cipher algorithms below to refer to all the operations specified in the referenced scheme to transform the message block into the cipher block size.

Field Summary

`static byte`	**`ALG_DES_CBC_ISO9797_M1`** Cipher algorithm `ALG_DES_CBC_ISO9797_M1` provides a cipher using DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 1 scheme.
`static byte`	**`ALG_DES_CBC_ISO9797_M2`** Cipher algorithm `ALG_DES_CBC_ISO9797_M2` provides a cipher using DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 2 (ISO 7816-4, EMV'96) scheme.
`static byte`	**`ALG_DES_CBC_NOPAD`** Cipher algorithm `ALG_DES_CBC_NOPAD` provides a cipher using DES in CBC mode. This algorithm uses outer CBC for triple DES. This algorithm does not pad input data.
`static byte`	**`ALG_DES_CBC_PKCS5`** Cipher algorithm ALG_DES_CBC_PKCS5 provides a cipher using DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the PKCS#5 scheme.
`static byte`	**`ALG_DES_ECB_ISO9797_M1`** Cipher algorithm `ALG_DES_ECB_ISO9797_M1` provides a cipher using DES in ECB mode. Input data is padded according to the ISO 9797 method 1 scheme.
`static byte`	**`ALG_DES_ECB_ISO9797_M2`** Cipher algorithm `ALG_DES_ECB_ISO9797_M2` provides a cipher using DES in ECB mode. Input data is padded according to the ISO 9797 method 2 (ISO 7816-4, EMV'96) scheme.

static byte	**ALG_DES_ECB_NOPAD** Cipher algorithm ALG_DES_ECB_NOPAD provides a cipher using DES in ECB mode. This algorithm does not pad input data.
static byte	**ALG_DES_ECB_PKCS5** Cipher algorithm ALG_DES_ECB_PKCS5 provides a cipher using DES in ECB mode. Input data is padded according to the PKCS#5 scheme.
static byte	**ALG_RSA_ISO14888** Cipher algorithm ALG_RSA_ISO14888 provides a cipher using RSA. Input data is padded according to the ISO 14888 scheme.
static byte	**ALG_RSA_ISO9796** Cipher algorithm ALG_RSA_ISO9796 provides a cipher using RSA. Input data is padded according to the ISO 9796 (EMV'96) scheme.
static byte	**ALG_RSA_PKCS1** Cipher algorithm ALG_RSA_PKCS1 provides a cipher using RSA. Input data is padded according to the PKCS#1 (v1.5) scheme.
static byte	**MODE_DECRYPT** Used in init() methods to indicate decryption mode.
static byte	**MODE_ENCRYPT** Used in init() methods to indicate encryption mode.

Constructor Summary

protected	**Cipher**() Protected Constructor

Method Summary	
abstract short	**doFinal**(byte[] inBuff, short inOffset, short inLength, byte[] outBuff, short outOffset) Generates encrypted/decrypted output from all/last input data.
abstract byte	**getAlgorithm**() Gets the Cipher algorithm.
static Cipher	**getInstance**(byte algorithm, boolean externalAccess) Creates a Cipher object instance of the selected algorithm.
abstract void	**init**(Key theKey, byte theMode) Initializes the Cipher object with the appropriate Key.
abstract void	**init**(Key theKey, byte theMode, byte[] bArray, short bOff, short bLen) Initializes the Cipher object with the appropriate Key and algorithm specific parameters.
abstract short	**update**(byte[] inBuff, short inOffset, short inLength, byte[] outBuff, short outOffset) Generates encrypted/decrypted output from input data.

Methods inherited from class java.lang.Object
equals

Field Detail

ALG_DES_CBC_NOPAD

```
public static final byte ALG_DES_CBC_NOPAD
```

Cipher algorithm ALG_DES_CBC_NOPAD provides a cipher using DES in CBC mode. This algorithm uses outer CBC for triple DES. This algorithm does not pad input data. If the input data is not (8 byte) block aligned it throws CryptoExeption with the reason code ILLEGAL_USE.

ALG_DES_CBC_ISO9797_M1

```
public static final byte ALG_DES_CBC_ISO9797_M1
```

Cipher algorithm ALG_DES_CBC_ISO9797_M1 provides a cipher using DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 1 scheme.

ALG_DES_CBC_ISO9797_M2

```
public static final byte ALG_DES_CBC_ISO9797_M2
```

Cipher algorithm ALG_DES_CBC_ISO9797_M2 provides a cipher using DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 2 (ISO 7816-4, EMV'96) scheme.

ALG_DES_CBC_PKCS5

```
public static final byte ALG_DES_CBC_PKCS5
```

Cipher algorithm ALG_DES_CBC_PKCS5 provides a cipher using DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the PKCS#5 scheme.

ALG_DES_ECB_NOPAD

```
public static final byte ALG_DES_ECB_NOPAD
```

Cipher algorithm ALG_DES_ECB_NOPAD provides a cipher using DES in ECB mode. This algorithm does not pad input data. If the input data is not (8 byte) block aligned it throws CryptoExeption with the reason code ILLEGAL_USE.

ALG_DES_ECB_ISO9797_M1

```
public static final byte ALG_DES_ECB_ISO9797_M1
```

Cipher algorithm ALG_DES_ECB_ISO9797_M1 provides a cipher using DES in ECB mode. Input data is padded according to the ISO 9797 method 1 scheme.

ALG_DES_ECB_ISO9797_M2

```
public static final byte ALG_DES_ECB_ISO9797_M2
```

Cipher algorithm ALG_DES_ECB_ISO9797_M2 provides a cipher using DES in ECB mode. Input data is padded according to the ISO 9797 method 2 (ISO 7816-4, EMV'96) scheme.

ALG_DES_ECB_PKCS5

```
public static final byte ALG_DES_ECB_PKCS5
```

Cipher algorithm `ALG_DES_ECB_PKCS5` provides a cipher using DES in ECB mode. Input data is padded according to the PKCS#5 scheme.

ALG_RSA_ISO14888

```
public static final byte ALG_RSA_ISO14888
```

Cipher algorithm `ALG_RSA_ISO14888` provides a cipher using RSA. Input data is padded according to the ISO 14888 scheme.

ALG_RSA_PKCS1

```
public static final byte ALG_RSA_PKCS1
```

Cipher algorithm `ALG_RSA_PKCS1` provides a cipher using RSA. Input data is padded according to the PKCS#1 (v1.5) scheme.

Note:

- *This algorithm is only suitable for messages of limited length. The total number of input bytes processed may not be more than k-11, where k is the RSA key's modulus size in bytes.*

ALG_RSA_ISO9796

```
public static final byte ALG_RSA_ISO9796
```

Cipher algorithm `ALG_RSA_ISO9796` provides a cipher using RSA. Input data is padded according to the ISO 9796 (EMV'96) scheme.

Note:

- *This algorithm is only suitable for messages of limited length. The total number of input bytes processed may not be more than k/2, where k is the RSA key's modulus size in bytes.*

MODE_DECRYPT

```
public static final byte MODE_DECRYPT
```

Used in `init()` methods to indicate decryption mode.

MODE_ENCRYPT

```
public static final byte MODE_ENCRYPT
```

Used in `init()` methods to indicate encryption mode.

Constructor Detail

Cipher

```
protected Cipher()
```

Protected Constructor

Method Detail

getInstance

```
public static final Cipher getInstance(byte algorithm,
                                       boolean externalAccess)
                                throws CryptoException
```

Creates a `Cipher` object instance of the selected algorithm.

Parameters:

`algorithm` - the desired Cipher algorithm. See above.

`externalAccess` - if `true` indicates that the instance will be shared among multiple applet instances and that the `Cipher` instance will also be accessed (via a `Shareable` interface) when the owner of the `Cipher` instance is not the currently selected applet.

Returns:

the `Cipher` object instance of the requested algorithm.

Throws:

CryptoException - with the following reason codes:

- `CryptoException.NO_SUCH_ALGORITHM` if the requested algorithm is not supported.

---

init

```
public abstract void init(Key theKey,
                          byte theMode)
                   throws CryptoException
```

Initializes the `Cipher` object with the appropriate `Key`. This method should be used for algorithms which do not need initialization parameters or use default parameter values.

Note:

- *DES and triple DES algorithms in CBC mode will use 0 for initial vector(IV) if this method is used.*

Parameters:

`theKey` - the key object to use for signing or verifying
`theMode` - one of `MODE_DECRYPT` or `MODE_ENCRYPT`

Throws:

CryptoException - with the following reason codes:

- `CryptoException.ILLEGAL_VALUE` if `theMode` option is an undefined value or if the `Key` is inconsistent with the `Cipher` implementation.

---

init

```
public abstract void init(Key theKey,
                          byte theMode,
                          byte[] bArray,
                          short bOff,
                          short bLen)
                   throws CryptoException
```

Initializes the `Cipher` object with the appropriate Key and algorithm specific parameters.

Note:

- *DES and triple DES algorithms in outer CBC mode expect an 8 byte parameter value for the initial vector(IV) in* `bArray`.
- *RSA and DSA algorithms throw* `CryptoException.ILLEGAL_VALUE`.

Parameters:

`theKey` - the key object to use for signing
`theMode` - one of `MODE_DECRYPT` or `MODE_ENCRYPT`
`bArray` - byte array containing algorithm specific initialization info.
`bOff` - offset withing bArray where the algorithm specific data begins.
`bLen` - byte length of algorithm specific parameter data

Throws:

CryptoException - with the following reason codes:

- `CryptoException.ILLEGAL_VALUE` if `theMode` option is an undefined value or if a byte array parameter option is not supported by the algorithm or if the `bLen` is an incorrect byte length for the algorithm specific data or if the `Key` is inconsistent with the `Cipher` implementation.

---

getAlgorithm

```
public abstract byte getAlgorithm()
```

Gets the Cipher algorithm.

Returns:
the algorithm code defined above.

---

doFinal

```
public abstract short doFinal(byte[] inBuff,
                              short inOffset,
                              short inLength,
                              byte[] outBuff,
                              short outOffset)
                       throws CryptoException
```

Generates encrypted/decrypted output from all/last input data. A call to this method also resets this `Cipher` object to the state it was in when previously initialized via a call to `init()`. That is, the object is reset and available to encrypt or decrypt (depending on the operation mode that was specified in the call to `init()`) more data.

The input and output buffer data may overlap.

Notes:

- *On decryption operations (except when ISO 9797 method 1 padding is used), the padding bytes are not written to* `outBuff`.
- *On encryption operations, the number of bytes output into* `outBuff` *may be larger than* `inLength`.

Parameters:
`inBuff` - the input buffer of data to be encrypted/decrypted.
`inOffset` - the offset into the input buffer at which to begin encryption/decryption.
`inLength` - the byte length to be encrypted/decrypted.
`outBuff` - the output buffer, may be the same as the input buffer
`outOffset` - the offset into the output buffer where the resulting hash value begins

Returns:
number of bytes output in `outBuff`

Throws:
CryptoException - with the following reason codes:

- `CryptoException.UNINITIALIZED_KEY` if key not initialized.
- `CryptoException.INVALID_INIT` if this `Cipher` object is not initialized.
- `CryptoException.ILLEGAL_USE` if this `Cipher` algorithm does not pad the message and the message is not block aligned or if the input message length is not supported.

---

update

```
public abstract short update(byte[] inBuff,
                             short inOffset,
```

```
                short inLength,
                byte[] outBuff,
                short outOffset)
        throws CryptoException
```

Generates encrypted/decrypted output from input data. When this method is used temporary storage of intermediate results is required. This method should only be used if all the input data required for the cipher is not available in one byte array. The `doFinal()` method is recommended whenever possible.

The input and output buffer data may overlap.

Notes:

- *On decryption operations(except when ISO 9797 method 1 padding is used), the padding bytes are not written to* `outBuff`.
- *On encryption operations, the number of bytes output into* `outBuff` *may be larger than* `inLength`.
- *On encryption and decryption operations(except when ISO 9797 method 1 padding is used), block alignment considerations may require that the number of bytes output into* `outBuff` *be smaller than* `inLength` *or even 0.*

Parameters:

`inBuff` - the input buffer of data to be encrypted/decrypted.
`inOffset` - the offset into the input buffer at which to begin encryption/decryption.
`inLength` - the byte length to be encrypted/decrypted.
`outBuff` - the output buffer, may be the same as the input buffer
`outOffset` - the offset into the output buffer where the resulting hash value begins

Returns:

number of bytes output in `outBuff`

Throws:

CryptoException - with the following reason codes:

- `CryptoException.UNINITIALIZED_KEY` if key not initialized.
- `CryptoException.INVALID_INIT` if this `Cipher` object is not initialized.
- `CryptoException.ILLEGAL_USE` if the input message length is not supported.

---

javacardx.crypto
Interface KeyEncryption

public abstract interface **KeyEncryption**

`KeyEncryption` interface defines the methods used to enable encrypted key data access to a key implementation.

See Also:
`KeyBuilder`, `Cipher`

Method Summary

`Cipher`	**`getKeyCipher`**`()` Returns the `Cipher` object to be used to decrypt the input key data and key parameters in the set methods. Default is `null` - no decryption performed.
`void`	**`setKeyCipher`**`(Cipher keyCipher)` Sets the `Cipher` object to be used to decrypt the input key data and key parameters in the set methods. Default `Cipher` object is `null` - no decryption performed.

Method Detail

setKeyCipher

```
public void setKeyCipher(Cipher keyCipher)
```

Sets the `Cipher` object to be used to decrypt the input key data and key parameters in the set methods.

Default `Cipher` object is `null` - no decryption performed.

Parameters:

`keyCipher` - the decryption `Cipher` object to decrypt the input key data. `null` parameter indicates that no decryption is required.

getKeyCipher

```
public Cipher getKeyCipher()
```

Returns the `Cipher` object to be used to decrypt the input key data and key parameters in the set methods.

Default is `null` - no decryption performed.

Returns:

keyCipher the decryption `Cipher` object to decrypt the input key data. `null` return indicates that no decryption is performed.

A B C D E G I J K L M N O P R S T U V W

A

ALG_DES_MAC4_NOPAD - Static variable in class javacard.security.Signature
Signature algorithm ALG_DES_MAC4_NOPAD generates a 4 byte MAC (most significant 4 bytes of encrypted block) using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. This algorithm does not pad input data.

ALG_DES_MAC4_PKCS5 - Static variable in class javacard.security.Signature
Signature algorithm ALG_DES_MAC4_PKCS5 generates a 4 byte MAC (most significant 4 bytes of encrypted block) using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the PKCS#5 scheme.

ALG_DES_MAC8_ISO9797_M1 - Static variable in class javacard.security.Signature
Signature algorithm ALG_DES_MAC8_ISO9797_M1 generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 1 scheme.

ALG_DES_MAC8_ISO9797_M2 - Static variable in class javacard.security.Signature
Signature algorithm ALG_DES_MAC8_ISO9797_M2 generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the ISO 9797 method 2 (ISO 7816-4, EMV'96) scheme.

ALG_DES_MAC8_NOPAD - Static variable in class javacard.security.Signature
Signature algorithm ALG_DES_MAC_8_NOPAD generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. This algorithm does not pad input data.

ALG_DES_MAC8_PKCS5 - Static variable in class javacard.security.Signature
Signature algorithm ALG_DES_MAC8_PKCS5 generates a 8 byte MAC using DES or triple DES in CBC mode. This algorithm uses outer CBC for triple DES. Input data is padded according to the PKCS#5 scheme.

ALG_DSA_SHA - Static variable in class javacard.security.Signature
Signature algorithm ALG_DSA_SHA signs/verifies the 20 byte SHA digest using DSA.

ALG_MD5 - Static variable in class javacard.security.MessageDigest
Message Digest algorithm MD5.

ALG_PSEUDO_RANDOM - Static variable in class javacard.security.RandomData
Utility pseudo random number generation algorithms.

ALG_RIPEMD160 - Static variable in class javacard.security.MessageDigest
Message Digest algorithm RIPE MD-160.

ALG_RSA_ISO14888 - Static variable in class javacardx.crypto.Cipher
Cipher algorithm ALG_RSA_ISO14888 provides a cipher using RSA. Input data is padded according to the ISO 14888 scheme.

ALG_RSA_ISO9796 - Static variable in class javacardx.crypto.Cipher
Cipher algorithm ALG_RSA_ISO9796 provides a cipher using RSA. Input data is padded according to the ISO 9796 (EMV'96) scheme.

ALG_RSA_MD5_PKCS1 - Static variable in class javacard.security.Signature
Signature algorithm ALG_RSA_MD5_PKCS1 encrypts the 16 byte MD5 digest using RSA. The digest is padded according to the PKCS#1 (v1.5) scheme.

ALG_RSA_MD5_RFC2409 - Static variable in class javacard.security.Signature
Signature algorithm ALG_RSA_MD5_RFC2409 encrypts the 16 byte MD5 digest using RSA. The digest is padded according to the RFC2409 scheme.

ALG_RSA_PKCS1 - Static variable in class javacardx.crypto.Cipher
Cipher algorithm ALG_RSA_PKCS1 provides a cipher using RSA. Input data is padded according to

the PKCS#1 (v1.5) scheme.

ALG_RSA_RIPEMD160_ISO9796 - Static variable in class javacard.security.Signature
Signature algorithm `ALG_RSA_RIPEMD160_ISO9796` encrypts the 20 byte RIPE MD-160 digest using RSA. The digest is padded according to the ISO 9796 scheme.

ALG_RSA_RIPEMD160_PKCS1 - Static variable in class javacard.security.Signature
Signature algorithm `ALG_RSA_RIPEMD160_PKCS1` encrypts the 20 byte RIPE MD-160 digest using RSA. The digest is padded according to the PKCS#1 (v1.5) scheme.

ALG_RSA_SHA_ISO9796 - Static variable in class javacard.security.Signature
Signature algorithm `ALG_RSA_SHA_ISO9796` encrypts the 20 byte SHA digest using RSA. The digest is padded according to the ISO 9796 (EMV'96) scheme.

ALG_RSA_SHA_PKCS1 - Static variable in class javacard.security.Signature
Signature algorithm `ALG_RSA_SHA_PKCS1` encrypts the 20 byte SHA digest using RSA. The digest is padded according to the PKCS#1 (v1.5) scheme.

ALG_RSA_SHA_RFC2409 - Static variable in class javacard.security.Signature
Signature algorithm `ALG_RSA_SHA_RFC2409` encrypts the 20 byte SHA digest using RSA. The digest is padded according to the RFC2409 scheme.

ALG_SECURE_RANDOM - Static variable in class javacard.security.RandomData
Cryptographically secure random number generation algorithms.

ALG_SHA - Static variable in class javacard.security.MessageDigest
Message Digest algorithm SHA.

APDU - class javacard.framework.APDU.
Application Protocol Data Unit (APDU) is the communication format between the card and the off-card applications.

APDUException - exception javacard.framework.APDUException.
`APDUException` represents an `APDU` related exception.

APDUException(short) - Constructor for class javacard.framework.APDUException
Constructs an APDUException.

Applet - class javacard.framework.Applet.
This abstract class defines an applet in Java Card.

Applet() - Constructor for class javacard.framework.Applet
Only this class's `install()` method should create the applet object.

ArithmeticException - exception java.lang.ArithmeticException.
A JCRE owned instance of `ArithmethicException` is thrown when an exceptional arithmetic condition has occurred.

ArithmeticException() - Constructor for class java.lang.ArithmeticException
Constructs an `ArithmeticException`.

arrayCompare(byte[], short, byte[], short, short) - Static method in class javacard.framework.Util
Compares an array from the specified source array, beginning at the specified position, with the specified position of the destination array from left to right.

arrayCopy(byte[], short, byte[], short, short) - Static method in class javacard.framework.Util
Copies an array from the specified source array, beginning at the specified position, to the specified position of the destination array.

arrayCopyNonAtomic(byte[], short, byte[], short, short) - Static method in class javacard.framework.Util
Copies an array from the specified source array, beginning at the specified position, to the specified position of the destination array (non-atomically).

B

C

check(byte[], short, byte) - Method in class javacard.framework.OwnerPIN
Compares `pin` against the PIN value.
check(byte[], short, byte) - Method in interface javacard.framework.PIN
Compares `pin` against the PIN value.
Cipher - class javacardx.crypto.Cipher.
The `Cipher` class is the abstract base class for Cipher algorthims.
Cipher() - Constructor for class javacardx.crypto.Cipher
Protected Constructor
CLA_ISO7816 - Static variable in interface javacard.framework.ISO7816
APDU command CLA : ISO 7816 = 0x00
ClassCastException - exception java.lang.ClassCastException.
A JCRE owned instance of `ClassCastException` is thrown to indicate that the code has attempted to cast an object to a subclass of which it is not an instance.
ClassCastException() - Constructor for class java.lang.ClassCastException
Constructs a `ClassCastException`.
CLEAR_ON_DESELECT - Static variable in class javacard.framework.JCSystem
This event code indicates that the contents of the transient object are cleared to the default value on applet deselection event or in `CLEAR_ON_RESET` cases.
CLEAR_ON_RESET - Static variable in class javacard.framework.JCSystem
This event code indicates that the contents of the transient object are cleared to the default value on card reset (or power on) event.
clearKey() - Method in interface javacard.security.Key
Clears the key and sets its initialized state to false.
commitTransaction() - Static method in class javacard.framework.JCSystem
Commits an atomic transaction.
CryptoException - exception javacard.security.CryptoException.
`CryptoException` represents a cryptography-related exception.
CryptoException(short) - Constructor for class javacard.security.CryptoException
Constructs a `CryptoException` with the specified reason.

D

deselect() - Method in class javacard.framework.Applet
Called by the JCRE to inform this currently selected applet that another (or the same) applet will be selected.
DESKey - interface javacard.security.DESKey.
`DESKey` contains an 8/16/24 byte key for single/2 key triple DES/3 key triple DES operations.
doFinal(byte[], short, short, byte[], short) - Method in class javacard.security.MessageDigest
Generates a hash of all/last input data.
doFinal(byte[], short, short, byte[], short) - Method in class javacardx.crypto.Cipher
Generates encrypted/decrypted output from all/last input data.
DSAKey - interface javacard.security.DSAKey.
The DSAKey interface is the base interface for the DSA algorithms private and public key implementaions.

DSAPrivateKey - interface javacard.security.DSAPrivateKey.
The `DSAPrivateKey` interface is used to sign data using the DSA algorithm.
DSAPublicKey - interface javacard.security.DSAPublicKey.
The `DSAPublicKey` interface is used to verify signatures on signed data using the DSA algorithm.

E

equals(byte[], short, byte) - Method in class javacard.framework.AID
Checks if the specified AID bytes in `bArray` are the same as those encapsulated in `this AID` object.
equals(Object) - Method in class java.lang.Object
Compares two Objects for equality.
equals(Object) - Method in class javacard.framework.AID
Compares the AID bytes in `this AID` instance to the AID bytes in the specified object.
Exception - exception java.lang.Exception.
The class `Exception` and its subclasses are a form of `Throwable` that indicates conditions that a reasonable applet might want to catch.
Exception() - Constructor for class java.lang.Exception
Constructs an `Exception` instance.

G

generateData(byte[], short, short) - Method in class javacard.security.RandomData
Generates random data.
getAID() - Static method in class javacard.framework.JCSystem
Returns the JCRE owned instance of the `AID` object associated with the current applet context.
getAlgorithm() - Method in class javacard.security.MessageDigest
Gets the Message digest algorithm.
getAlgorithm() - Method in class javacard.security.Signature
Gets the Signature algorithm.
getAlgorithm() - Method in class javacardx.crypto.Cipher
Gets the Cipher algorithm.
getAppletShareableInterfaceObject(AID, byte) - Static method in class javacard.framework.JCSystem
This method is called by a client applet to get a server applet's shareable interface object.
getBuffer() - Method in class javacard.framework.APDU
Returns the APDU buffer byte array.
getBytes(byte[], short) - Method in class javacard.framework.AID
Called to get the AID bytes encapsulated within `AID` object.
getDP1(byte[], short) - Method in interface javacard.security.RSAPrivateCrtKey
Returns the value of the DP1 parameter in plain text.
getDQ1(byte[], short) - Method in interface javacard.security.RSAPrivateCrtKey
Returns the value of the DQ1 parameter in plain text.

getExponent(byte[], short) - Method in interface javacard.security.RSAPrivateKey
Returns the private exponent value of the key in plain text.
getExponent(byte[], short) - Method in interface javacard.security.RSAPublicKey
Returns the private exponent value of the key in plain text.
getG(byte[], short) - Method in interface javacard.security.DSAKey
Returns the subprime parameter value of the key in plain text.
getInBlockSize() - Static method in class javacard.framework.APDU
Returns the configured incoming block size. In T=1 protocol, this corresponds to IFSC (information field size for ICC), the maximum size of incoming data blocks into the card. In T=0 protocol, this method returns 1.
getInstance(byte) - Static method in class javacard.security.RandomData
Creates a `RandomData` instance of the selected algorithm.
getInstance(byte, boolean) - Static method in class javacard.security.MessageDigest
Creates a `MessageDigest` object instance of the selected algorithm.
getInstance(byte, boolean) - Static method in class javacard.security.Signature
Creates a `Signature` object instance of the selected algorithm.
getInstance(byte, boolean) - Static method in class javacardx.crypto.Cipher
Creates a `Cipher` object instance of the selected algorithm.
getKey(byte[], short) - Method in interface javacard.security.DESKey
Returns the `Key` data in plain text.
getKeyCipher() - Method in interface javacardx.crypto.KeyEncryption
Returns the `Cipher` object to be used to decrypt the input key data and key parameters in the set methods. Default is `null` - no decryption performed.
getLength() - Method in class javacard.security.MessageDigest
Returns the byte length of the hash.
getLength() - Method in class javacard.security.Signature
Returns the byte length of the signature data.
getMaxCommitCapacity() - Static method in class javacard.framework.JCSystem
Returns the total number of bytes in the commit buffer.
getModulus(byte[], short) - Method in interface javacard.security.RSAPrivateKey
Returns the modulus value of the key in plain text.
getModulus(byte[], short) - Method in interface javacard.security.RSAPublicKey
Returns the modulus value of the key in plain text.
getNAD() - Method in class javacard.framework.APDU
In T=1 protocol, this method returns the Node Address byte, NAD. In T=0 protocol, this method returns 0.
getOutBlockSize() - Static method in class javacard.framework.APDU
Returns the configured outgoing block size. In T=1 protocol, this corresponds to IFSD (information field size for interface device), the maximum size of outgoing data blocks to the CAD. In T=0 protocol, this method returns 258 (accounts for 2 status bytes).
getP(byte[], short) - Method in interface javacard.security.DSAKey
Returns the base parameter value of the key in plain text.
getP(byte[], short) - Method in interface javacard.security.RSAPrivateCrtKey
Returns the value of the P parameter in plain text.
getPQ(byte[], short) - Method in interface javacard.security.RSAPrivateCrtKey
Returns the value of the PQ parameter in plain text.

getPreviousContextAID() - Static method in class javacard.framework.JCSystem
This method is called to obtain the JCRE owned instance of the `AID` object associated with the previously active applet context.
getProtocol() - Static method in class javacard.framework.APDU
Returns the ISO 7816 transport protocol type, T=1 or T=0 in progress.
getQ(byte[], short) - Method in interface javacard.security.DSAKey
Returns the prime parameter value of the key in plain text.
getQ(byte[], short) - Method in interface javacard.security.RSAPrivateCrtKey
Returns the value of the Q parameter in plain text.
getReason() - Method in class javacard.framework.CardRuntimeException
Get reason code
getReason() - Method in class javacard.framework.CardException
Get reason code
getShareableInterfaceObject(AID, byte) - Method in class javacard.framework.Applet
Called by the JCRE to obtain a shareable interface object from this server applet, on behalf of a request from a client applet.
getShort(byte[], short) - Static method in class javacard.framework.Util
Concatenates two bytes in a byte array to form a short value.
getSize() - Method in interface javacard.security.Key
Returns the key size in number of bits.
getTransactionDepth() - Static method in class javacard.framework.JCSystem
Returns the current transaction nesting depth level.
getTriesRemaining() - Method in class javacard.framework.OwnerPIN
Returns the number of times remaining that an incorrect PIN can be presented before the `PIN` is blocked.
getTriesRemaining() - Method in interface javacard.framework.PIN
Returns the number of times remaining that an incorrect PIN can be presented before the `PIN` is blocked.
getType() - Method in interface javacard.security.Key
Returns the key interface type.
getUnusedCommitCapacity() - Static method in class javacard.framework.JCSystem
Returns the number of bytes left in the commit buffer.
getValidatedFlag() - Method in class javacard.framework.OwnerPIN
This protected method returns the validated flag.
getVersion() - Static method in class javacard.framework.JCSystem
Returns the current major and minor version of the Java Card API.
getX(byte[], short) - Method in interface javacard.security.DSAPrivateKey
Returns the value of the key in plain text.
getY(byte[], short) - Method in interface javacard.security.DSAPublicKey
Returns the value of the key in plain text.

I

ILLEGAL_AID - Static variable in class javacard.framework.SystemException
This reason code is used by the `javacard.framework.Applet.register()` method to indicate that the input AID parameter is not a legal AID value.

ILLEGAL_TRANSIENT - Static variable in class javacard.framework.SystemException
This reason code is used to indicate that the request to create a transient object is not allowed in the current applet context.

ILLEGAL_USE - Static variable in class javacard.framework.APDUException
This APDUException reason code indicates that the method should not be invoked based on the current state of the APDU.

ILLEGAL_USE - Static variable in class javacard.security.CryptoException
This reason code is used to indicate that the signature or cipher algorithm does not pad the incoming message and the input message is not block aligned.

ILLEGAL_VALUE - Static variable in class javacard.framework.PINException
This reason code is used to indicate that one or more input parameters is out of allowed bounds.

ILLEGAL_VALUE - Static variable in class javacard.framework.SystemException
This reason code is used to indicate that one or more input parameters is out of allowed bounds.

ILLEGAL_VALUE - Static variable in class javacard.security.CryptoException
This reason code is used to indicate that one or more input parameters is out of allowed bounds.

IN_PROGRESS - Static variable in class javacard.framework.TransactionException
This reason code is used by the `beginTransaction` method to indicate a transaction is already in progress.

IndexOutOfBoundsException - exception java.lang.IndexOutOfBoundsException.
A JCRE owned instance of `IndexOutOfBoundsException` is thrown to indicate that an index of some sort (such as to an array) is out of range.

IndexOutOfBoundsException() - Constructor for class java.lang.IndexOutOfBoundsException
Constructs an `IndexOutOfBoundsException`.

init(Key, byte) - Method in class javacard.security.Signature
Initializes the `Signature` object with the appropriate `Key`.

init(Key, byte) - Method in class javacardx.crypto.Cipher
Initializes the `Cipher` object with the appropriate `Key`.

init(Key, byte, byte[], short, short) - Method in class javacard.security.Signature
Initializes the `Signature` object with the appropriate `Key` and algorithm specific parameters.

init(Key, byte, byte[], short, short) - Method in class javacardx.crypto.Cipher
Initializes the `Cipher` object with the appropriate Key and algorithm specific parameters.

INS_EXTERNAL_AUTHENTICATE - Static variable in interface javacard.framework.ISO7816
APDU command INS : EXTERNAL AUTHENTICATE = 0x82

INS_SELECT - Static variable in interface javacard.framework.ISO7816
APDU command INS : SELECT = 0xA4

install(byte[], short, byte) - Static method in class javacard.framework.Applet
To create an instance of the `Applet` subclass, the JCRE will call this static method first.

INTERNAL_FAILURE - Static variable in class javacard.framework.TransactionException
This reason code is used during a transaction to indicate an internal JCRE problem (fatal error).

J

K

KeyEncryption - interface javacardx.crypto.KeyEncryption.
`KeyEncryption` interface defines the methods used to enable encrypted key data access to a key implementation.

L

LENGTH_DES - Static variable in class javacard.security.KeyBuilder
DES Key Length `LENGTH_DES` = 64.
LENGTH_DES3_2KEY - Static variable in class javacard.security.KeyBuilder
DES Key Length `LENGTH_DES3_2KEY` = 128.
LENGTH_DES3_3KEY - Static variable in class javacard.security.KeyBuilder
DES Key Length `LENGTH_DES3_3KEY` = 192.
LENGTH_DSA_1024 - Static variable in class javacard.security.KeyBuilder
DSA Key Length `LENGTH_DSA_1024` = 1024.
LENGTH_DSA_512 - Static variable in class javacard.security.KeyBuilder
DSA Key Length `LENGTH_DSA_512` = 512.
LENGTH_DSA_768 - Static variable in class javacard.security.KeyBuilder
DSA Key Length `LENGTH_DSA_768` = 768.
LENGTH_RSA_1024 - Static variable in class javacard.security.KeyBuilder
RSA Key Length `LENGTH_RSA_1024` = 1024.
LENGTH_RSA_2048 - Static variable in class javacard.security.KeyBuilder
RSA Key Length `LENGTH_RSA_2048` = 2048.
LENGTH_RSA_512 - Static variable in class javacard.security.KeyBuilder
RSA Key Length `LENGTH_RSA_512` = 512.
LENGTH_RSA_768 - Static variable in class javacard.security.KeyBuilder
RSA Key Length `LENGTH_RSA_768` = 768.
lookupAID(byte[], short, byte) - Static method in class javacard.framework.JCSystem
Returns the JCRE owned instance of the `AID` object, if any, encapsulating the specified AID bytes in the `buffer` parameter if there exists a successfully installed applet on the card whose instance AID exactly matches that of the specified AID bytes.

M

makeShort(byte, byte) - Static method in class javacard.framework.Util
Concatenates the two parameter bytes to form a short value.
makeTransientBooleanArray(short, byte) - Static method in class javacard.framework.JCSystem
Create a transient boolean array with the specified array length.
makeTransientByteArray(short, byte) - Static method in class javacard.framework.JCSystem
Create a transient byte array with the specified array length.
makeTransientObjectArray(short, byte) - Static method in class javacard.framework.JCSystem
Create a transient array of `Object` with the specified array length.
makeTransientShortArray(short, byte) - Static method in class javacard.framework.JCSystem
Create a transient short array with the specified array length.

MessageDigest - class javacard.security.MessageDigest.
The `MessageDigest` class is the base class for hashing algorthims.
MessageDigest() - Constructor for class javacard.security.MessageDigest
Protected Constructor
MODE_DECRYPT - Static variable in class javacardx.crypto.Cipher
Used in `init()` methods to indicate decryption mode.
MODE_ENCRYPT - Static variable in class javacardx.crypto.Cipher
Used in `init()` methods to indicate encryption mode.
MODE_SIGN - Static variable in class javacard.security.Signature
Used in `init()` methods to indicate signature sign mode.
MODE_VERIFY - Static variable in class javacard.security.Signature
Used in `init()` methods to indicate signature verify mode.

N

NegativeArraySizeException - exception java.lang.NegativeArraySizeException.
A JCRE owned instance of `NegativeArraySizeException` is thrown if an applet tries to create an array with negative size.
NegativeArraySizeException() - Constructor for class java.lang.NegativeArraySizeException
Constructs a `NegativeArraySizeException`.
NO_RESOURCE - Static variable in class javacard.framework.SystemException
This reason code is used to indicate that there is insufficient resource in the Card for the request.
NO_SUCH_ALGORITHM - Static variable in class javacard.security.CryptoException
This reason code is used to indicate that the requested algorithm or key type is not supported.
NO_T0_GETRESPONSE - Static variable in class javacard.framework.APDUException
This reason code indicates that during T=0 protocol, the CAD did not return a GET RESPONSE command in response to a <61xx> response status to send additional data.
NO_TRANSIENT_SPACE - Static variable in class javacard.framework.SystemException
This reason code is used by the `makeTransient..()` methods to indicate that no room is available in volatile memory for the requested object.
NOT_A_TRANSIENT_OBJECT - Static variable in class javacard.framework.JCSystem
This event code indicates that the object is not transient.
NOT_IN_PROGRESS - Static variable in class javacard.framework.TransactionException
This reason code is used by the `abortTransaction` and `commintTransaction` methods when a transaction is not in progress.
NullPointerException - exception java.lang.NullPointerException.
A JCRE owned instance of `NullPointerException`is thrown when an applet attempts to use `null` in a case where an object is required.
NullPointerException() - Constructor for class java.lang.NullPointerException
Constructs a `NullPointerException`.

O

Object - class java.lang.Object.
Class `Object` is the root of the Java Card class hierarchy.
Object() - Constructor for class java.lang.Object

OFFSET_CDATA - Static variable in interface javacard.framework.ISO7816
APDU command data offset : CDATA = 5
OFFSET_CLA - Static variable in interface javacard.framework.ISO7816
APDU header offset : CLA = 0
OFFSET_INS - Static variable in interface javacard.framework.ISO7816
APDU header offset : INS = 1
OFFSET_LC - Static variable in interface javacard.framework.ISO7816
APDU header offset : LC = 4
OFFSET_P1 - Static variable in interface javacard.framework.ISO7816
APDU header offset : P1 = 2
OFFSET_P2 - Static variable in interface javacard.framework.ISO7816
APDU header offset : P2 = 3
OwnerPIN - class javacard.framework.OwnerPIN.
This class represents an Owner PIN.
OwnerPIN(byte, byte) - Constructor for class javacard.framework.OwnerPIN
Constructor.

P

partialEquals(byte[], short, byte) - Method in class javacard.framework.AID
Checks if the specified partial AID byte sequence matches the first `length` bytes of the encapsulated AID bytes within `this AID` object.
PIN - interface javacard.framework.PIN.
This interface represents a PIN.
PINException - exception javacard.framework.PINException.
`PINException` represents a `OwnerPIN` class access-related exception.
PINException(short) - Constructor for class javacard.framework.PINException
Constructs a PINException.
PrivateKey - interface javacard.security.PrivateKey.
The `PrivateKey` class is the base class for private keys used in asymmetric algorithms.
process(APDU) - Method in class javacard.framework.Applet
Called by the JCRE to process an incoming APDU command.
PROTOCOL_T0 - Static variable in class javacard.framework.APDU
ISO 7816 transport protocol type T=0
PROTOCOL_T1 - Static variable in class javacard.framework.APDU
ISO 7816 transport protocol type T=1
PublicKey - interface javacard.security.PublicKey.
The `PublicKey` class is the base class for public keys used in asymmetric algorithms.

R

RandomData - class javacard.security.RandomData.
The `RandomData` abstract class is the base class for random number generation.

RandomData() - Constructor for class javacard.security.RandomData
Protected constructor for subclassing.

receiveBytes(short) - Method in class javacard.framework.APDU
Gets as many data bytes as will fit without APDU buffer overflow, at the specified offset `bOff`. Gets all the remaining bytes if they fit.

register() - Method in class javacard.framework.Applet
This method is used by the applet to register `this` applet instance with the JCRE and to assign the `Applet` subclass AID bytes as its instance AID bytes.

register(byte[], short, byte) - Method in class javacard.framework.Applet
This method is used by the applet to register `this` applet instance with the JCRE and assign the specified AID bytes as its instance AID bytes.

reset() - Method in class javacard.framework.OwnerPIN
If the validated flag is set, this method resets it.

reset() - Method in interface javacard.framework.PIN
If the validated flag is set, this method resets it.

resetAndUnblock() - Method in class javacard.framework.OwnerPIN
This method resets the validated flag and resets the `PIN` try counter to the value of the `PIN` try limit.

RIDEquals(AID) - Method in class javacard.framework.AID
Checks if the RID (National Registered Application provider identifier) portion of the encapsulated AID bytes within the `otherAID` object matches that of `this AID` object.

RSAPrivateCrtKey - interface javacard.security.RSAPrivateCrtKey.
The `RSAPrivateCrtKey` interface is used to sign data using the RSA algorithm in its Chinese Remainder Theorem form.

RSAPrivateKey - interface javacard.security.RSAPrivateKey.
The `RSAPrivateKey` class is used to sign data using the RSA algorithm in its modulus/exponent form.

RSAPublicKey - interface javacard.security.RSAPublicKey.
The `RSAPublicKey` is used to verify signatures on signed data using the RSA algorithm.

RuntimeException - exception java.lang.RuntimeException.
`RuntimeException` is the superclass of those exceptions that can be thrown during the normal operation of the Java Card Virtual Machine. A method is not required to declare in its throws clause any subclasses of `RuntimeException` that might be thrown during the execution of the method but not caught.

RuntimeException() - Constructor for class java.lang.RuntimeException
Constructs a `RuntimeException` instance.

S

SecretKey - interface javacard.security.SecretKey.
The `SecretKey` class is the base interface for keys used in symmetric alogrightms (e.g. DES).

SecurityException - exception java.lang.SecurityException.
A JCRE owned instance of `SecurityException` is thrown by the Java Card Virtual Machine to indicate a security violation. This exception is thrown when an attempt is made to illegally access an object belonging to a another applet.

SecurityException() - Constructor for class java.lang.SecurityException
Constructs a `SecurityException`.

select() - Method in class javacard.framework.Applet
Called by the JCRE to inform this applet that it has been selected.

selectingApplet() - Method in class javacard.framework.Applet
This method is used by the applet `process()` method to distinguish the SELECT APDU command which selected `this` applet, from all other other SELECT APDU commands which may relate to file or internal applet state selection.

sendBytes(short, short) - Method in class javacard.framework.APDU
Sends `len` more bytes from APDU buffer at specified offset `bOff`.

sendBytesLong(byte[], short, short) - Method in class javacard.framework.APDU
Sends `len` more bytes from `outData` byte array starting at specified offset `bOff`.

setDP1(byte[], short, short) - Method in interface javacard.security.RSAPrivateCrtKey
Sets the value of the DP1 parameter.

setDQ1(byte[], short, short) - Method in interface javacard.security.RSAPrivateCrtKey
Sets the value of the DQ1 parameter.

setExponent(byte[], short, short) - Method in interface javacard.security.RSAPrivateKey
Sets the private exponent value of the key.

setExponent(byte[], short, short) - Method in interface javacard.security.RSAPublicKey
Sets the public exponent value of the key.

setG(byte[], short, short) - Method in interface javacard.security.DSAKey
Sets the subprime parameter value of the key.

setIncomingAndReceive() - Method in class javacard.framework.APDU
This is the primary receive method.

setKey(byte[], short) - Method in interface javacard.security.DESKey
Sets the `Key` data.

setKeyCipher(Cipher) - Method in interface javacardx.crypto.KeyEncryption
Sets the `Cipher` object to be used to decrypt the input key data and key parameters in the set methods. Default `Cipher` object is `null` - no decryption performed.

setModulus(byte[], short, short) - Method in interface javacard.security.RSAPrivateKey
Sets the modulus value of the key.

setModulus(byte[], short, short) - Method in interface javacard.security.RSAPublicKey
Sets the modulus value of the key.

setOutgoing() - Method in class javacard.framework.APDU
This method is used to set the data transfer direction to outbound and to obtain the expected length of response (Le).

setOutgoingAndSend(short, short) - Method in class javacard.framework.APDU
This is the "convenience" send method.
setOutgoingLength(short) - Method in class javacard.framework.APDU
Sets the actual length of response data.
setOutgoingNoChaining() - Method in class javacard.framework.APDU
This method is used to set the data transfer direction to outbound without using BLOCK CHAINING(See ISO 7816-3/4) and to obtain the expected length of response (Le).
setP(byte[], short, short) - Method in interface javacard.security.DSAKey
Sets the base parameter value of the key.
setP(byte[], short, short) - Method in interface javacard.security.RSAPrivateCrtKey
Sets the value of the P parameter.
setPQ(byte[], short, short) - Method in interface javacard.security.RSAPrivateCrtKey
Sets the value of the PQ parameter.
setQ(byte[], short, short) - Method in interface javacard.security.DSAKey
Sets the prime parameter value of the key.
setQ(byte[], short, short) - Method in interface javacard.security.RSAPrivateCrtKey
Sets the value of the Q parameter.
setReason(short) - Method in class javacard.framework.CardRuntimeException
Set reason code
setReason(short) - Method in class javacard.framework.CardException
Set reason code
setSeed(byte[], short, short) - Method in class javacard.security.RandomData
Seeds the random data generator.
setShort(byte[], short, short) - Static method in class javacard.framework.Util
Deposits the short value as two successive bytes at the specified offset in the byte array.
setValidatedFlag(boolean) - Method in class javacard.framework.OwnerPIN
This protected method sets the value of the validated flag.
setX(byte[], short, short) - Method in interface javacard.security.DSAPrivateKey
Sets the value of the key.
setY(byte[], short, short) - Method in interface javacard.security.DSAPublicKey
Sets the value of the key.
Shareable - interface javacard.framework.Shareable.
The Shareable interface serves to identify all shared objects.
sign(byte[], short, short, byte[], short) - Method in class javacard.security.Signature
Generates the signature of all/last input data.
Signature - class javacard.security.Signature.
The `Signature` class is the base class for Signature algorthims.
Signature() - Constructor for class javacard.security.Signature
Protected Constructor
SW_APPLET_SELECT_FAILED - Static variable in interface javacard.framework.ISO7816
Response status : Applet selection failed = 0x6999;
SW_BYTES_REMAINING_00 - Static variable in interface javacard.framework.ISO7816
Response status : Response bytes remaining = 0x6100
SW_CLA_NOT_SUPPORTED - Static variable in interface javacard.framework.ISO7816
Response status : CLA value not supported = 0x6E00

SW_COMMAND_NOT_ALLOWED - Static variable in interface javacard.framework.ISO7816
Response status : Command not allowed (no current EF) = 0x6986
SW_CONDITIONS_NOT_SATISFIED - Static variable in interface javacard.framework.ISO7816
Response status : Conditions of use not satisfied = 0x6985
SW_CORRECT_LENGTH_00 - Static variable in interface javacard.framework.ISO7816
Response status : Correct Expected Length (Le) = 0x6C00
SW_DATA_INVALID - Static variable in interface javacard.framework.ISO7816
Response status : Data invalid = 0x6984
SW_FILE_FULL - Static variable in interface javacard.framework.ISO7816
Response status : Not enough memory space in the file = 0x6A84
SW_FILE_INVALID - Static variable in interface javacard.framework.ISO7816
Response status : File invalid = 0x6983
SW_FILE_NOT_FOUND - Static variable in interface javacard.framework.ISO7816
Response status : File not found = 0x6A82
SW_FUNC_NOT_SUPPORTED - Static variable in interface javacard.framework.ISO7816
Response status : Function not supported = 0x6A81
SW_INCORRECT_P1P2 - Static variable in interface javacard.framework.ISO7816
Response status : Incorrect parameters (P1,P2) = 0x6A86
SW_INS_NOT_SUPPORTED - Static variable in interface javacard.framework.ISO7816
Response status : INS value not supported = 0x6D00
SW_NO_ERROR - Static variable in interface javacard.framework.ISO7816
Response status : No Error = (short)0x9000
SW_RECORD_NOT_FOUND - Static variable in interface javacard.framework.ISO7816
Response status : Record not found = 0x6A83
SW_SECURITY_STATUS_NOT_SATISFIED - Static variable in interface javacard.framework.ISO7816
Response status : Security condition not satisfied = 0x6982
SW_UNKNOWN - Static variable in interface javacard.framework.ISO7816
Response status : No precise diagnosis = 0x6F00
SW_WRONG_DATA - Static variable in interface javacard.framework.ISO7816
Response status : Wrong data = 0x6A80
SW_WRONG_LENGTH - Static variable in interface javacard.framework.ISO7816
Response status : Wrong length = 0x6700
SW_WRONG_P1P2 - Static variable in interface javacard.framework.ISO7816
Response status : Incorrect parameters (P1,P2) = 0x6B00
SystemException - exception javacard.framework.SystemException.
`SystemException` represents a `JCSystem` class related exception.
SystemException(short) - Constructor for class javacard.framework.SystemException
Constructs a SystemException.

T

T1_IFD_ABORT - Static variable in class javacard.framework.APDUException
This reason code indicates that during T=1 protocol, the CAD returned an ABORT S-Block command and aborted the data transfer.

Throwable - class java.lang.Throwable.
The Throwable class is the superclass of all errors and exceptions in the Java Card subset of the Java language.

Throwable() - Constructor for class java.lang.Throwable
Constructs a new `Throwable`.

throwIt(short) - Static method in class javacard.framework.CardRuntimeException
Throw the JCRE owned instance of the `CardRuntimeException` class with the specified reason.

throwIt(short) - Static method in class javacard.framework.PINException
Throws the JCRE owned instance of `PINException` with the specified reason.

throwIt(short) - Static method in class javacard.framework.ISOException
Throws the JCRE owned instance of the ISOException class with the specified status word.

throwIt(short) - Static method in class javacard.framework.CardException
Throw the JCRE owned instance of `CardException` class with the specified reason.

throwIt(short) - Static method in class javacard.framework.UserException
Throws the JCRE owned instance of `UserException` with the specified reason.

throwIt(short) - Static method in class javacard.framework.SystemException
Throws the JCRE owned instance of `SystemException` with the specified reason.

throwIt(short) - Static method in class javacard.framework.TransactionException
Throws the JCRE owned instance of `TransactionException` with the specified reason.

throwIt(short) - Static method in class javacard.framework.APDUException
Throws the JCRE owned instance of `APDUException` with the specified reason.

throwIt(short) - Static method in class javacard.security.CryptoException
Throws the JCRE owned instance of `CryptoException` with the specified reason.

TransactionException - exception javacard.framework.TransactionException.
`TransactionException` represents an exception in the transaction subsystem.

TransactionException(short) - Constructor for class javacard.framework.TransactionException
Constructs a TransactionException with the specified reason.

TYPE_DES - Static variable in class javacard.security.KeyBuilder
`Key` object which implements interface type `DESKey` with persistent key data.

TYPE_DES_TRANSIENT_DESELECT - Static variable in class javacard.security.KeyBuilder
`Key` object which implements interface type `DESKey` with CLEAR_ON_DESELECT transient key data.

TYPE_DES_TRANSIENT_RESET - Static variable in class javacard.security.KeyBuilder
`Key` object which implements interface type `DESKey` with CLEAR_ON_RESET transient key data.

TYPE_DSA_PRIVATE - Static variable in class javacard.security.KeyBuilder
`Key` object which implements the interface type `DSAPrivateKey` for the DSA algorithm.

TYPE_DSA_PUBLIC - Static variable in class javacard.security.KeyBuilder
`Key` object which implements the interface type `DSAPublicKey` for the DSA algorithm.

TYPE_RSA_CRT_PRIVATE - Static variable in class javacard.security.KeyBuilder
`Key` object which implements interface type `RSAPrivateCrtKey` which uses Chinese Remainder Theorem.

TYPE_RSA_PRIVATE - Static variable in class javacard.security.KeyBuilder
`Key` object which implements interface type `RSAPrivateKey` which uses modulus/exponent form.

TYPE_RSA_PUBLIC - Static variable in class javacard.security.KeyBuilder
`Key` object which implements interface type `RSAPublicKey`.

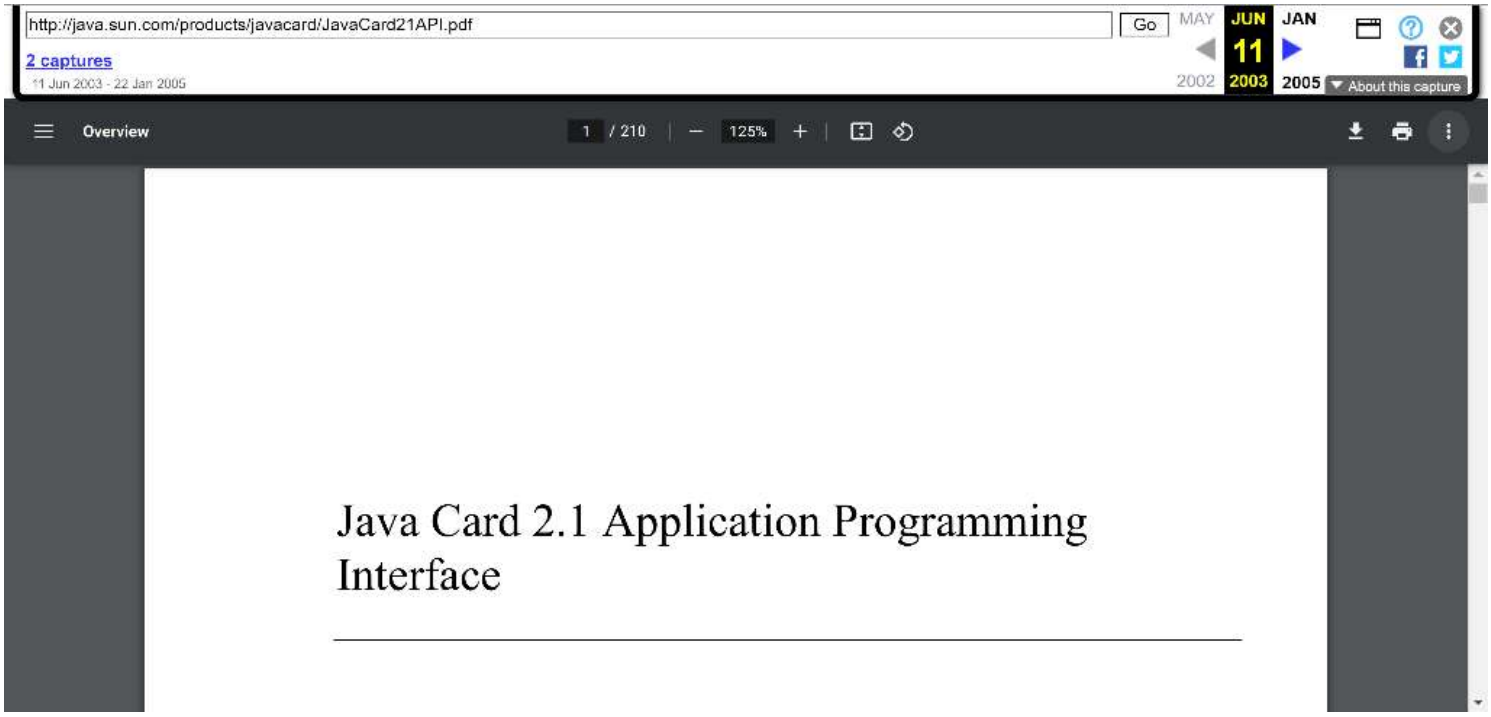
U

V

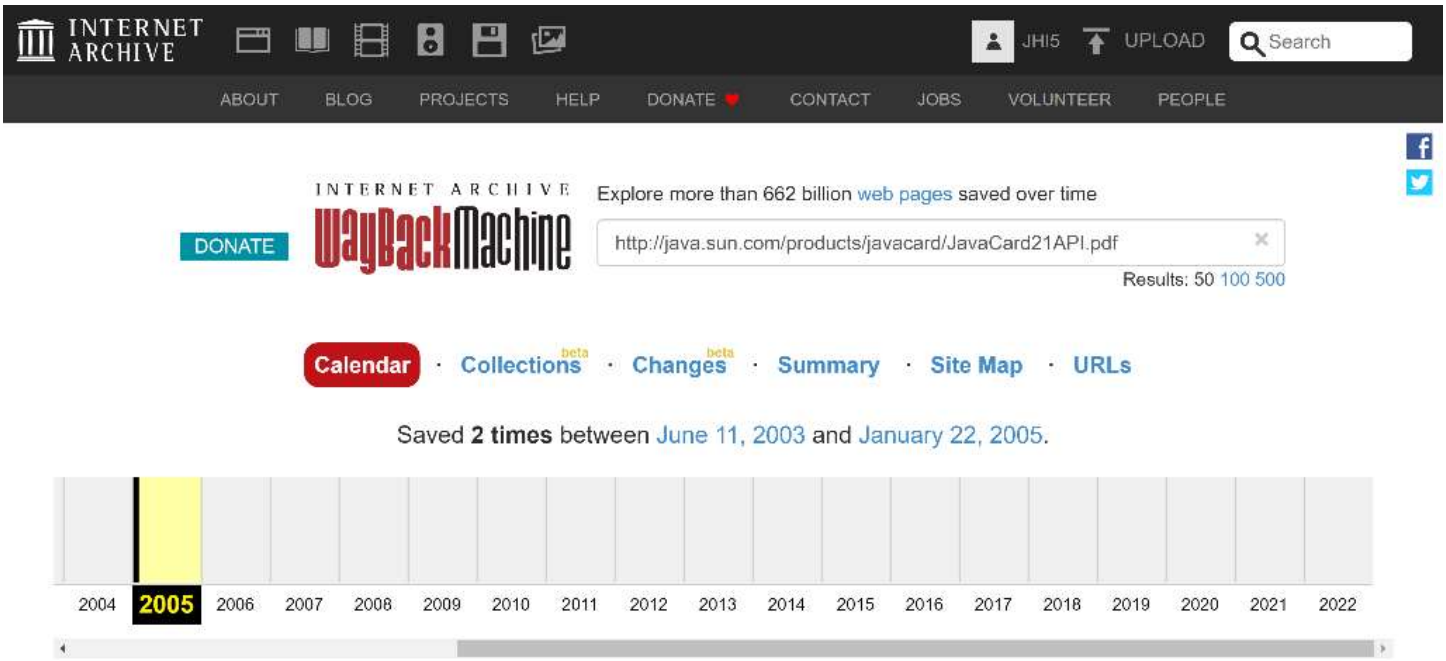
W

A B C D E G I J K L M N O P R S T U V W

screenshot-web.archive.org-2022.03.01-07_34_54
https://web.archive.org/web/20030611045849/http://java.sun.com/products/javacard/JavaCard21API.pdf
01.03.2022



screenshot-web.archive.org-2022.03.01-07_35_41
https://web.archive.org/web/2005/http://java.sun.com/products/javacard/JavaCard21API.pdf*
01.03.2022



23 24 25 26 27 28 29 27 28 29 30 25 26 27 28 29 30 31

30 31

Note

This calendar view maps the number of times **http://java.sun.com/products/javacard/JavaCard21API.pdf** was crawled by the Wayback Machine, *not* how many times the site was actually updated. More info in the FAQ.

Java Card™ Technology

Reference Implementation | Documentation | Datasheet

Java Card 2.1 Platform

The *Java Card 2.1 API Specification*, the *Java Card 2.1 Runtime Environment (JCRE) Specification* and the *Java Card 2.1 Virtual Machine Specification* are currently available.

Enhancements in this Release

For a more complete list of enhancements, please refer to the Release Notes.

- The *Java Card 2.1 Runtime Environment Specification* is a new document for Java Card 2.1. It specifies the details of the runtime environment for applet execution.
- The *Java Card 2.1 Virtual Machine Specification* is a new document for Java Card 2.1. It specifies the Java Card binary portability standards - the Java Card language subset, the Java Card Virtual Machine specifications and the binary representation of Java Card programs.
- The *Java Card 2.1 Application Programming Interfaces Specification* is a revision to the *Java Card 2.0 Application Programming Interfaces Specification*. It retains the basic functionality of 2.0 and improves and adds functions for real world card applications. The following is a list of the major enhancements and changes :
  - The newly restructured `javacard.security` and `javacardx.crypto` packages provide extensible support for security primitives. All the export controlled classes are packaged in `javacardx.crypto`.
  - The Firewall is more robust with explicit and detailed specifications. The object sharing mechanism uses a system channel for initial communication and allows applets to customize access control.
  - Applet programs are now more portable between various vendor implementations, and the applet creation API is installer independent.
  - Transient objects are now created using factory methods. This model is conveniently simulated on a workstation and provides intrinsic creation atomicity. Transient objects are now restricted to arrays.
  - A new parameter checking policy to insure behavior that is compatible among applets.
  - The Java Card 2.1 API re-defines the classes in `java.lang` as strict subsets of Java. This makes development and simulation of Java Card on a workstation simple and convenient.
  - The ISO 7816-4 file system extension package `javacardx.framework` has been deleted. The commonly used functionality in that package is better accomplished using simple Java objects in the application itself.

Java Card 2.1 API Specification

Working with the feedback from the Java Card platform licensees as well as the public, Sun engineers kept the basic functionality of 2.0 intact when adding features to the new and improved *Java Card 2.1*

API Specification. Developers will be comfortable with the consistent usability between the 2.0 and 2.1 APIs, and yet impressed with the updates and design enhancements in the new release.

The Java Card 2.1 Runtime Environment (JCRE) Specification

The JCRE 2.1 Specification complements the 2.1 API Specification and defines the necessary behavior of the runtime environment in any implementation of the Java Card technology. Such an implementation includes an implementation of the Java Card Virtual Machine, the Java Card Application Programming Interface (API) classes, and runtime support services such as the selection and deselection of applets.

The Java Card 2.1 Virtual Machine Specification

The *Java Card 2.1 Virtual Machine Specification* defines the features, services, and behavior required of an implementation of the Java Card technology. It includes the instruction set of a Java Card virtual machine, the supported subset of the Java language, and the file formats used for installing applets and libraries into devices, like smart cards, which implement Java Card technology.

Reference Implementation

You can download the Reference Implementation early access software and documentation from the Java Developer Connection℠ website. If you're not yet a member of the Java Card Developer Connection, you can register for free at the Java Card Developer Connection website.

Java Card 2.1 Platform Documentation

You can browse the Java Card API 2.1 Specification on line, or download the following documents:

- Java Card 2.1 API Specification (as a zipped set of HTML files)
- Java Card 2.1 API Specification (in a single PDF file)
- Java Card 2.1 API Specification Release Notes (PDF)
- Java Card 2.1 Runtime Environment (JCRE) Specification (PDF)
- Java Card 2.1 Virtual Machine (JCVM) Specification (PDF)
- Java Card 2.1 Virtual Machine Specification Release Notes (PDF)
- Documents Bundle - a zipped set of all of the above documents

Java Card 2.0 Platform Documentation

You can find documentation and Reference Implementation for the previous version of Java Card platform here.

screenshot-web.archive.org-2022.03.01-07_37_42
https://web.archive.org/web/19991103041851/http://www.java.sun.com:80/products/javacard/javacard21.html
01.03.2022

Java Card™ Technology

Reference Implementation | Documentation | Datasheet

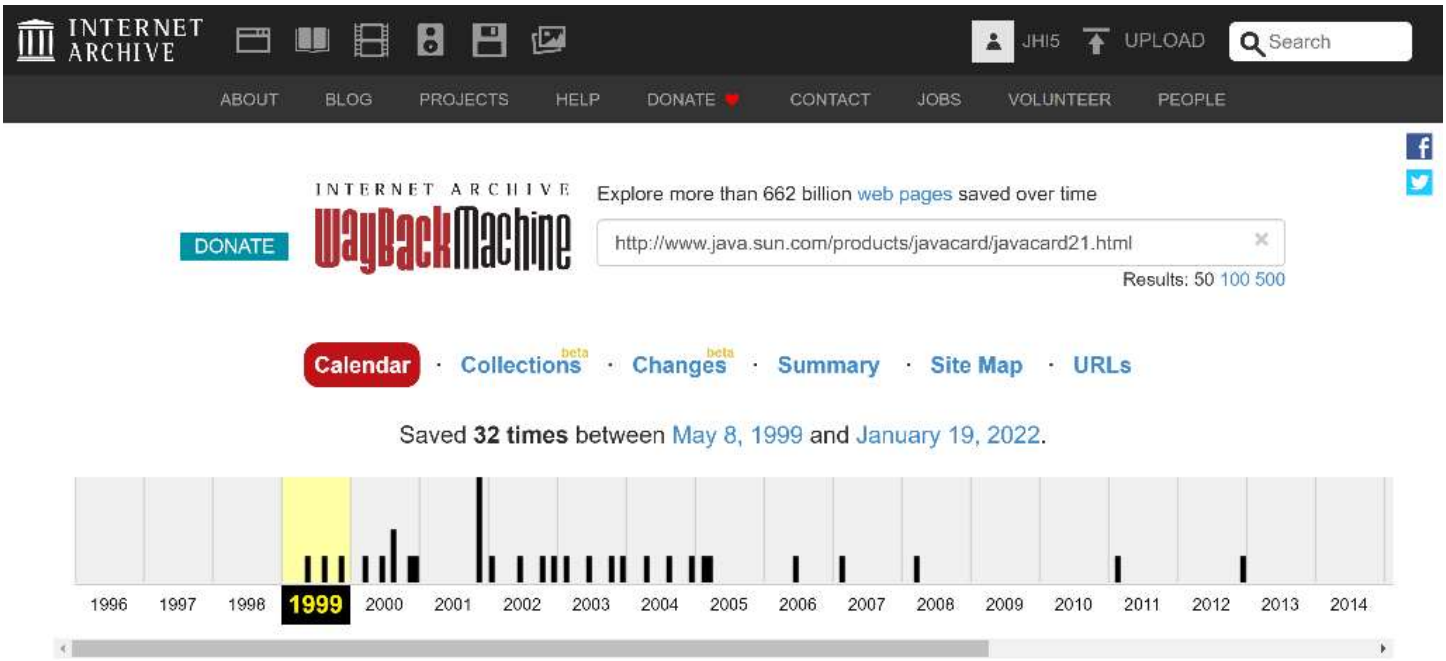
Java Card 2.1 Platform

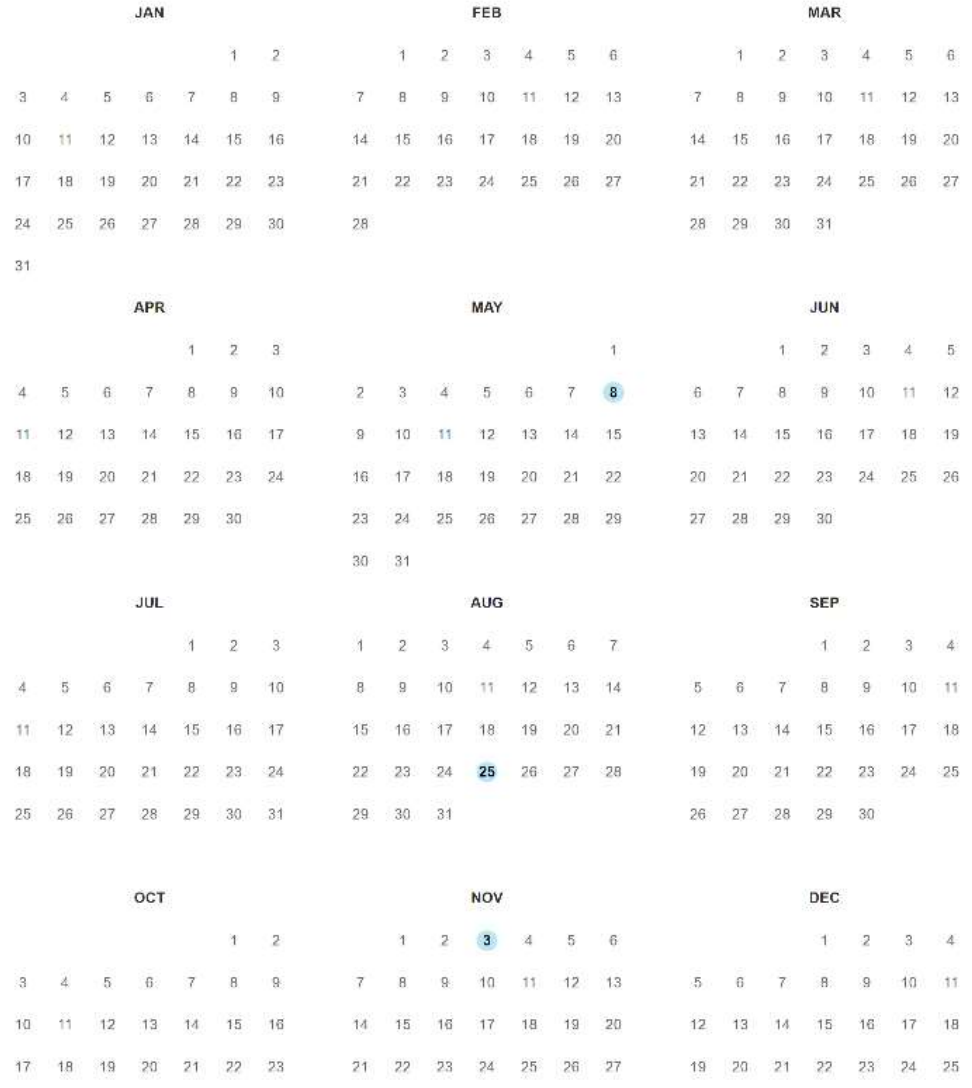
The *Java Card 2.1 API Specification*, the *Java Card 2.1 Runtime Environment (JCRE) Specification* and the *Java Card 2.1 Virtual Machine Specification* are currently available.

Enhancements in this Release

For a more complete list of enhancements, please refer to the Release Notes.

screenshot-web.archive.org-2022.03.01-07_41_02
https://web.archive.org/web/19991101000000*/http://www.java.sun.com/products/javacard/javacard21.html
01.03.2022





24 25 26 27 28 29 30 28 29 30 26 27 28 29 30 31

31

Note

This calendar view maps the number of times **http://www.java.sun.com/products/javacard/javacard21.html** was crawled by the Wayback Machine, *not* how many times the site was actually updated. More info in the FAQ.

Java Card ™ 2.1 Runtime Environment (JCRE) Specification

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303 USA
650 960-1300

Final Revision 1.0, February 24, 1999

Contents

Preface

Java Card™ technology combines a portion of the Java programming language with a runtime environment optimized for smart cards and related, small-memory embedded devices. The goal of Java Card technology is to bring many of the benefits of Java software programming to the resource-constrained world of smart cards.

This document is a specification of the Java Card 2.1 Runtime Environment (JCRE). A vendor of a Java Card-enabled device provides an implementation of the JCRE. A JCRE implementation within the context of this specification refers to a vendor's implementation of the Java Card Virtual Machine (VM), the Java Card Application Programming Interface (API), or other component, based on the Java Card technology specifications. A *Reference Implementation* is an implementation produced by Sun Microsystems, Inc. Applets written for the Java Card platform are referred to as Java Card applets.

Who Should Use This Specification?

This specification is intended to assist JCRE implementers in creating an implementation, developing a specification to extend the Java Card technology specifications, or in creating an extension to the Java Card Runtime Environment (JCRE). This specification is also intended for Java Card applet developers who want a greater understanding of the Java Card technology specifications.

Before You Read This Specification

Before reading this guide, you should be familiar with the Java programming language, the Java Card technology specifications, and smart card technology. A good resource for becoming familiar with Java technology and Java Card technology is the Sun Microsystems, Inc. website, located at: `http://java.sun.com`.

How This Specification Is Organized

Chapter 1, "The Scope and Responsibilities of the JCRE," gives an overview of the services required of a JCRE implementation.

Chapter 2, "Lifetime of the Java Card Virtual Machine," defines the lifetime of the Java Card Virtual Machine.

Chapter 3, "Java Card Applet Lifetime," defines the lifetime of an applet.

Chapter 4, "Selection," describes how the JCRE handles applet selection.

Chapter 5, "Transient Objects," describes the properties of transient objects.

Chapter 6, "Applet Isolation and Object Sharing," describes applet isolation and object sharing.

Chapter 7, "Transactions and Atomicity," describes the functionality of atomicity and transactions.

Chapter 8, "API Topics," describes API functionality required of a JCRE but not completely specified in the *Java Card 2.1 API Specification*.

Chapter 9, "Virtual Machine Topics," describes virtual machine specifics.

Chapter 10, "Applet Installer," provides an overview of the Applet Installer and JCRE required behavior.

Chapter 11, "API Constants," provides the numeric value of constants that are not specified in the *Java Card 2.1 API Specification*.

Glossary is a list of words and their definitions to assist you in using this book.

Related Documents and Publications

References to various documents or products are made in this manual. You should have the following documents available:

- *Java Card 2.1 API Specification*, Sun Microsystems, Inc.
- *Java Card 2.1 Virtual Machine Specification,* Sun Microsystems, Inc.
- *Java Card Applet Developer's Guide*, Sun Microsystems, Inc.
- *The Java Language Specification* by James Gosling, Bill Joy, and Guy L. Steele. Addison-Wesley, 1996, ISBN 0-201-63451-1.
- *The Java Virtual Machine Specification* (Java Series) by Tim Lindholm and Frank Yellin. Addison-Wesley, 1996, ISBN 0-201-63452-X.
- *The Java Class Libraries: An Annotated Reference (Java Series)* by Patrick Chan and Rosanna Lee. Addison-Wesley, two volumes, ISBN: 0201310023 and 0201310031.
- ISO 7816 Specification Parts 1-6.
- EMV '96 Integrated Circuit Card Specification for Payment Systems.

Appendix JCRE01

1. Introduction

The Java Card 2.1 Runtime Environment (JCRE) contains the Java Card Virtual Machine (VM), the Java Card Application Programming Interface (API) classes (and industry-specific extensions), and support services.

This document, the Java Card 2.1 Environment (JCRE) Specification, specifies the JCRE functionality required by the Java Card technology. Any implementation of Java Card technology shall provide this necessary behavior and environment.

Appendix JCRE01

2. Lifetime of the Java Card Virtual Machine

In a PC or workstation, the Java Virtual Machine runs as an operating system process. When the OS process is terminated, the Java applications and their objects are automatically destroyed.

In Java Card technology the execution lifetime of the Virtual Machine (VM) is the lifetime of the card. Most of the information stored on a card shall be preserved even when power is removed from the card. Persistent memory technology (such as EEPROM) enables a smart card to store information when power is removed. Since the VM and the objects created on the card are used to represent application information that is persistent, the Java Card VM appears to run forever. When power is removed, the VM only stops temporarily. When the card is next reset, the VM starts up again and recovers its previous object heap from persistent storage.

Aside from its persistent nature, the Java Card Virtual Machine is just like the Java Virtual Machine.

The card initialization time is the time after masking, and prior to the time of card personalization and issuance. At the time of card initialization, the JCRE is initialized. The framework objects created by the JCRE exist for the lifetime of the Virtual Machine. Because the execution lifetime of the Virtual Machine and the JCRE framework span CAD sessions of the card, the lifetimes of objects created by applets will also span CAD sessions. (CAD means Card Acceptance Device, or card reader. Card sessions are those periods when the card is inserted in the CAD, powered up, and exchanging streams of APDUs with the CAD. The card session ends when the card is removed from the CAD.) Objects that have this property are called persistent objects.

The JCRE implementer shall make an object persistent when:

- The `Applet.register` method is called. The JCRE stores a reference to the instance of the applet object. The JCRE implementer shall ensure that instances of class `applet` are persistent.
- A reference to an object is stored in a field of any other persistent object or in a class's static field. This requirement stems from the need to preserve the integrity of the JCRE's internal data structures.

Appendix JCRE01

3. Java Card Applet Lifetime

For the purposes of this specification, a Java Card applet's lifetime begins at the point that it has been correctly loaded into card memory, linked, and otherwise prepared for execution. (For the remainder of this specification, *applet* refers to an applet written for the Java Card platform.) Applets registered with the `Applet.register` method exist for the lifetime of the card. The JCRE initiates interactions with the applet via the applet's public methods `install`, `select`, `deselect`, and `process`. An applet shall implement the static `install(byte[], short, byte)` method. If the `install(byte[], short, byte)` method is not implemented, the applet's objects cannot be created or initialized. A JCRE implementation shall call an applet's `install`, `select`, `deselect`, and `process` methods as described below.

When the applet is installed on the smart card, the static `install(byte[], short, byte)` method is called once by the JCRE for each applet instance created. The JCRE shall not call the applet's constructor directly.

3.1 The Method `install`

When the `install(byte[], short, byte)` method is called, no objects of the applet exist. The main task of the `install` method within the applet is to create an instance of the `Applet` subclass using its constructor, and to register the instance. All other objects that the applet will need during its lifetime can be created as is feasible. Any other preparations necessary for the applet to be selected and accessed by a CAD also can be done as is feasible. The `install` method obtains initialization parameters from the contents of the incoming byte array parameter.

Typically, an applet creates various objects, initializes them with predefined values, sets some internal state variables, and calls either the `Applet.register()` method or the `Applet.register(byte[], short, byte)` method to specify the AID (applet IDentifier as defined in ISO 7816-5) to be used to select it. This installation is considered successful when the call to the `Applet.register` method completes without an exception. The installation is deemed unsuccessful if the `install` method does not call the `Applet.register` method, or if an exception is thrown from within the `install` method prior to the `Applet.register` method being called, or if the `Applet.register` method throws an exception. If the installation is unsuccessful, the JCRE shall perform all cleanup when it regains control. That is, all persistent objects shall be returned to the state they had prior to calling the `install` method. If the installation is successful, the JCRE can mark the applet as available for selection.

3.2 The Method `select`

Applets remain in a suspended state until they are explicitly selected. Selection occurs when the JCRE receives a SELECT APDU in which the name data matches the AID of the applet. Selection causes an applet to become the currently selected applet.

Prior to calling SELECT, the JCRE shall deselect the previously selected applet. The JCRE indicates this to the applet by invoking the applet's `deselect` method.

The JCRE informs the applet of selection by invoking its `select()` method.

The applet may decline to be selected by returning `false` from the call to the `select` method or by throwing an exception. If the applet returns `true`, the actual SELECT APDU command is supplied to the applet in the subsequent call to its `process` method, so that the applet can examine the APDU contents. The applet can process the SELECT APDU command exactly like it processes any other APDU command. It can respond to the SELECT APDU with data (see the `process` method for details), or it can flag errors by throwing an `ISOException` with the appropriate SW (returned status word). The SW and optional response data are returned to the CAD.

The `Applet.selectingApplet` method shall return true when called during the `select` method. The `Applet.selectingApplet` method will continue to return true during the subsequent `process` method, which is called to process the SELECT APDU command.

If the applet declines to be selected, the JCRE will return an APDU response status word of `ISO7816.SW_APPLET_SELECT_FAILED` to the CAD. Upon selection failure, the JCRE state is set to indicate that no applet is selected. (See section 4.2 for more details).

After successful selection, all subsequent APDUs are delivered to the currently selected applet via the `process` method.

3.3 The Method `process`

All APDUs are received by the JCRE, which passes an instance of the APDU class to the `process(APDU)` method of the currently selected applet.

Note – A SELECT APDU might cause a change in the currently selected applet prior to the call to the `process` method. (The actual change occurs before the call to the `select` method).

On normal return, the JCRE automatically appends 0x9000 as the completion response SW to any data already sent by the applet.

At any time during `process`, the applet may throw an `ISOException` with an appropriate SW, in which case the JCRE catches the exception and returns the SW to the CAD.

If any other exception is thrown during `process`, the JCRE catches the exception and returns the status word `ISO7816.SW_UNKNOWN` to the CAD.

3.4 The Method `deselect`

When the JCRE receives a SELECT APDU command in which the name matches the AID of an applet, the JCRE calls the `deselect()` method of the currently selected applet. This allows the applet to perform any cleanup operations that may be required in order to allow some other applet to execute.

The `Applet.selectingApplet` method shall return false when called during the `deselect` method. Exceptions thrown by the `deselect` method are caught by the JCRE, but the applet is deselected.

3.5 Power Loss and Reset

Power loss occurs when the card is withdrawn from the CAD or if there is some other mechanical or electrical failure. When power is reapplied to the card and on card reset (warm or cold) the JCRE shall ensure that:

- Transient data is reset to the default value.
- The transaction in progress, if any, when power was lost (or reset occurred) is aborted.
- The applet that was selected when power was lost (or reset occurred) becomes implicitly deselected. (In this case the `deselect` method is not called.)
- If the JCRE implements default applet selection (see section 4.1), the default applet is selected as the currently selected applet, and the default applet's `select` method is called. Otherwise, the JCRE sets its state to indicate that no applet is selected.

Appendix JCRE01

4. Selection

Cards receive requests for service from the CAD in the form of APDUs. The SELECT APDU is used by the JCRE to designate a *currently selected applet*. Once selected, an applet receives all subsequent APDUs until the applet becomes deselected.

There is no currently selected applet when either of the following occurs:

- The card is reset and no applet has been pre-designated as the *default applet*.
- A SELECT command fails when attempting to select an applet via its `select` method .

4.1 The Default Applet

Normally, applets become selected only via a successful SELECT command. However, some smart card CAD applications require that there be a default applet that is implicitly selected after every card reset. The behavior is:

1. After card reset (or power on, which is a form of reset) the JCRE performs its initializations and checks to see if its internal state indicates that a particular applet is the default applet. If so, the JCRE makes this applet the currently selected applet, and the applet's `select` method is called. If the applet's `select` method throws an exception or returns `false`, then the JCRE sets its state to indicate that no applet is selected. (The applet's `process` method is not called during default applet selection because there is no SELECT APDU.) When a default applet is selected at card reset, it shall not require its `process` method to be called.
2. The JCRE ensures that the ATR has been sent and the card is now ready to accept APDU commands.

If a default applet was successfully selected, then APDU commands can be sent directly to this applet. If a default applet was not selected, then only SELECT commands for applet selection can be processed.

The mechanism for specifying a default applet is not defined in the Java Card 2.1 API. It is a JCRE implementation detail and is left to the individual JCRE implementers.

4.2 SELECT Command Processing

The SELECT APDU command is used to select an applet. Its behavior is:

1. The SELECT APDU is always processed by the JCRE regardless of which, if any, applet is active.

2. The JCRE searches the internal applet table which lists all successfully installed applets on the card for a matching AID. The JCRE shall support selecting an applet where the full AID is present in the SELECT command.

   JCRE implementers are free to enhance their JCRE to support other selection criterion. An example of this is selection via partial AID match as specified in ISO 7816-4. The specific requirements are as follows:

Note – An asterisk indicates binary notation(%b) using bit numbering as in ISO7816. Most significant bit = b8. Least significant bit = b1.

---

   a) Applet SELECT command uses CLA=0x00, INS=0xA4.

   b) Applet SELECT command uses "Selection by DF name". Therefore, P1=0x04.

   c) Any other value of P1 implies that is not an applet select. The APDU is processed by the currently selected applet.

   d) JCRE shall support exact DF name (AID) selection (i.e. P2=%b0000xx00). (b4,b3* are don't care).

   e) All other partial DF name SELECT options (b2,b1*) are JCRE implementation dependent.

   f) All file control information option codes (b4,b3*) shall be supported by the JCRE and interpreted and processed by the applet.

3. If no AID match is found:

   a. If there is no currently selected applet, the JCRE responds to the SELECT command with status code 0x6999 (SW_APPLET_SELECT_FAILED).

   b. Otherwise, the SELECT command is forwarded to the currently selected applet's `process` method. A context switch into the applet's context occurs at this point. (Context of an applet is defined in section 6.1.1.) Applets may use the SELECT APDU command for their own internal SELECT processing.

4. If a matching AID is found, the JCRE prepares to select the new applet. If there is an currently selected applet, it is deselected via a call to its `deselect` method. A context switch into the deselected applet's context occurs at this point. The JCRE context is restored upon exit from `deselect`.

5. The JCRE now clears the fields of all CLEAR_ON_DESELECT transient objects (see section 5.1) owned by the applet being deselected.

6. The JCRE sets the new currently selected applet. The new applet is selected via a call to its select method, and a context switch into the new applet's context occurs

   a. If the applet's `select` method throws an exception or returns `false`, then the JCRE state is set so that no applet is selected. The JCRE responds to the SELECT command with status code 0x6999 (SW_APPLET_SELECT_FAILED).

b. The new currently selected applet's `process` method is then called with the SELECT APDU as an input parameter. A context switch into the applet's context occurs.

Notes –

If there is no matching AID, the SELECT command is forwarded to the currently selected applet (if any) for processing as a normal applet APDU command.

If there is a matching AID and the SELECT command fails, the JCRE always enters the state where no applet is selected.

If the matching AID is the same as the currently selected applet, the JCRE still goes through the process of deselecting the applet and then selecting it. Reselection could fail, leaving the card in a state where no applet is selected.

4.3 Non-SELECT Command Processing

When a non-SELECT APDU is received and there is no currently selected applet, the JCRE shall respond to the APDU with status code 0x6999 (SW_APPLET_SELECT_FAILED).

When a non-SELECT APDU is received and there is a currently selected applet, the JCRE invokes the `process` method of the currently selected applet passing the APDU as a parameter. This causes a context switch from the JCRE context into the currently selected applet's context. When the `process` method exits, the VM switches back to the JCRE context. The JCRE sends a response APDU and waits for the next command APDU.

Appendix JCRE01

5. Transient Objects

Applets sometimes require objects that contain temporary (transient) data that need not be persistent across CAD sessions. Java Card does not support the Java keyword `transient`. However, Java Card technology provides methods to create transient arrays with primitive components or references to `Object`.

The term “transient object” is a misnomer. It can be incorrectly interpreted to mean that the object itself is transient. However, only the *contents* of the fields of the object (except for the length field) have a transient nature. As with any other object in the Java programming language, transient objects within the Java Card platform exist as long as they are referenced from:

- The stack
- Local variables
- A class static field
- A field in another existing object

A transient object within the Java Card platform has the following required behavior:

- The fields of a transient object shall be *cleared* to the field’s default value (zero, false, or `null`) at the occurrence of certain events (see section 5.1).
- For security reasons, the fields of a transient object shall never be stored in a “persistent memory technology.” Using current smart card technology as an example, the contents of transient objects can be stored in RAM, but never in EEPROM. The purpose of this requirement is to allow transient objects to be used to store session keys.
- Writes to the fields of a transient object shall not have a performance penalty. (Using current smart card technology as an example, the contents of transient objects can be stored in RAM, while the contents of persistent objects can be stored in EEPROM. Typically, RAM technology has a much faster write cycle time than EEPROM.)
- Writes to the fields of a transient object shall not be affected by “transactions.” That is, an `abortTransaction` will never cause a field in a transient object to be restored to a previous value.

This behavior makes transient objects ideal for small amounts of temporary applet data that is frequently modified, but that need not be preserved across CAD or select sessions.

5.1 Events That Clear Transient Objects

Persistent objects are used for maintaining states that shall be preserved across card resets. When a transient object is created, one of two events is specified that causes its fields to be cleared. CLEAR_ON_RESET transient objects are used for maintaining states that shall be preserved across applet selections, but not across card resets. CLEAR_ON_DESELECT transient objects are used for maintaining states that must be preserved while an applet is selected, but not across applet selections or card resets.

Details of the two clear events are as follows:

- CLEAR_ON_RESET—the object's fields (except for the length field) are cleared when the card is reset. When a card is powered on, this also causes a card reset.

  Note – It is not necessary to clear the fields of transient objects before power is removed from a card. However, it is necessary to guarantee that the previous contents of such fields cannot be recovered once power is lost.

- CLEAR_ON_DESELECT—the object's fields (except for the length field) are cleared whenever the applet is deselected. Because a card reset implicitly deselects the currently selected applet, the fields of CLEAR_ON_DESELECT objects are also cleared by the same events specified for CLEAR_ON_RESET.

The currently selected applet is explicitly deselected (its `deselect` method is called) only when a SELECT command is processed. The currently selected applet is deselected and then the fields of all CLEAR_ON_DESELECT transient objects owned by the applet are cleared regardless of whether the SELECT command:

- Fails to select an applet.
- Selects a different applet.
- Reselects the same applet.

6. Applet Isolation and Object Sharing

Any implementation of the JCRE shall support isolation of contexts and applets. Isolation means that one applet can not access the fields or objects of an applet in another context unless the other applet explicitly provides an interface for access. The JCRE mechanisms for applet isolation and object sharing are detailed in the sections below.

6.1 Applet Firewall

The *applet firewall* within Java Card technology is runtime-enforced protection and is separate from the Java technology protections. The Java language protections still apply to Java Card applets. The Java language ensures that strong typing and protection attributes are enforced.

Applet firewalls are always enforced in the Java Card VM. They allow the VM to automatically perform additional security checks at runtime.

6.1.1 Contexts and Context Switching

Firewalls essentially partition the Java Card platform's object system into separate protected object spaces called *contexts*. The firewall is the boundary between one context and another. The JCRE shall allocate and manage a *context* for each applet that is installed on the card. (But see section 6.1.1.2 below for a discussion of group contexts.)

In addition, the JCRE maintains its own *JCRE context*. This context is much like the context of an applet, but it has special system privileges so that it can perform operations that are denied to contexts of applets.

At any point in time, there is only one *active context* within the VM. (This is called the *currently active context*.) All bytecodes that access objects are checked at *runtime* against the currently active context in order to determine if the access is allowed. A `java.lang.SecurityException` is thrown when an access is disallowed.

When certain well-defined conditions are met during the execution of invoke-type bytecodes as described in section 6.2.8, the VM performs a *context switch*. The previous context is pushed on an internal VM stack, a new context becomes the currently active context, and the invoked method executes in this new context. Upon exit from that method the VM performs a restoring context switch. The original context (of the caller of the method) is popped from the stack and is restored as the currently active context. Context switches can be nested. The maximum depth depends on the amount of VM stack space available.

Most method invocations in Java Card technology do not cause a context switch. Context switches only occur during invocation of and return from certain methods, as well as during exception exits from those methods (see 6.2.8).

During a context-switching method invocation, an additional piece of data, indicating the currently active context, is pushed onto the return stack. This context is restored when the method is exited.

Further details of contexts and context switching are provided in later sections of this chapter.

6.1.1.1 Group Contexts

Usually, each instance of a Java Card applet defines a separate context. But with Java Card 2.1 technology, the concept of *group context* is introduced. If more than one applet is contained in a single Java package, they share the same context. Additionally, all instances of the same applet class share the same context. In other words, there is no firewall between two applet instances in a group context.

The discussion of contexts and context switching above in section 6.1.1 assumes that each applet instance is associated with a separate context. In Java Card 2.1 technology, contexts are compared to enforce the firewall, and the instance AID is pushed onto the stack. Additionally, this happens not only when the context switches, but also when control switches from an object owned by one applet instance to an object owned by another instance within the same package.

6.1.2 Object Ownership

When a new object is created, it is associated with the currently active context. But the object is *owned* by the applet instance within the currently active context when the object is instantiated. An object is owned by an applet instance, or by the JCRE.

6.1.3 Object Access

In general, an object can only be *accessed* by its owning context, that is, when the owning context is the currently active context. The firewall prevents an object from being accessed by another applet in a different context.

In implementation terms, each time an object is accessed, the object's owner context is compared to the currently active context. If these do not match, the access is not performed and a `SecurityException` is thrown.

An object is accessed when one of the following bytecodes is executed using the object's reference:

```
getfield, putfield, invokevirtual, invokeinterface,
athrow, <T>aload, <T>astore, arraylength, checkcast, instanceof
```

`<T>` refers to the various types of array bytecodes, such as `baload`, `sastore`, etc.

This list includes any special or optimized forms of these bytecodes implemented in the Java Card VM, such as `getfield_b`, `sgetfield_s_this`, etc.

6.1.4 Firewall Protection

The Java Card firewall provides protection against the most frequently anticipated security concern: developer mistakes and design oversights that might allow sensitive data to be "leaked" to another applet. An applet may be able to obtain an object reference from a publicly accessible location, but if the object is owned by an applet in another context, the firewall ensures security.

The firewall also provides protection against incorrect code. If incorrect code is loaded onto a card, the firewall still protects objects from being accessed by this code.

The *Java Card 2.1 JCRE Specification* specifies the basic minimum protection requirements of contexts and firewalls because the features described in this document are not transparent to the applet developer. Developers shall be aware of the behavior of objects, APIs, and exceptions related to the firewall.

JCRE implementers are free to implement additional security mechanisms beyond those of the applet firewall, as long as these mechanisms are transparent to applets and do not change the externally visible operation of the VM.

6.1.5 Static Fields and Methods

It should also be noted that classes are not owned by contexts. There is no runtime context check that can be performed when a class static field is accessed. Neither is there a context switch when a static method is invoked. (Similarly, `invokespecial` causes no context switch.)

Public static fields and public static methods are accessible from any context: static methods execute in the same context as their caller.

Objects referenced in static fields are just regular objects. They are owned by whomever created them and standard firewall access rules apply. If it is necessary to share them across multiple contexts, then these objects need to be *Shareable Interface Objects* (SIOs). (See section 6.2.4 below.)

Of course, the conventional Java technology protections are still enforced for static fields and methods. In addition, when applets are installed, the Installer verifies that each attempt to link to an external static field or method is permitted. Installation and specifics about linkage are beyond the scope of this specification.

6.1.5.1 Optional static access checks

The JCRE may perform optional runtime checks that are redundant with the constraints enforced by a verifier. A Java Card VM may detect when code violates fundamental language restrictions, such as invoking a private method in another class, and report or otherwise address the violation.

6.2 Object Access Across Contexts

To enable applets to interact with each other and with the JCRE, some well-defined yet secure mechanisms are provided so one context can access an object belonging to another context.

These mechanisms are provided in the Java Card 2.1 API and are discussed in the following sections:

- JCRE Entry Point Objects
- Global Arrays
- JCRE Privileges
- Shareable Interfaces

6.2.1 JCRE Entry Point Objects

Secure computer systems must have a way for non-privileged user processes (that are restricted to a subset of resources) to request system services performed by privileged “system” routines.

In the Java Card 2.1 API, this is accomplished using *JCRE Entry Point Objects*. These are objects owned by the JCRE context, but they have been flagged as containing entry point methods.

The firewall protects these objects from access by applets. The entry point designation allows the methods of these objects to be invoked from any context. When that occurs, a context switch to the JCRE context is performed. These methods are the gateways through which applets request privileged JCRE system services.

There are two categories of JCRE Entry Point Objects :

- Temporary JCRE Entry Point Objects

  Like all JCRE Entry Point Objects, methods of temporary JCRE Entry Point Objects can be invoked from any context. However, references to these objects cannot be stored in class variables, instance variables or array components. The JCRE detects and restricts attempts to store references to these objects as part of the firewall functionality to prevent unauthorized re-use.

  The APDU object and all JCRE owned exception objects are examples of temporary JCRE Entry Point Objects.

- Permanent JCRE Entry Point Objects

  Like all JCRE Entry Point Objects, methods of permanent JCRE Entry Point Objects can be invoked from any context. Additionally, references to these objects can be stored and freely re-used.

  JCRE owned AID instances are examples of permanent JCRE Entry Point Objects.

The JCRE is responsible for:

- Determining what privileged services are provided to applets.
- Defining classes containing the entry point methods for those services.
- Creating one or more object instances of those classes.
- Designating those instances as JCRE Entry Point Objects.
- Designating JCRE Entry Point Objects as temporary or permanent.
- Making references to those objects available to applets as needed.

Note – Only the *methods* of these objects are accessible through the firewall. The fields of these objects are still protected by the firewall and can only be accessed by the JCRE context.

Only the JCRE itself can designate Entry Point Objects and whether they are temporary or permanent. JCRE implementers are responsible for implementing the mechanism by which JCRE Entry Point Objects are designated and how they become temporary or permanent.

6.2.2 Global Arrays

The global nature of some objects requires that they be accessible from any context. The firewall would ordinarily prevent these objects from being used in a flexible manner. The Java Card VM allows an object to be designated as *global*.

All global arrays are temporary global array objects. These objects are owned by the JCRE context, but can be accessed from any context. However, references to these objects cannot be stored in class variables, instance

variables or array components. The JCRE detects and restricts attempts to store references to these objects as part of the firewall functionality to prevent unauthorized re-use.

For added security, only arrays can be designated as global and only the JCRE itself can designate global arrays. Because applets cannot create them, no API methods are defined. JCRE implementers are responsible for implementing the mechanism by which global arrays are designated.

At the time of publication of this specification, the only global arrays required in the Java Card 2.1 API are the APDU buffer and the byte array input parameter (`bArray`) to the applet's `install` method.

Note – Because of its global status, the *Java Card 2.1 API Specification* specifies that the APDU buffer is cleared to zeroes whenever an applet is selected, before the JCRE accepts a new APDU command. This is to prevent an applet's potentially sensitive data from being "leaked" to another applet via the global APDU buffer. The APDU buffer can be accessed from a shared interface object context and is suitable for passing data across different contexts. The applet is responsible for protecting secret data that may be accessed from the APDU buffer.

6.2.3 JCRE Privileges

Because it is the "system" context, the JCRE context has a special privilege. It can invoke a method of any object on the card. For example, assume that object X is owned by applet A. Normally, only the context of A can access the fields and methods of X. But the JCRE context is allowed to invoke any of the methods of X. During such an invocation, a context switch occurs from the JCRE context to the context of the applet that owns X.

Note – The JCRE can access both *methods* and *fields* of X. Method access is the mechanism by which the JCRE enters the context of an applet. Although the JCRE could invoke any method through the firewall, it shall only invoke the `select`, `process`, `deselect`, and `getShareableInterfaceObject` (see 6.2.7.1) methods defined in the `Applet` class, and methods on the objects passed to the API as parameters.

The JCRE context is the currently active context when the VM begins running after a card reset. The JCRE context is the "root" context and is always either the currently active context or the bottom context saved on the stack.

6.2.4 Shareable Interfaces

Shareable interfaces are a new feature in the Java Card 2.1 API to enable applet interaction. A shareable interface defines a set of shared interface methods. These interface methods can be invoked from one context even if the object implementing them is owned by an applet in another context.

In this specification, an object instance of a class implementing a shareable interface is called a *Shareable Interface Object (SIO).*

To the owning context, the SIO is a normal object whose fields and methods can be accessed. To any other context, the SIO is an instance of the shareable interface, and only the methods defined in the shareable interface are accessible. All other fields and methods of the SIO are protected by the firewall.

Shareable interfaces provide a secure mechanism for inter-applet communication, as follows:

6.2.4.1 Server applet A builds a Shareable Interface Object

1. To make an object available for sharing with another applet in a different context, applet A first defines a shareable interface, SI. A shareable interface extends the interface

`javacard.framework.Shareable`. The methods defined in the shareable interface, SI, represent the services that applet A makes accessible to other applets.

2. Applet A then defines a class C that implements the shareable interface SI. C implements the methods defined in SI. C may also define other methods and fields, but these are protected by the applet firewall. Only the methods defined in SI are accessible to other applets.

3. Applet A creates an object instance O of class C. O belongs to applet A, and the firewall allows A to access any of the fields and methods of O.

6.2.4.2 Client applet B obtains the Shareable Interface Object

1. To access applet A's object O, applet B creates an object reference SIO of type SI.

2. Applet B invokes a special method (`JCSystem.getAppletShareableInterfaceObject`, described in section 6.2.7.2) to request a shared interface object reference from applet A.

3. Applet A receives the request and the AID of the requester (B) via `Applet.getShareableInterfaceObject`, and determines whether or not it will share object O with applet B. A's implementation of the `getShareableInterfaceObject` method executes in A's context.

4. If applet A agrees to share with applet B, A responds to the request with a reference to O. As this reference is returned as type `Shareable`, none of the fields or methods of O are visible.

5. Applet B receives the object reference from applet A, casts it to the interface type SI, and stores it in object reference variable SIO. Even though SIO actually refers to A's object O, SIO is an interface of type SI. Only the shareable interface methods defined in SI are visible to B. The firewall prevents the other fields and methods of O from being accessed by B.

In the above sequence, applet B initiates communication with applet A using the special system method in the `JCSystem` class to request a Shareable Interface Object from applet A. Once this communication is established, applet B can obtain other Shareable Interface Objects from applet A using normal parameter passing and return mechanisms. It can also continue to use the special `JCSystem` method described above to obtain other Shareable Interface Objects.

6.2.4.3 Client applet B requests services from applet A

1. Applet B can request service from applet A by invoking one of the shareable interface methods of SIO. During the invocation the Java Card VM performs a context switch. The original currently active context (B) is saved on a stack and the context of the owner (A) of the actual object (O) becomes the new currently active context. A's implementation of the shareable interface method (SI method) executes in A's context.

2. The SI method can find out the AID of its client (B) via the `JCSystem.getPreviousContextAID` method. This is described in section 6.2.5. The method determines whether or not it will perform the service for applet B.

3. Because of the context switch, the firewall allows the SI method to access all the fields and methods of object O and any other object in the context of A. At the same time, the firewall prevents the method from accessing non-shared objects in the context of B.

4. The SI method can access the parameters passed by B and can provide a return value to B.

5. During the return, the Java Card VM performs a restoring context switch. The original currently active context (B) is popped from the stack, and again becomes the current context.

6. Because of the context switch, the firewall again allows B to access any of its objects and prevents B from accessing non-shared objects in the context of A.

6.2.5 Determining the Previous Context

When an applet calls `JCSystem.getPreviousContextAID`, the JCRE shall return the instance AID of the applet instance active at the time of the last context switch.

6.2.5.1 The JCRE Context

The JCRE context does not have an AID. If an applet calls the `getPreviousContextAID` method when the context of the applet was entered directly from the JCRE context, this method returns `null`.

If the applet calls `getPreviousContextAID` from a method that may be accessed either from within the applet itself or when accessed via a shareable interface from an external applet, it shall check for `null` return before performing caller AID authentication.

6.2.6 Shareable Interface Details

A shareable interface is simply one that extends (either directly or indirectly) the *tagging* interface `javacard.framework.Shareable`. This `Shareable` interface is similar in concept to the `Remote` interface used by the RMI facility, in which calls to the interface methods take place across a local/remote boundary.

6.2.6.1 The Java Card Shareable Interface

Interfaces extending the `Shareable` tagging interface have this special property: calls to the interface methods take place across Java Card's applet firewall boundary via a context switch.

The Shareable interface serves to identify all shared objects. Any object that needs to be shared through the applet firewall shall directly or indirectly implement this interface. Only those methods specified in a shareable interface are available through the firewall.

Implementation classes can implement any number of shareable interfaces and can extend other shareable implementation classes.

Like any Java platform interface, a shareable interface simply defines a set of service methods. A service provider class declares that it "implements" the shareable interface and provides implementations for each of the service methods of the interface. A service client class accesses the services by obtaining an object reference, casting it to the shareable interface type, and invoking the service methods of the interface.

The shareable interfaces within the Java Card technology shall have the following properties:

- When a method in a shareable interface is invoked, a context switch occurs to the context of the object's owner.
- When the method exits, the context of the caller is restored.
- Exception handling is enhanced so that the currently active context is correctly restored during the stack frame unwinding that occurs as an exception is thrown.

6.2.7 Obtaining Shareable Interface Objects

Inter-applet communication is accomplished when a client applet invokes a shareable interface method of a SIO belonging to a server applet. In order for this to work, there must be a way for the client applet to obtain the SIO from the server applet in the first place. The JCRE provides a mechanism to make this possible. The `Applet` class and the `JCSystem` class provide methods to enable a client to request services from the server.

6.2.7.1 The Method `Applet.getShareableInterfaceObject(AID, byte)`

This method is implemented by the server applet instance. It shall be called by the JCRE to mediate between a client applet that requests to use an object belonging to another applet, and the server applet that makes its objects available for sharing.

The default behavior shall return `null`, which indicates that an applet does not participate in inter-applet communication.

A server applet that is intended to be invoked from another applet needs to override this method. This method should examine the `clientAID` and the `parameter`. If the `clientAID` is not one of the expected AIDs, the method should return `null`. Similarly, if the `parameter` is not recognized or if it is not allowed for the `clientAID`, then the method also should return `null`. Otherwise, the applet should return an SIO of the shareable interface type that the client has requested.

The server applet need not respond with the same SIO to all clients. The server can support multiple types of shared interfaces for different purposes and use `clientAID` and `parameter` to determine which kind of SIO to return to the client.

6.2.7.2 The Method `JCSystem.getAppletShareableInterfaceObject`

The `JCSystem` class contains the method `getAppletShareableInterfaceObject`, which is invoked by a client applet to communicate with a server applet.

The JCRE shall implement this method to behave as follows:

1. The JCRE searches its internal applet table which lists all successfully installed applets on the card for one with `serverAID`. If not found, `null` is returned.

2. The JCRE invokes this applet's `getShareableInterfaceObject` method, passing the `clientAID` of the caller and the `parameter`.

3. A context switch occurs to the server applet, and its implementation of `getShareableInterfaceObject` proceeds as described in the previous section. The server applet returns a SIO (or `null`).

4. `getAppletShareableInterfaceObject` returns the same SIO (or `null`) to its caller.

For enhanced security, the implementation shall make it impossible for the client to tell which of the following conditions caused a null value to be returned:

- The `serverAID` was not found.
- The server applet does not participate in inter-applet communication.
- The server applet does not recognize the `clientAID` or the `parameter`.
- The server applet won't communicate with this client.
- The server applet won't communicate with this client as specified by the `parameter`.

6.2.8 Class and Object Access Behavior

A static class field is *accessed* when one of the following Java bytecodes is executed:

```
getstatic, putstatic
```

An object is *accessed* when one of the following Java bytecodes is executed using the object's reference:

```
getfield, putfield, invokevirtual, invokeinterface, athrow,
<T>aload, <T>astore, arraylength, checkcast, instanceof
```

`<T>` refers to the various types of array bytecodes, such as `baload`, `sastore`, etc.

This list also includes any special or optimized forms of these bytecodes that may be implemented in the Java Card VM, such as `getfield_b`, `sgetfield_s_this`, etc.

Prior to performing the work of the bytecode as specified by the Java VM, the Java Card VM will perform an *access check* on the referenced object. If access is denied, then a `java.lang.SecurityException` is thrown.

The access checks performed by the Java Card VM depend on the type and owner of the referenced object, the bytecode, and the currently active context. They are described in the following sections.

6.2.8.1 Accessing Static Class Fields

Bytecodes:

```
getstatic, putstatic
```

- If the JCRE is the currently active context, then access is allowed.
- Otherwise, if the bytecode is `putstatic` and the field being stored is a reference type and the reference being stored is a reference to a temporary JCRE Entry Point Object or a global array, then access is denied.
- Otherwise, access is allowed.

6.2.8.2 Accessing Array Objects

Bytecodes:

```
<T>aload, <T>astore, arraylength, checkcast, instanceof
```

- If the JCRE is the currently active context, then access is allowed.
- Otherwise, if the bytecode is `aastore` and the component being stored is a reference type and the reference being stored is a reference to a temporary JCRE Entry Point Object or a global array, then access is denied.
- Otherwise, if the array is owned by an applet in the currently active context, then access is allowed.
- Otherwise, if the array is designated global, then access is allowed.
- Otherwise, access is denied.

6.2.8.3 Accessing Class Instance Object Fields

Bytecodes:

`getfield, putfield`

- If the JCRE is the currently active context, then access is allowed.
- Otherwise, if the bytecode is `putfield` and the field being stored is a reference type and the reference being stored is a reference to a temporary JCRE Entry Point Object or a global array, then access is denied.
- Otherwise if the object is owned by an applet in the currently active context, then access is allowed.
- Otherwise, access is denied.

6.2.8.4 Accessing Class Instance Object Methods

Bytecodes:

`invokevirtual`

- If the object is owned by an applet in the currently active context, then access is allowed. Context is switched to the object owner's context.
- Otherwise, if the object is designated a JCRE Entry Point Object, then access is allowed. Context is switched to the object owner's context (shall be JCRE).
- Otherwise, if JCRE is the currently active context, then access is allowed. Context is switched to the object owner's context.
- Otherwise, access is denied.

6.2.8.5 Accessing Standard Interface Methods

Bytecodes:

`invokeinterface`

- If the object is owned by an applet in the currently active context, then access is allowed.
- Otherwise, if the JCRE is the currently active context, then access is allowed. Context is switched to the object owner's context.
- Otherwise, access is denied.

6.2.8.6 Accessing Shareable Interface Methods

Bytecodes:

`invokeinterface`

- If the object is owned by an applet in the currently active context, then access is allowed.
- Otherwise, if the object's class implements a `Shareable` interface, and if the interface being invoked extends the `Shareable` interface, then access is allowed. Context is switched to the object owner's context.

- Otherwise, if the JCRE is the currently active context, then access is allowed. Context is switched to the object owner's context.
- Otherwise, access is denied.

6.2.8.7 Throwing Exception Objects

Bytecodes:

`athrow`

- If the object is owned by an applet in the currently active context, then access is allowed.
- Otherwise, if the object is designated a JCRE Entry Point Object, then access is allowed.
- Otherwise, if the JCRE is the currently active context, then access is allowed.
- Otherwise, access is denied.

6.2.8.8 Accessing Class Instance Objects

Bytecodes:

`checkcast, instanceof`

- If the object is owned by an applet in the currently active context, then access is allowed.
- Otherwise, if the object is designated a JCRE Entry Point Object, then access is allowed.
- Otherwise, if the JCRE is the currently active context, then access is allowed.
- Otherwise, access is denied.

6.2.8.9 Accessing Standard Interfaces

Bytecodes:

`checkcast, instanceof`

- If the object is owned by an applet in the currently active context, then access is allowed.
- Otherwise, if the JCRE is the currently active context, then access is allowed.
- Otherwise, access is denied.

6.2.8.10 Accessing Shareable Interfaces

Bytecodes:

`checkcast, instanceof`

- If the object is owned by an applet in the currently active context, then access is allowed.
- Otherwise, if the object's class implements a `Shareable` interface, and if the object is being cast into (checkcast) or is an instance of (instanceof) an interface that extends the `Shareable` interface, then access is allowed.
- Otherwise, if the JCRE is the currently active context, then access is allowed.

- Otherwise, access is denied.

6.3 Transient Objects and Contexts

Transient objects of `CLEAR_ON_RESET` type behave like persistent objects in that they can be accessed only when the currently active context is the same context as the owner of the object (the currently active context at the time when the object was created).

Transient objects of `CLEAR_ON_DESELECT` type can only be created or accessed when the currently active context is the context of the currently selected applet. If any of the `makeTransient` factory methods of `JCSystem` class are called to create a `CLEAR_ON_DESELECT` type transient object when the currently active context is not the context of the currently selected applet, the method shall throw a `java.lang.SystemException` with reason code of `ILLEGAL_TRANSIENT`. If an attempt is made to access a transient object of `CLEAR_ON_DESELECT` type when the currently active context is not the context of the currently selected applet, the JCRE shall throw a `java.lang.SecurityException`.

Applets that are part of the same package share the same group context. Every applet instance from a package shares all its object instances with all other instances from the same package. (This includes transient objects of both `CLEAR_ON_RESET` type and `CLEAR_ON_DESELECT` type owned by these applet instances.)

The transient objects of `CLEAR_ON_DESELECT` type owned by any applet instance within the same package shall be accessible when any of the applet instances in this package is the currently selected applet.

7. Transactions and Atomicity

A *transaction* is a logical set of updates of persistent data. For example, transferring some amount of money from one account to another is a banking transaction. It is important for transactions to be *atomic*: either all of the data fields are updated, or none are. The JCRE provides robust support for atomic transactions, so that card data is restored to its original pre-transaction state if the transaction does not complete normally. This mechanism protects against events such as power loss in the middle of a transaction, and against program errors that might cause data corruption should all steps of a transaction not complete normally.

7.1 Atomicity

Atomicity defines how the card handles the contents of persistent storage after a stop, failure, or fatal exception during an update of a single object or class field or array component. If power is lost during the update, the applet developer shall be able to rely on what the field or array component contains when power is restored.

The Java Card platform guarantees that any update to a single persistent object or class field will be atomic. In addition, the Java Card platform provides single component level atomicity for persistent arrays. That is, if the smart card loses power during the update of a data element (field in an object/class or component of an array) that shall be preserved across CAD sessions, that data element shall be restored to its previous value.

Some methods also guarantee atomicity for block updates of multiple data elements. For example, the atomicity of the `Util.arrayCopy` method guarantees that either all bytes are correctly copied or else the destination array is restored to its previous byte values.

An applet might not require atomicity for array updates. The `Util.arrayCopyNonAtomic` method is provided for this purpose. It does not use the transaction commit buffer even when called with a transaction in progress.

7.2 Transactions

An applet might need to atomically update several different fields or array components in several different objects. Either all updates take place correctly and consistently, or else all fields/components are restored to their previous values.

The Java Card platform supports a transactional model in which an applet can designate the beginning of an atomic set of updates with a call to the `JCSystem.beginTransaction` method. Each object update after this

point is conditionally updated. The field or array component appears to be updated—reading the field/array component back yields its latest conditional value—but the update is not yet committed.

When the applet calls `JCSystem.commitTransaction`, all conditional updates are committed to persistent storage. If power is lost or if some other system failure occurs prior to the completion of `JCSystem.commitTransaction`, all conditionally updated fields or array components are restored to their previous values. If the applet encounters an internal problem or decides to cancel the transaction, it can programmatically undo conditional updates by calling `JCSystem.abortTransaction`.

7.3 Transaction Duration

A transaction always ends when the JCRE regains programmatic control upon return from the applet's `select`, `deselect`, `process` or `install` methods.. This is true whether a transaction ends normally, with an applet's call to `commitTransaction`, or with an abortion of the transaction (either programmatically by the applet, or by default by the JCRE). For more details on transaction abortion, refer to section 7.6.

Transaction duration is the life of a transaction between the call to `JCSystem.beginTransaction`, and either a call to `commitTransaction` or an abortion of the transaction.

7.4 Nested Transactions

The model currently assumes that nested transactions are not possible. There can be only one transaction in progress at a time. If `JCSystem.beginTransaction` is called while a transaction is already in progress, then a `TransactionException` is thrown.

The `JCSystem.transactionDepth` method is provided to allow you to determine if a transaction is in progress.

7.5 Tear or Reset Transaction Failure

If power is lost (tear) or the card is reset or some other system failure occurs while a transaction is in progress, then the JCRE shall restore to their previous values all fields and array components conditionally updated since the previous call to `JCSystem.beginTransaction`.

This action is performed automatically by the JCRE when it reinitializes the card after recovering from the power loss, reset, or failure. The JCRE determines which of those objects (if any) were conditionally updated, and restores them.

Note – Object space used by instances created during the transaction that failed due to power loss or card reset can be recovered by the JCRE.

7.6 Aborting a Transaction

Transactions can be aborted either by an applet or by the JCRE.

7.6.1 Programmatic Abortion

If an applet encounters an internal problem or decides to cancel the transaction, it can programmatically undo conditional updates by calling `JCSystem.abortTransaction`. If this method is called, all conditionally updated fields and array components since the previous call to `JCSystem.beginTransaction` are restored to their previous values, and the `JCSystem.transactionDepth` value is reset to 0.

7.6.2 Abortion by the JCRE

If an applet returns from the `select`, `deselect`, `process`, or `install` methods with a transaction in progress, the JCRE automatically aborts the transaction. If a return from any of `select`, `deselect`, `process` or `install` methods occurs with a transaction in progress, the JCRE acts as if an exception was thrown.

7.6.3 Cleanup Responsibilities of the JCRE

Object instances created during the transaction that is being aborted can be deleted only if references to these deleted objects can no longer be used to access these objects. The JCRE shall ensure that a reference to an object created during the aborted transaction is equivalent to a `null` reference.

7.7 Transient Objects

Only updates to persistent objects participate in the transaction. Updates to transient objects are never undone, regardless of whether or not they were “inside a transaction.”

7.8 Commit Capacity

Since platform resources are limited, the number of bytes of conditionally updated data that can be accumulated during a transaction is limited. The Java Card technology provides methods to determine how much *commit capacity* is available on the implementation. The commit capacity represents an upper bound on the number of conditional byte updates available. The actual number of conditional byte updates available may be lower due to management overhead.

A `TransactionException` is thrown if the commit capacity is exceeded during a transaction.

7.9 Context Switching

Context switches shall not alter the state of a transaction in progress. If a transaction is in progress at the time of a context switch (see section 6.1.1), updates to persistent data continue to be conditional in the new context until the transaction is committed or aborted.

8. API Topics

The topics in this chapter complement the requirements specified in the *Java Card 2.1 API Specification*.

8.1 Resource Use within the API

Unless specified in the *Java Card 2.1 API Specification*, the implementation shall support the invocation of API instance methods, even when the owner of the object instance is not the currently selected applet. In other words, unless specifically called out, the implementation shall not use resources such as transient objects of CLEAR_ON_DESELECT type.

8.2 Exceptions thrown by API classes

All exception objects thrown by the API implementation shall be temporary JCRE Entry Point Objects. Temporary JCRE Entry Point Objects cannot be stored in class variables, instance variables or array components (See section 6.2.1).

8.3 Transactions within the API

Unless explicitly called out in the API descriptions, implementation of the Java Card 2.1 API methods shall not initiate or otherwise alter the state of a transaction in progress. Even if a transaction is in progress, updates to implementation persistent state within the API need not be conditional unless specifically called out by the API method.

8.4 The APDU Class

The APDU class encapsulates access to the ISO 7816-4 based I/O across the card serial line. The APDU Class is designed to be independent of the underlying I/O transport protocol.

The JCRE may support T=0 or T=1 transport protocols or both.

8.4.1 T=0 specifics for outgoing data transfers

For compatibility with legacy CAD/terminals that do not support block chained mechanisms, the APDU Class allows mode selection via the `setOutgoingNoChaining` method.

8.4.1.1 Constrained transfers with no chaining

When the no chaining mode of output transfer is requested by the applet by calling the `setOutgoingNoChaining` method, the following protocol sequence shall be followed:

Note – when the no chaining mode is used (i.e. after the invocation of the `setOutgoingNoChaining` method), calls to the `waitExtension` method shall throw an `APDUException` with reason code `ILLEGAL_USE`.

Notation

Le = CAD expected length.

Lr = Applet response length set via `setOutgoingLength` method.

<INS> = the protocol byte equal to the incoming header INS byte, which indicates that all data bytes will be transferred next.

<~INS> = the protocol byte that is the complement of the incoming header INS byte, which indicates that 1 data byte will be transferred next.

<SW1,SW2> = the response status bytes as in ISO7816-4.

ISO 7816-4 CASE 2

Le == Lr

1. The card sends Lr bytes of output data using the standard T=0 <INS> or <~INS> procedure byte mechanism.

2. The card sends <SW1,SW2> completion status on completion of the `Applet.process` method.

Lr < Le

1. The card sends <0x61,Lr> completion status bytes

2. The CAD sends GET RESPONSE command with Le = Lr.

3. The card sends Lr bytes of output data using the standard T=0 <INS> or <~INS> procedure byte mechanism.

4. The card sends <SW1,SW2> completion status on completion of the `Applet.process` method.

Lr > Le

1. The card sends Le bytes of output data using the standard T=0 <INS> or <~INS> procedure byte mechanism.

2. The card sends <0x61,(Lr-Le)> completion status bytes

3. The CAD sends GET RESPONSE command with new Le <= Lr.

4. The card sends (new) Le bytes of output data using the standard T=0 <INS> or <~INS> procedure byte mechanism.

5. Repeat steps 2-4 as necessary to send the remaining output data bytes (Lr) as required.

6. The card sends <SW1,SW2> completion status on completion of the `Applet.process` method.

ISO 7816-4 CASE 4

In Case 4, Le is determined after the following initial exchange:

1. The card sends <0x61,Lr status bytes>

2. The CAD sends GET RESPONSE command with Le <= Lr.

The rest of the protocol sequence is identical to CASE 2 described above.

If the applet aborts early and sends less than Le bytes, zeros shall be sent instead to fill out the length of the transfer expected by the CAD.

8.4.1.2 Regular Output transfers

When the no chaining mode of output transfer is not requested by the applet (that is, the `setOutgoing` method is used), any ISO-7816-3/4 compliant T=0 protocol transfer sequence may be used.

Note – The `waitExtension` method may be invoked by the applet at any time. The `waitExtension` method shall request an additional work waiting time (ISO 7816-3) using the 0x60 procedure byte.

8.4.1.3 Additional T=0 requirements

At any time, when the T=0 output transfer protocol is in use, and the APDU class is awaiting a GET RESPONSE command from the CAD in reaction to a response status of <0x61, xx> from the card, if the CAD sends in a different command, the `sendBytes` or the `sendBytesLong` methods shall throw an `APDUException` with reason code `NO_T0_GETRESPONSE`.

Calls to `sendBytes` or `sendBytesLong` methods from this point on shall result in an `APDUException` with reason code `ILLEGAL_USE`. If an `ISOException` is thrown by the applet after the `NO_T0_GETRESPONSE` exception has been thrown, the JCRE shall discard the response status in its reason code. The JCRE shall restart APDU processing with the newly received command and resume APDU dispatching.

8.4.2 T=1 specifics for outgoing data transfers

8.4.2.1 Constrained transfers with no chaining

When the no chaining mode of output transfer is requested by the applet by calling the `setOutgoingNoChaining` method, the following protocol specifics shall be followed:

Notation

Le = CAD expected length.

Lr = Applet response length set via `setOutgoingLength` method.

The transport protocol sequence shall not use block chaining. Specifically, the M-bit (more data bit) shall not be set in the PCB of the I-blocks during the transfers (ISO 7816-3). In other words, the entire outgoing data (Lr bytes) shall be transferred in one I-block.

If the applet aborts early and sends less than Lr bytes, zeros shall be sent instead to fill out the remaining length of the block.

Note – When the no chaining mode is used (i.e. after the invocation of the `setOutgoingNoChaining` method), calls to the `waitExtension` method shall throw an `APDUException` with reason code `ILLEGAL_USE`.

8.4.2.2 Regular Output transfers

When the no chaining mode of output transfer is not requested by the applet (i.e. the `setOutgoing` method is used) any ISO-7816-3/4 compliant T=1 protocol transfer sequence may be used.

Note – The `waitExtension` method may be invoked by the applet at anytime. The `waitExtension` method shall send an S-block command with WTX request of INF units, which is equivalent to a request of 1 additional work waiting time in T=0 mode. (See ISO 7816-3).

8.4.2.2.1 Chain abortion by the CAD

If the CAD aborts a chained outbound transfer using an S-block ABORT request (see ISO 7816-3), the `sendBytes` or `sendBytesLong` method shall throw an APDUException with reason code T1_IFD_ABORT.

Calls to `sendBytes` or `sendBytesLong` methods from this point on shall result in an `APDUException` with reason code `ILLEGAL_USE`. If an `ISOException` is thrown by the applet after the `T1_IFD_ABORT` exception has been thrown, the JCRE shall discard the response status in its reason code. The JCRE shall restart APDU processing with the newly received command, and resume APDU dispatching.

8.4.3 T=1 specifics for incoming data transfers

8.4.3.1 Incoming transfers using chaining

8.4.3.1.1 Chain abortion by the CAD

If the CAD aborts a chained inbound transfer using an S-block ABORT request (see ISO 7816-3), the `setIncomingAndReceive` or `receiveBytes` method shall throw an APDUException with reason code `T1_IFD_ABORT`.

Calls to `receiveBytes` , `sendBytes` or `sendBytesLong` methods from this point on shall result in an `APDUException` with reason code `ILLEGAL_USE`. If an `ISOException` is thrown by the applet after the `T1_IFD_ABORT` exception has been thrown, the JCRE shall discard the response status in its reason code. The JCRE shall restart APDU processing with the newly received command, and resume APDU dispatching.

8.5 The Security and Crypto packages

The `getInstance` method in the following classes return an implementation instance in the context of the calling applet of the requested algorithm:

`javacard.security.MessageDigest`

`javacard.security.Signature`

`javacard.security.RandomData`

`javacardx.crypto.Cipher`

An implementation of the JCRE may implement 0 or more of the algorithms listed in the *Java Card 2.1 API Specification*. When an algorithm that is not implemented is requested this method shall throw a `CryptoException` with reason code `NO_SUCH_ALGORITHM`.

Implementations of the above classes shall extend the corresponding base class and implement all the abstract methods. All data allocation associated with the implementation instance shall be performed at the time of instance construction to ensure that any lack of required resources can be flagged early during the installation of the applet.

Similarly, the `buildKey` method of the `javacard.security.keyBuilder` class returns an implementation instance of the requested Key type. The JCRE may implement 0 or more types of keys. When a key type that is not implemented is requested, the method shall throw a `CryptoException` with reason code `NO_SUCH_ALGORITHM`.

Implementations of key types shall implement the associated interface. All data allocation associated with the key implementation instance shall be performed at the time of instance construction to ensure that any lack of required resources can be flagged early during the installation of the applet.

8.6 JCSystem Class

In Java Card 2.1, the `getVersion` method shall return (short) 0x0201.

9. Virtual Machine Topics

The topics in this chapter detail virtual machine specifics.

9.1 Resource Failures

A lack of resources condition (such as heap space) which is recoverable shall result in a `SystemException` with reason code `NO_RESOURCE`. The factory methods in `JCSystem` used to create transient arrays throw a `SystemException` with reason code `NO_TRANSIENT_SPACE` to indicate lack of transient space.

All other (non-recoverable) virtual machine errors such as stack overflow shall result in a virtual machine error. These conditions shall cause the virtual machine to halt. When such a non-recoverable virtual machine error occurs, an implementation can optionally require the card to be muted or blocked from further use.

Appendix JCRE01

10. Applet Installer

Applet installation on smart cards using Java Card technology is a complex topic. The design of the *Java Card 2.1 API Specification* is intended to give JCRE implementers as much freedom as possible in their implementations. However, some basic common specifications are required in order to allow Java Card applets to be installed without knowing the implementation details of a particular installer.

This specification defines the concept of an Installer and specifies minimal installation requirements in order to achieve interoperability across a wide range of possible Installer implementations.

The Applet Installer is an optional part of the Java Card 2.1 Environment (JCRE) Specification. That is, an implementation of the JCRE does not necessarily need to include a post-issuance Installer. However, if implemented, the installer is required to support the behavior specified in this chapter.

10.1 The Installer

The mechanisms necessary to install an applet on smart cards using Java Card technology are embodied in an on-card component called the *Installer*.

To the CAD the Installer appears to be an applet. It has an AID, and it becomes the currently selected applet when this AID is successfully processed by a SELECT command. Once selected, the Installer behaves in much the same way as any other applet:

- It receives all APDUs just like any other selected applet.
- Its design specification prescribes the various kinds and formats of APDUs that it expects to receive along with the semantics of those commands under various preconditions.
- It processes and responds to all APDUs that it receives. Incorrect APDUs are responded to with an error condition of some kind.
- When another applet is selected (or when the card is reset or when power is removed from the card), the Installer becomes deselected and remains suspended until the next time that it is SELECTed.

10.1.1 Installer Implementation

The Installer need not be implemented as an applet on the card. The requirement is only that the Installer functionality be SELECTable. The corollary to this requirement is that Installer component shall not be able to be invoked when a non-Installer applet is selected nor when no applet is selected.

Obviously, a JCRE implementer could choose to implement the Installer as an applet. If so, then the Installer might be coded to extend the `Applet` class and respond to invocations of the `select`, `process`, and `deselect` methods.

But a JCRE implementer could also implement the Installer in other ways, as long as it provides the SELECTable behavior to the outside world. In this case, the JCRE implementer has the freedom to provide some other mechanism by which APDUs are delivered to the Installer code module.

10.1.2 Installer AID

Because the Installer is SELECTable, it shall have an AID. JCRE implementers are free to choose their own AID by which their Installer is selected. Multiple installers may be implemented.

10.1.3 Installer APDUs

The Java Card 2.1 API does not specify any APDUs for the Installer. JCRE implementers are entirely free to choose their own APDU commands to direct their Installer in its work.

The model is that the Installer on the card is initiated by an installation program running on the CAD. In order for installation to succeed, this CAD installation program shall be able to:

- Recognize the card.
- SELECT the Installer on the card.
- Coordinate the installation process by sending the appropriate APDUs to the card Installer. These APDUs will include:
  - Authentication information, to ensure that the installation is authorized.
  - The applet code to be loaded into the card's memory.
  - Linkage information to link the applet code with code already on the card.
  - Instance initialization parameter data to be sent to the applet's `install` method.

The *Java Card 2.1 API Specification* does not specify the details of the CAD installation program nor the APDUs passed between it and the Installer.

10.1.4 Installer Behavior

JCRE implementers shall also define other behaviors of their Installer, including:

- Whether or not installation can be aborted and how this is done.
- What happens if an exception, reset, or power fail occurs during installation.
- What happens if another applet is selected before the Installer is finished with its work.

The JCRE shall guarantee that an applet will *not* be deemed successfully installed if:

- the applet package must link with another package already resident on the card , but the version of the resident package is not binary compatible with the applet package. For more information on binary compatibility in the Java programming language please see *The Java Language Specification.* Binary compatibility in Java Card technology is discussed in the *Java Card 2.1 Virtual Machine Specification.*

- the applet's `install` method throws an exception before successful return from the `Applet.register` method (see section 3.1).

10.1.5 Installer Privileges

Although an Installer may be implemented as an applet, an Installer will typically require access to features that are not available to "other" applets. For example, depending on the JCRE implementer's implementation, the Installer will need to:

- Read and write directly to memory, bypassing the object system and/or standard security.
- Access objects owned by other applets or by the JCRE.
- Invoke non-entry point methods of the JCRE.
- Be able to invoke the `install` method of a newly installed applet.

Again, it is up to each JCRE implementer to determine the Installer implementation and supply such features in their JCRE implementations as necessary to support their Installer. JCRE implementers are also responsible for the security of such features, so that they are not available to normal applets.

10.2 The Newly Installed Applet

There is a single interface between the Installer and the applet that is being installed. After the Installer has correctly prepared the applet for execution (performed steps such as loading and linking), the Installer shall invoke the applet's `install` method. This method is defined in the `Applet` class.

The precise mechanism by which an applet's `install(byte[], short, byte)` method is invoked from the Installer is a JCRE implementer-defined implementation detail. However, there shall be a context switch so that any context-related operations performed by the `install` method (such as creating new objects) are done in the context of the new applet and not in the context of the Installer. The Installer shall also ensure that array objects created during applet class initialization (<clinit>) methods are also owned by the context of the new applet.

The installation of an applet is deemed complete if all steps are completed without failure or an exception being thrown, up to and including successful return from executing the `Applet.register` method. At that point, the installed applet will be selectable.

The maximum size of the parameter data is 32 bytes. And for security reasons, the `bArray` parameter is zeroed after the return (just as the APDU buffer is zeroed on return from an applet's `process` method.)

10.2.1 Installation Parameters

Other than the maximum size of 32 bytes, the Java Card 2.1 API does not specify anything about the contents of the global byte array installation parameter. This is fully defined by the applet designer and can be in any format desired. In addition, these installation parameters are intended to be opaque to the Installer.

JCRE implementers should design their Installers so that it is possible for an installation program running in a CAD to specify an arbitrary byte array to be delivered to the Installer. The Installer simply forwards this byte array to the target applet's `install` method in the `bArray` parameter. A typical implementation might define a JCRE implementer-proprietary APDU command that has the semantics "call the applet's `install` method passing the contents of the accompanying byte array."

Appendix JCRE01

11. API Constants

Some of the API classes don't have values specified for their constants in the *Java Card 2.1 API Specification*. If constant values are not specified consistently by implementers of this Java Card 2.1 Environment (JCRE) Specification, industry-wide interoperability is impossible. This chapter provides the required values for constants that are not specified in the *Java Card 2.1 API Specification*.

Class javacard.framework.APDU

```
public static final byte PROTOCOL_T0 = 0;
public static final byte PROTOCOL_T1 = 1;
```

Class javacard.framework.APDUException

```
public static final short ILLEGAL_USE = 1;
public static final short BUFFER_BOUNDS = 2;
public static final short BAD_LENGTH = 3;
public static final short IO_ERROR = 4;
public static final short NO_T0_GETRESPONSE = 0xAA;
public static final short T1_IFD_ABORT = 0xAB;
```

Interface javacard.framework.ISO7816

```
public final static short SW_NO_ERROR = (short)0x9000;
public final static short SW_BYTES_REMAINING_00 = 0x6100;
public final static short SW_WRONG_LENGTH = 0x6700;
public static final short SW_SECURITY_STATUS_NOT_SATISFIED = 0x6982;
public final static short SW_FILE_INVALID = 0x6983;
public final static short SW_DATA_INVALID = 0x6984;
public final static short SW_CONDITIONS_NOT_SATISFIED = 0x6985;
public final static short SW_COMMAND_NOT_ALLOWED = 0x6986;
public final static short SW_APPLET_SELECT_FAILED = 0x6999;
public final static short SW_WRONG_DATA = 0x6A80;
public final static short SW_FUNC_NOT_SUPPORTED = 0x6A81;
public final static short SW_FILE_NOT_FOUND = 0x6A82;
public final static short SW_RECORD_NOT_FOUND = 0x6A83;
public final static short SW_INCORRECT_P1P2  = 0x6A86;
public final static short SW_WRONG_P1P2  = 0x6B00;
public final static short SW_CORRECT_LENGTH_00 = 0x6C00;
public final static short SW_INS_NOT_SUPPORTED = 0x6D00;
public final static short SW_CLA_NOT_SUPPORTED = 0x6E00;
public final static short SW_UNKNOWN = 0x6F00;
public static final short SW_FILE_FULL = 0x6A84;
public final static byte OFFSET_CLA = 0;
public final static byte OFFSET_INS = 1;
public final static byte OFFSET_P1 = 2;
```

```
public final static byte OFFSET_P2 = 3;
public final static byte OFFSET_LC = 4;
public final static byte OFFSET_CDATA= 5;
public final static byte CLA_ISO7816 = 0x00;
public final static byte INS_SELECT = (byte) 0xA4;
public final static byte INS_EXTERNAL_AUTHENTICATE = (byte) 0x82;
```

Class javacard.framework.JCSystem

```
public static final byte NOT_A_TRANSIENT_OBJECT = 0;
public static final byte CLEAR_ON_RESET = 1;
public static final byte CLEAR_ON_DESELECT = 2;
```

Class javacard.framework.PINException

```
public static final short ILLEGAL_VALUE = 1;
```

Class javacard.framework.SystemException

```
public static final short ILLEGAL_VALUE = 1;
public static final short NO_TRANSIENT_SPACE = 2;
public static final short ILLEGAL_TRANSIENT = 3;
public static final short ILLEGAL_AID = 4;
public static final short NO_RESOURCE = 5;
```

Class javacard.framework.TransactionException

```
public static final short IN_PROGRESS  = 1;
public static final short NOT_IN_PROGRESS  = 2;
public static final short BUFFER_FULL  = 3;
public static final short INTERNAL_FAILURE  = 4;
```

Class javacard.security.CryptoException

```
public static final short ILLEGAL_VALUE = 1;
public static final short UNINITIALIZED_KEY = 2;
public static final short NO_SUCH_ALGORITHM = 3;
public static final short INVALID_INIT = 4;
public static final short ILLEGAL_USE = 5;
```

Class javacard.security.KeyBuilder

```
public static final byte TYPE_DES_TRANSIENT_RESET = 1;
public static final byte TYPE_DES_TRANSIENT_DESELECT = 2;
public static final byte TYPE_DES = 3;
public static final byte TYPE_RSA_PUBLIC = 4;
public static final byte TYPE_RSA_PRIVATE = 5;
public static final byte TYPE_RSA_CRT_PRIVATE = 6;
public static final byte TYPE_DSA_PUBLIC = 7;
public static final byte TYPE_DSA_PRIVATE = 8;
public static final short LENGTH_DES = 64;
public static final short LENGTH_DES3_2KEY = 128;
public static final short LENGTH_DES3_3KEY = 192;
public static final short LENGTH_RSA_512 = 512;
public static final short LENGTH_RSA_768 = 768;
public static final short LENGTH_RSA_1024 = 1024;
public static final short LENGTH_RSA_2048 = 2048;
public static final short LENGTH_DSA_512 = 512;
public static final short LENGTH_DSA_768 = 768;
public static final short LENGTH_DSA_1024 = 1024;
```

Class javacard.security.MessageDigest

```
public static final byte ALG_SHA = 1;
public static final byte ALG_MD5 = 2;
public static final byte ALG_RIPEMD160 = 3;
```

Class javacard.security.RandomData

```
public static final byte ALG_PSEUDO_RANDOM = 1;
public static final byte ALG_SECURE_RANDOM = 2;
```

Class javacard.security.Signature

```
public static final byte ALG_DES_MAC4_NOPAD = 1;
public static final byte ALG_DES_MAC8_NOPAD = 2;
public static final byte ALG_DES_MAC4_ISO9797_M1 = 3;
public static final byte ALG_DES_MAC8_ISO9797_M1 = 4;
public static final byte ALG_DES_MAC4_ISO9797_M2 = 5;
public static final byte ALG_DES_MAC8_ISO9797_M2 = 6;
public static final byte ALG_DES_MAC4_PKCS5 = 7;
public static final byte ALG_DES_MAC8_PKCS5 = 8;
public static final byte ALG_RSA_SHA_ISO9796 = 9;
public static final byte ALG_RSA_SHA_PKCS1 = 10;
public static final byte ALG_RSA_MD5_PKCS1 = 11;
public static final byte ALG_RSA_RIPEMD160_ISO9796 = 12;
public static final byte ALG_RSA_RIPEMD160_PKCS1 = 13;
public static final byte ALG_DSA_SHA = 14;
public static final byte ALG_RSA_SHA_RFC2409  = 15;
public static final byte ALG_RSA_MD5_RFC2409  = 16;
public static final byte MODE_SIGN = 1;
public static final byte MODE_VERIFY = 2;
```

Class javacardx.crypto.Cipher

```
public static final byte ALG_DES_CBC_NOPAD = 1;
public static final byte ALG_DES_CBC_ISO9797_M1 = 2;
public static final byte ALG_DES_CBC_ISO9797_M2 = 3;
public static final byte ALG_DES_CBC_PKCS5 = 4;
public static final byte ALG_DES_ECB_NOPAD = 5;
public static final byte ALG_DES_ECB_ISO9797_M1 = 6;
public static final byte ALG_DES_ECB_ISO9797_M2 = 7;
public static final byte ALG_DES_ECB_PKCS5 = 8;
public static final byte ALG_RSA_ISO14888 = 9;
public static final byte ALG_RSA_PKCS1 = 10;
public static final byte ALG_RSA_ISO9796 = 11;
public static final byte MODE_DECRYPT = 1;
public static final byte MODE_ENCRYPT = 2;
```

Appendix JCRE01

Glossary

AID is an acronym for Application IDentifier as defined in ISO 7816-5.

APDU is an acronym for Application Protocol Data Unit as defined in ISO 7816-4.

API is an acronym for Application Programming Interface. The API defines calling conventions by which an application program accesses the operating system and other services.

Applet within the context of this document means a Java Card Applet, which is the basic unit of selection, context, functionality, and security in Java Card technology.

Applet developer refers to a person creating a Java Card applet using the Java Card technology specifications.

Applet firewall is the mechanism in the Java Card technology by which the VM prevents an applet in one context from making unauthorized accesses to objects owned by an applet in another context or the JCRE context, and reports or otherwise addresses the violation.

Atomic operation is an operation that either completes in its entirety (if the operation succeeds) or no part of the operation completes at all (if the operation fails).

Atomicity refers to whether a particular operation is atomic or not and is necessary for proper data recovery in cases in which power is lost or the card is unexpectedly removed from the CAD.

ATR is an acronym for Answer to Reset. An ATR is a string of bytes sent by the Java Card after a reset condition.

CAD is an acronym for Card Acceptance Device. The CAD is the device in which the card is inserted.

Cast is the explicit conversion from one data type to another.

cJCK is the test suite to verify the compliance of the implementation of the Java Card Technology specifications. The cJCK uses the JavaTest tool to run the test suite.

Class is the prototype for an object in an object-oriented language. A class may also be considered a set of objects that share a common structure and behavior. The structure of a class is determined by the class variables that represent the state of an object of that class and the behavior is given by a set of methods associated with the class.

Classes are related in a class hierarchy. One class may be a specialization (a subclass) of another (its superclass), it may have reference to other classes, and it may use other classes in a client-server relationship.

Context (See Applet execution context.)

Currently active context. The JCRE keeps track of the currently active Java Card context. When a virtual method is invoked on an object, and a context switch is required and permitted, the currently active context is

changed to correspond to the context of the applet that owns the object. When that method returns, the previous context is restored. Invocations of static methods have no effect on the currently active context. The currently active context and sharing status of an object together determine if access to an object is permissible.

Currently selected applet. The JCRE keeps track of the currently selected Java Card applet. Upon receiving a SELECT command with this applet's AID, the JCRE makes this applet the currently selected applet. The JCRE sends all APDU commands to the currently selected applet.

EEPROM is an acronym for Electrically Erasable, Programmable Read Only Memory.

Firewall (see Applet Firewall).

Framework is the set of classes that implement the API. This includes core and extension packages. Responsibilities include dispatching of APDUs, applet selection, managing atomicity, and installing applets.

Garbage collection is the process by which dynamically allocated storage is automatically reclaimed during the execution of a program.

Instance variables, also known as fields, represent a portion of an object's internal state. Each object has its own set of instance variables. Objects of the same class will have the same instance variables, but each object can have different values.

Instantiation, in object-oriented programming, means to produce a particular object from its class template. This involves allocation of a data structure with the types specified by the template, and initialization of instance variables with either default values or those provided by the class's constructor function.

JAR is an acronym for Java Archive. JAR is a platform-independent file format that combines many files into one.

Java Card Runtime Environment (JCRE) consists of the Java Card Virtual Machine, the framework, and the associated native methods.

JC21RI is an acronym for the Java Card 2.1 Reference Implementation.

JCRE implementer refers to a person creating a vendor-specific implementation using the Java Card API.

JCVM is an acronym for the Java Card Virtual Machine. The JCVM is the foundation of the OP card architecture. The JCVM executes byte code and manages classes and objects. It enforces separation between applications (firewalls) and enables secure data sharing.

JDK is an acronym for Java Development Kit. The JDK is a Sun Microsystems, Inc. product that provides the environment required for programming in Java. The JDK is available for a variety of platforms, but most notably Sun Solaris and Microsoft Windows®.

Method is the name given to a procedure or routine, associated with one or more classes, in object-oriented languages.

Namespace is a set of names in which all names are unique.

Object-Oriented is a programming methodology based on the concept of an *object*, which is a data structure encapsulated with a set of routines, called *methods*, which operate on the data.

Objects, in object-oriented programming, are unique instances of a data structure defined according to the template provided by its class. Each object has its own values for the variables belonging to its class and can respond to the messages (methods) defined by its class.

Package is a namespace within the Java programming language and can have classes and interfaces. A package is the smallest unit within the Java programming language.

Persistent object Persistent objects and their values persist from one CAD session to the next, indefinitely. Objects are persistent by default. Persistent object values are updated atomically using transactions. The term persistent does not mean there is an object-oriented database on the card or that objects are serialized/deserialized, just that the objects are not lost when the card loses power.

Shareable interface Defines a set of shared interface methods. These interface methods can be invoked from an applet in one context when the object implementing them is owned by an applet in another context.

Shareable interface object (SIO) An object that implements the shareable interface.

Transaction is an atomic operation in which the developer defines the extent of the operation by indicating in the program code the beginning and end of the transaction.

Transient object. The values of transient objects do not persist from one CAD session to the next, and are reset to a default state at specified intervals. Updates to the values of transient objects are not atomic and are not affected by transactions.

Java Card™ 2.1 Virtual Machine Specification

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303 USA
415 960-1300 fax 415 969-9131

Final Revision 1.0, March 3, 1999

Contents

Figures

Appendix JCVM01

Tables

Preface

Java Card™ technology combines a subset of the Java programming language with a runtime environment optimized for smart cards and similar small-memory embedded devices. The goal of Java Card technology is to bring many of the benefits of Java software programming to the resource-constrained world of devices such as smart cards.

The Java Card platform is defined by three specifications: this *Java Card™ 2.1 Virtual Machine Specification*, the *Java Card™ 2.1 Application Programming Interface*, and the *Java Card™ 2.1 Runtime Environment (JCRE) Specification*.

This specification describes the required behavior of the Java Card 2.1 Virtual Machine (VM) that developers should adhere to when creating an *implementation*. An implementation within the context of this document refers to a licensee's implementation of the Java Card Virtual Machine (VM), Application Programming Interface (API), Converter, or other component, based on the Java Card technology specifications. A Reference Implementation is an implementation produced by Sun Microsystems, Inc. Application software written for the Java Card platform is referred to as a Java Card applet.

Who Should Use This Specification?

This document is for licensees of the Java Card technology to assist them in creating an implementation, developing a specification to extend the Java Card technology specifications, or in creating an extension to the Java Card Runtime Environment (JCRE). This document is also intended for Java Card applet developers who want a more detailed understanding of the Java Card technology specifications.

Before You Read This Specification

Before reading this document, you should be familiar with the Java programming language, the Java Card technology specifications, and smart card technology. A good resource for becoming familiar with Java technology and Java Card technology is the Sun Microsystems, Inc. website, located at: `http://java.sun.com`.

How This Book Is Organized

Chapter 1, "Introduction," provides an overview of the Java Card Virtual Machine architecture.

Chapter 2, "A Subset of the Java Virtual Machine," describes the subset of the Java programming language and Virtual Machine that is supported by the Java Card specification.

Chapter 3, "Structure of the Java Card Virtual Machine," describes the differences between the Java Virtual Machine and the Java Card Virtual Machine.

Chapter 4, "Binary Representation," provides information about how Java Card programs are represented in binary form.

Chapter 5, "The Export File," describes the Converter `export` file used to link code against another package.

Chapter 6, "The CAP File Format," describes the format of the `CAP` file.

Chapter 7, "Instruction Set," describes the byte codes (opcodes) that comprise the Java Card Virtual Machine instruction set.

Chapter 8, "Tables of Instructions," summarizes the Java Card Virtual Machine instructions in two different tables: one sorted by Opcode Value and the other sorted by Mnemonic.

Glossary is a list of words and their definitions to assist you in using this book.

Prerequisites

This specification is not intended to stand on its own; rather it relies heavily on existing documentation of the Java platform. In particular, two books are required for the reader to understand the material presented here.

[1] Gosling, James, Bill Joy, and Guy Steele. *The Java™ Language Specification*. Addison-Wesley, 1996, ISBN 0-201-63451-1 – contains the definitive definition of the Java programming language. The Java Card 2.1 language subset defined here is based on the language specified in this book.

[2] Lindholm, Tim, and Frank Yellin. *The Java™ Virtual Machine Specification*. Addison-Wesley, 1996, ISBN 0-201-63452-X – defines the standard operation of the Java Virtual Machine. The Java Card virtual machine presented here is based on the definition specified in this book.

Related Documents

References to various documents or products are made in this manual. You should have the following documents available:

- *Java Card™ 2.1 Application Programming Interface*, Sun Microsystems, Inc.
- *Java Card™ 2.1 Runtime Environment (JCRE) 2.1 Specification*, Sun Microsystems, Inc.
- *Java Card™ 2.1 Applet Developer's Guide*, Sun Microsystems, Inc.
- *The Java™ Language Specification* by James Gosling, Bill Joy, and Guy L. Steele. Addison-Wesley, 1996, ISBN 0-201-63451-1.
- *The Java™ Virtual Machine Specification* (Java Series) by Tim Lindholm and Frank Yellin. Addison-Wesley, 1996, ISBN 0-201-63452-X.
- *The Java™ Class Libraries: An Annotated Reference (Java Series)* by Patrick Chan and Rosanna Lee. Addison-Wesley, ISBN: 0201634589.
- *ISO 7816 International Standard*, First Edition 1987-07-01.
- *EMV '96 Integrated Circuit Card Specification for Payment Systems*, Version 3.0, June 30, 1996.

Ordering Sun Documents

The SunDocs™ program provides more than 250 manuals from Sun Microsystems, Inc. If you live in the United States, Canada, Europe, or Japan, you can purchase documentation sets or individual manuals using this program.

For a list of documents and how to order them, see the catalog section of the SunExpress™ Internet site at `http://www.sun.com/sunexpress`.

What Typographic Changes Mean

The following table describes the typographic changes used in this book.

TABLE P-1 Typographic Conventions

Typeface or Symbol	Meaning	Example
`AaBbCc123`	Java code, Java keywords or variables, or class files.	The `token` item of a `CONSTANT_StaticFieldref_info` structure ...
bytecode	Java language bytecodes	*invokespecial*
AaBbCc123	Command-line placeholder: replace with a real name or value	To delete a file, type `rm` *filename.*
AaBbCc123	Book titles, new words or terms, or words to be emphasized	Read Chapter 6 in *User's Guide*. These are called *class* options. You *must* be root to do this.

Acknowledgements

Java Card technology is based on Java technology. This specification could not exist without all the hard work that went into the development of the Java platform specifications. In particular, this specification is based significantly on the *Java™ Virtual Machine Specification*. In order to maintain consistency with that specification, as well as to make differences easier to notice, we have, where possible, used the words, the style, and even the visual design of that book. Many thanks to Tim Lindholm and Frank Yellin for providing a solid foundation for our work.

CHAPTER 1

Introduction

1.1 Motivation

Java Card technology enables programs written in the Java programming language to be run on smart cards and other small, resource-constrained devices. Developers can build and test programs using standard software development tools and environments, then convert them into a form that can be installed onto a Java Card technology enabled device. Application software for the Java Card platform is called an applet, or more specifically, a Java Card applet or card applet (to distinguish it from browser applets).

While Java Card technology enables programs written in the Java programming language to run on smart cards, such small devices are far too under-powered to support the full functionality of the Java platform. Therefore, the Java Card platform supports only a carefully chosen, customized subset of the features of the Java platform. This subset provides features that are well-suited for writing programs for small devices and preserves the object-oriented capabilities of the Java programming language.

A simple approach to specifying a Java Card virtual machine would be to describe the subset of the features of the Java virtual machine that must be supported to allow for portability of source code across all Java Card technology enabled devices. Combining that subset specification and the information in the *Java Virtual Machine Specification*, smart card manufacturers could construct their own Java Card implementations. While that approach is feasible, it has a serious drawback. The resultant platform would be missing the important feature of binary portability of Java Card applets.

The standards that define the Java platform allow for binary portability of Java programs across all Java platform implementations. This “write once, run anywhere” quality of Java programs is perhaps the most significant feature of the platform. Part

of the motivation for the creation of the Java Card platform was to bring just this kind of binary portability to the smart card industry. In a world with hundreds of millions or perhaps even billions of smart cards with varying processors and configurations, the costs of supporting multiple binary formats for software distribution could be overwhelming.

This *Java Card 2.1 Virtual Machine Specification* is the key to providing binary portability. One way of understanding what this specification does is to compare it to its counterpart in the Java platform. The *Java Virtual Machine Specification* defines a Java virtual machine as an engine that loads Java `class` files and executes them with a particular set of semantics. The `class` file is a central piece of the Java architecture, and it is the standard for the binary compatibility of the Java platform. The *Java Card 2.1 Virtual Machine Specification* also defines a file format that is the standard for binary compatibility for the Java Card platform: the `CAP` file format is the form in which software is loaded onto devices which implement a Java Card virtual machine.

1.2 The Java Card Virtual Machine

The role of the Java Card virtual machine is best understood in the context of the process for production and deployment of Java Card software. There are several components that make up a Java Card system, including the Java Card virtual machine, the Java Card Converter, a terminal installation tool, and an installation program that runs on the device, as shown in Figures 1-1 and 1-2.

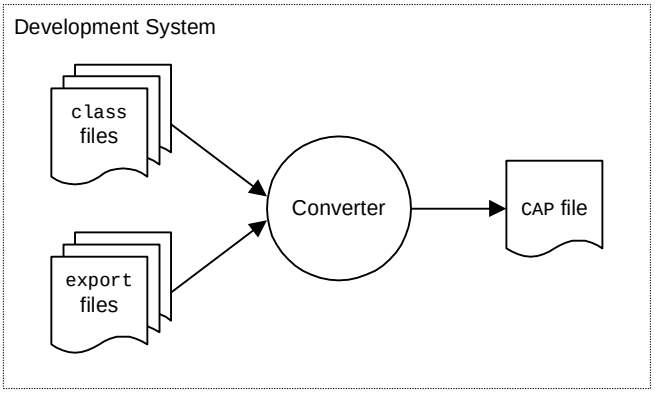


FIGURE 1-1 Java Card Applet Conversion

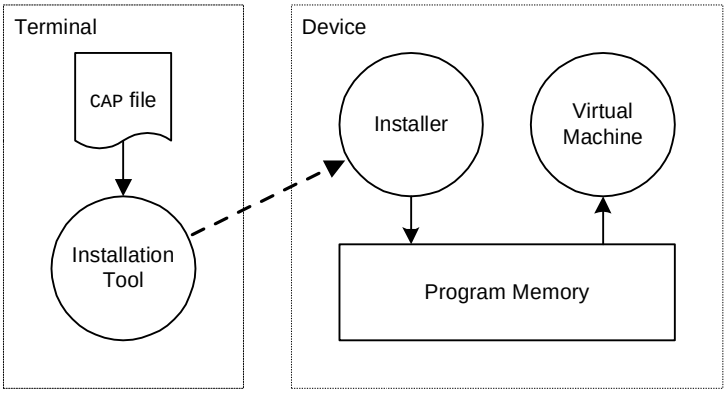


FIGURE 1-2 Java Card Applet Installation

Development of a Java Card applet begins as with any other Java program: a developer writes one or more Java classes, and compiles the source code with a Java compiler, producing one or more `class` files. The applet is run, tested and debugged on a workstation using simulation tools to emulate the device environment. Then, when an applet is ready to be downloaded to a device, the `class` files comprising the applet are converted to a CAP (converted applet) file using a Java Card Converter.

The Java Card Converter takes as input not only the `class` files to be converted, but also one or more `export` files. An `export` file contains name and link information for the contents of other packages that are imported by the classes being converted. When an applet or library package is converted, the converter can also produce an `export` file for that package.

After conversion, the CAP file is copied to a card terminal, such as a desktop computer with a card reader peripheral. Then an installation tool on the terminal loads the CAP file and transmits it to the Java Card technology enabled device. An installation program on the device receives the contents of the CAP file and prepares the applet to be run by the Java Card virtual machine. The virtual machine itself need not load or manipulate CAP files; it need only execute the applet code found in the CAP file that was loaded onto the device by the installation program.

The division of functionality between the Java Card virtual machine and the installation program keeps both the virtual machine and the installation program small. The installation program may be implemented as a Java program and executed on top of the Java Card virtual machine. Since Java Card instructions are denser than typical machine code, this may reduce the size of the installer. The modularity may enable different installers to be used with a single Java Card virtual machine implementation.

1.3 Java Language Security

One of the fundamental features of the Java virtual machine is the strong security provided in part by the `class` file verifier. Many devices that implement the Java Card platform may be too small to support verification of `CAP` files on the device itself. This consideration led to a design that enables verification on a device but does not rely on it. The data in a `CAP` file that is needed only for verification is packaged separately from the data needed for the actual execution of its applet. This allows for flexibility in how security is managed in an implementation.

There are several options for providing language-level security on a Java Card technology enabled device. The conceptually simplest is to verify the contents of a `CAP` file on the device as it is downloaded or after it is downloaded. This option might only be feasible in the largest of devices. However, some subset of verification might be possible even on smaller devices. Other options rely on some combination of one or more of: physical security of the installation terminal, a cryptographically enforced chain of trust from the source of the `CAP` file, and pre-download verification of the contents of a `CAP` file.

The Java Card platform standards say as little as possible about `CAP` file installation and security policies. Since smart cards must serve as secure processors in many different systems with different security requirements, it is necessary to allow a great deal of flexibility to meet the needs of smart card issuers and users.

1.4 Java Card Runtime Environment Security

The standard runtime environment for the Java Card platform is the Java Card Runtime Environment (JCRE). The JCRE consists of an implementation of the Java Card virtual machine along with the Java Card API classes. While the Java Card virtual machine has responsibility for ensuring Java language-level security, the JCRE imposes additional runtime security requirements on devices that implement the JCRE, which results in a need for additional features on the Java Card virtual machine. Throughout this document, these additional features are designated as JCRE-specific.

The basic runtime security feature imposed by the JCRE enforces isolation of applets using what is called an *applet firewall.* The applet firewall prevents the objects that were created by one applet from being used by another applet. This prevents unauthorized access to both the fields and methods of class instances, as well as the length and contents of arrays.

Isolation of applets is an important security feature, but it requires a mechanism to allow applets to share objects in situations where there is a need to interoperate. The JCRE allows such sharing using the concept of shareable interface objects. These objects provide the only way an applet can make its objects available for use by other applets. For more information about using sharable interface objects, see the description of the interface `javacard.framework.Shareable` in the *Java Card 2.1 Application Programming Interface* specification. Some descriptions of firewall-related features will make reference to the `Shareable` interface.

The applet firewall also protects from unauthorized use the objects owned by the JCRE itself. The JCRE can use mechanisms not reflected in the Java Card API to make its objects available for use by applets. A full description of the JCRE-related isolation and sharing features can be found in the *Java Card 2.1 Runtime Environment Specification*.

Appendix JCVM01

CHAPTER 2

A Subset of the Java Virtual Machine

This chapter describes the subset of the Java virtual machine and language that is supported in the Java Card 2.1 platform.

2.1 Why a Subset is Needed

It would be ideal if programs for smart cards could be written using all of the Java programming language, but a full implementation of the Java virtual machine is far too large to fit on even the most advanced resource-constrained devices available today.

A typical resource-constrained device has on the order of 1K of RAM, 16K of non-volatile memory (EEPROM or flash) and 24K of ROM. The code for implementing string manipulation, single and double-precision floating point arithmetic, and thread management would be larger than the ROM space on such a device. Even if it could be made to fit, there would be no space left over for class libraries or application code. RAM resources are also very limited. The only workable option is to implement Java Card technology as a subset of the Java platform.

2.2 Java Card Language Subset

Applets written for the Java Card platform are written in the Java programming language. They are compiled using Java compilers. Java Card technology uses a subset of the Java language, and familiarity with the Java platform is required to understand the Java Card platform.

The items discussed in this section are not described to the level of a language specification. For complete documentation on the Java programming language, see *The Java Language Specification* (§1.1).

2.2.1 Unsupported Items

The items listed in this section are elements of the Java programming language and platform that are not supported by the Java Card platform.

2.2.1.1 Unsupported Features

Dynamic Class Loading

Dynamic class loading is not supported in the Java Card platform. An implementation of the Java Card platform is not able to load classes dynamically. Classes are either masked into the card during manufacturing or downloaded through an installation process after the card has been issued. Programs executing on the card may only refer to classes that already exist on the card, since there is no way to download classes during the normal execution of application code.

Security Manager

Security management in the Java Card platform differs significantly from that of the Java platform. In the Java platform, there is a Security Manager class (`java.lang.SecurityManager`) responsible for implementing security features. In the Java Card platform, language security policies are implemented by the virtual machine. There is no Security Manager class that makes policy decisions on whether to allow operations.

Garbage Collection & Finalization

Java Card technology does not require a garbage collector. Nor does Java Card technology allow explicit deallocation of objects, since this would break the Java programming language's required pointer-safety. Therefore, application programmers cannot assume that objects that are allocated are ever deallocated. Storage for unreachable objects will not necessarily be reclaimed.

Finalization is also not required. `finalize()` will not necessarily be called automatically by the Java Card virtual machine, and programmers should not rely on this behavior.

Threads

The Java Card virtual machine does not support multiple threads of control. Java Card programs cannot use class `Thread` or any of the thread-related keywords in the Java programming language.

Cloning

The Java Card platform does not support cloning of objects. Java Card API class `Object` does not implement a `clone` method, and there is no `Cloneable` interface provided.

Access Control in Java Packages

The Java Card language subset supports the package access control defined in the Java language. However, there are two cases that are not supported.

- If a class implements a method with `package` access visibility, a subclass cannot override the method and change the access visibility of the method to `protected` or `public`.
- An interface that is defined with `package` access visibility cannot be extended by an interface with `public` access visibility.

2.2.1.2 Keywords

The following keywords indicate unsupported options related to native methods, threads and memory management.

```
native          synchronized    transient       volatile
```

2.2.1.3 Unsupported Types

The Java Card platform does not support types `char`, `double`, `float` or `long`, or operations on those types. It also does not support arrays of more than one dimension.

2.2.1.4 Classes

In general, none of the Java core API classes are supported in the Java Card platform. Some classes from the `java.lang` package are supported (see §2.2.2.4), but none of the rest are. For example, classes that are *not* supported are `String`, `Thread` (and all thread-related classes), wrapper classes such as `Boolean` and `Integer`, and class `Class`.

System

Class `java.lang.System` is not supported. Java Card technology supplies a class `javacard.framework.JCSystem`, which provides an interface to system behavior.

2.2.2 Supported Items

If a language feature is not explicitly described as unsupported, it is part of the supported subset. Notable supported features are described in this section.

2.2.2.1 Features

Packages

Software written for the Java Card platform follows the standard rules for the Java platform packages. Java Card API classes are written as Java source files, which include package designations. Package mechanisms are used to identify and control access to classes, static fields and static methods. Except as noted in “Access Control in Java Packages” (§2.2.1.1), packages in the Java Card platform are used exactly the way they are in the Java platform.

Dynamic Object Creation

The Java Card platform programs supports dynamically created objects, both class instances and arrays. This is done, as usual, by using the `new` operator. Objects are allocated out of the heap.

As noted in “Garbage Collection & Finalization” (§2.2.1.1), a Java Card virtual machine will not necessarily garbage collect objects. Any object allocated by a virtual machine may continue to exist and consume resources even after it becomes unreachable.

Virtual Methods

Since Java Card objects are Java programming language objects, invoking virtual methods on objects in a program written for the Java Card platform is exactly the same as in a program written for the Java platform. Inheritance is supported, including the use of the `super` keyword.

Interfaces

Java Card classes may define or implement interfaces as in the Java programming language. Invoking methods on interface types works as expected. Type checking and the `instanceof` operator also work correctly with interfaces.

Exceptions

Java Card programs may define, throw and catch exceptions, as in Java programs. Class `Throwable` and its relevant subclasses are supported. (Some `Exception` and `Error` subclasses are omitted, since those exceptions cannot occur in the Java Card platform. See §2.3.3 for specification of errors and exceptions.)

2.2.2.2 Keywords

The following keywords are supported. Their use is the same as in the Java programming language.

`abstract`	`default`	`if`	`private`	`this`
`boolean`	`do`	`implements`	`protected`	`throw`
`break`	`else`	`import`	`public`	`throws`
`byte`	`extends`	`instanceof`	`return`	`try`
`case`	`final`	`int`	`short`	`void`
`catch`	`finally`	`interface`	`static`	`while`
`class`	`for`	`new`	`super`	
`continue`	`goto`	`package`	`switch`	

2.2.2.3 Types

Java programming language types `boolean`, `byte`, `short`, and `int` are supported. Objects (class instances and single-dimensional arrays) are also supported. Arrays can contain the supported primitive data types, objects, and other arrays.

Some Java Card implementations might not support use of the `int` data type. (Refer to §2.2.3.1.)

2.2.2.4 Classes

Most of the classes in the `java.lang` package are not supported in Java Card. The following classes from `java.lang` are supported on the card in a limited form.

Object

Java Card classes descend from `java.lang.Object`, just as in the Java programming language. Most of the methods of `Object` are not available in the Java Card API, but the class itself exists to provide a root for the class hierarchy.

Throwable

Class `Throwable` and its subclasses are supported. Most of the methods of `Throwable` are not available in the Java Card API, but the class itself exists to provide a common ancestor for all exceptions.

2.2.3 Optionally Supported Items

This section describes the optional features of the Java Card platform. An optional feature is not required to be supported in a Java Card compatible implementation. However, if an implementation does include support for an optional feature, it must be supported fully, and exactly as specified in this document.

2.2.3.1 `int`

The `int` keyword and 32-bit integer data types need not be supported in a Java Card implementation. A Java Card virtual machine that does not support the `int` data type will reject programs which use the `int` data type or 32-bit intermediate values.

2.2.4 Limitations of the Java Card Virtual Machine

The limitations of resource-constrained hardware prevent Java Card programs from supporting the full range of functionality of certain Java platform features. The features in question are supported, but a particular virtual machine may limit the range of operation to less than that of the Java platform.

To ensure a level of portability for application code, this section establishes a minimum required level for partial support of these language features.

The limitations here are listed as maximums from the application programmer's perspective. Applets that do not violate these maximum values can be converted into Java Card CAP files, and will be portable across all Java Card implementations. From the Java Card virtual machine implementer's perspective, each maximum listed indicates a minimum level of support that will allow portability of applets.

2.2.4.1 Classes

Classes in a Package

A package can contain at most 255 public classes and interfaces.

Interfaces

A class can implement at most 15 interfaces, including interfaces implemented by superclasses.

An interface can inherit from at most 15 superinterfaces.

Static Fields

A class can have at most 256 public or protected static fields.

Static Methods

A class can have at most 256 public or protected static methods.

2.2.4.2 Objects

Methods

A class can implement a maximum of 128 public or protected instance methods, and a maximum of 128 instance methods with package visibility. These limits include inherited methods.

Class Instances

Class instances can contain a maximum of 255 fields, where an `int` data type is counted as occupying two fields.

Arrays

Arrays can hold a maximum of 32767 fields.

2.2.4.3 Methods

The maximum number of local variables that can be used in a method is 255, where an `int` data type is counted as occupying two local variables.

A method can have at most 32767 Java Card virtual machine bytecodes. The number of Java Card bytecodes may differ from the number of Java bytecodes in the Java virtual machine implementation of that method.

2.2.4.4 Switch Statements

The format of the Java Card virtual machine switch instructions limits switch statements to a maximum of 65536 cases. This limit is far greater than the limit imposed by the maximum size of methods (§2.2.4.3).

2.2.4.5 Class Initialization

There is limited support for initialization of static field values in `<clinit>` methods. Static fields of applets may only be initialized to primitive compile-time constant values, or arrays of primitive compile-time constants. Static fields of user libraries may only be initialized to primitive compile-time constant values. Primitive constant data types include `boolean`, `byte`, `short`, and `int`.

2.3 Java Card VM Subset

Java Card technology uses a subset of the Java virtual machine, and familiarity with the Java platform is required to understand the Java Card virtual machine.

The items discussed in this section are not described to the level of a virtual machine specification. For complete documentation on the Java virtual machine, refer to §1.1 of *The Java™ Virtual Machine Specification*.

2.3.1 `class` File Subset

The operation of the Java Card virtual machine can be defined in terms of standard Java platform `class` files. Since the Java Card virtual machine supports only a subset of the behavior of the Java virtual machine, it also supports only a subset of the standard `class` file format.

2.3.1.1 Not Supported in `Class` Files

Field Descriptors

Field descriptors may not contain *BaseType* characters `C`, `D`, `F` or `L`. *ArrayType* descriptors for arrays of more than one dimension may not be used.

Constant Pool

Constant pool table entry tags that indicate unsupported types are not supported.

Constant Type	Value
`CONSTANT_String`	8
`CONSTANT_Float`	4
`CONSTANT_Long`	5
`CONSTANT_Double`	6

TABLE 2-1 Unsupported Java constant pool tags

Constant pool structures for types `CONSTANT_String_info`, `CONSTANT_Float_info`, `CONSTANT_Long_info` and `CONSTANT_Double_info` are not supported.

Fields

In `field_info` structures, the access flags `ACC_VOLATILE` and `ACC_TRANSIENT` are not supported.

Methods

In `method_info` structures, the access flags `ACC_SYNCHRONIZED` and `ACC_NATIVE` are not supported.

2.3.1.2 Supported in Class Files

ClassFile

All items in the `ClassFile` structure are supported.

Field Descriptors

Field descriptors may contain *BaseType* characters `B`, `I`, `S` and `Z`, as well as any *ObjectType*. *ArrayType* descriptors for arrays of a single dimension may also be used.

Method Descriptors

All forms of method descriptors are supported.

Constant pool

Constant pool table entry tags for supported data types are supported.

Constant Type	Value
`CONSTANT_Class`	`7`
`CONSTANT_Fieldref`	`9`
`CONSTANT_Methodref`	`10`
`CONSTANT_InterfaceMethodref`	`11`
`CONSTANT_Integer`	`3`
`CONSTANT_NameAndType`	`12`
`CONSTANT_Utf8`	`1`

TABLE 2-2 Supported Java constant pool tags.

Constant pool structures for types `CONSTANT_Class_info`, `CONSTANT_Fieldref_info`, `CONSTANT_Methodref_info`, `CONSTANT_InterfaceMethodref_info`, `CONSTANT_Integer_info`, `CONSTANT_NameAndType_info` and `CONSTANT_Utf8_info` are supported.

Fields

In `field_info` structures, the supported access flags are `ACC_PUBLIC`, `ACC_PRIVATE`, `ACC_PROTECTED`, `ACC_STATIC` and `ACC_FINAL`.

The remaining components of `field_info` structures are fully supported.

Methods

In `method_info` structures, the supported access flags are `ACC_PUBLIC`, `ACC_PRIVATE`, `ACC_PROTECTED`, `ACC_STATIC`, `ACC_FINAL` and `ACC_ABSTRACT`.

The remaining components of `method_info` structures are fully supported.

Attributes

The `attribute_info` structure is supported. The `Code`, `ConstantValue`, `Exceptions` and `LocalVariableTable` attributes are supported.

2.3.2 Bytecode Subset

The following sections detail the bytecodes that are either supported or unsupported in the Java Card platform. For more details, refer to Chapter 6, “Instruction Set.”

2.3.2.1 Unsupported Bytecodes

lconst_<l>	fconst_<f>	dconst_<d>	ldc2_w2
lload	fload	dload	lload_<n>
fload_<n>	dload_<n>	laload	faload
daload	caload	lstore	fstore
dstore	lstore_<n>	fstore_<n>	dstore_<n>
lastore	fastore	dastore	castore
ladd	fadd	dadd	lsub
fsub	dsub	lmul	fmul
dmul	ldiv	fdiv	ddiv
lrem	frem	drem	lneg
fneg	dneg	lshl	lshr
lushr	land	lor	lxor
i2l	i2f	i2d	l2i
l2f	l2d	f2i	f2d
d2i	d2l	d2f	i2c
lcmp	fcmpl	fcmpg	dcmpl
dcmpg	lreturn	freturn	dreturn
monitorenter	monitorexit	multianewarray	goto_w
jsr_w			

2.3.2.2 Supported Bytecodes

nop	aconst_null	iconst_<i>	bipush
sipush	ldc	ldc_w	iload
aload	iload_<n>	aload_<n>	iaload
aaload	baload	saload	istore
astore	istore_<n>	astore_<n>	iastore
aastore	bastore	sastore	pop
pop2	dup	dup_x1	dup_x2
dup2	dup2_x1	dup2_x2	swap
iadd	isub	imul	idiv
irem	ineg	ior	ishl
ishr	iushr	iand	ixor
iinc	i2b	i2s	if<cond>
ificmp_<cond>	ifacmp_<cond>	goto	jsr
ret	tableswitch	lookupswitch	ireturn
areturn	return	getstatic	putstatic
getfield	putfield	invokevirtual	invokespecial
invokestatic	invokeinterface	new	newarray
anewarray	arraylength	athrow	checkcast
instanceof	wide	ifnull	ifnonnull

2.3.2.3 Static Restrictions on Bytecodes

For it to be acceptable to a Java Card virtual machine, a `class` file must conform to the following restrictions on the static form of bytecodes.

ldc, ldc_w

The *ldc* and *ldc_w* bytecodes can only be used to load integer constants. The constant pool entry at *index* must be a `CONSTANT_Integer` entry. If a program contains an *ldc* or *ldc_w* instruction that is used to load an integer value less than -32768 or greater than 32767, that program will require the optional `int` instructions (§2.2.3.1).

lookupswitch

The value of the *npairs* operand must be less than 65536. The bytecode can contain at most 65535 cases. This limit is far greater than the limit imposed by the maximum size of methods (§2.2.4.3). If a program contains a *lookupswitch* instruction that uses keys of type `int`, that program will require the optional `int` instructions (§2.2.3.1). Otherwise, key values must be in the range -32768 to 32767.

tableswitch

The values of the *high* and *low* operands must both be at least -32768 and at most 32767 (so they can fit in a `short`). The bytecode can contain at most 65536 cases. This limit is far greater than the limit imposed by the maximum size of methods (§2.2.4.3).If a program contains a *tableswitch* instruction that uses indexes of type `int`, that program will require the optional `int` instructions (§2.2.3.1). Otherwise, index values must be in the range -32768 to 32767.

wide

The *wide* bytecode cannot be used to generate local indices greater than 127, and it cannot be used with any instructions other than *iinc*. It can only be used with an *iinc* bytecode to extend the range of the increment constant.

2.3.3 Exceptions

Java Card provides full support for the Java platform's exception mechanism. Users can define, throw and catch exceptions just as in the Java platform. Java Card also makes use of the exceptions and errors defined in *The Java Language Specification* [1]. An updated list of the Java platform's exceptions is provided in the JDK documentation.

Not all of the Java platform's exceptions are supported in Java Card. Exceptions related to unsupported features are naturally not supported. Class loader exceptions (the bulk of the checked exceptions) are not supported. And no exceptions or errors defined in packages other than `java.lang` are supported.

Note that some exceptions may be supported to the extent that their error conditions are detected correctly, but classes for those exceptions will not necessarily be present in the API.

The supported subset is described in the tables below.

2.3.3.1 Uncaught and Uncatchable Exceptions

In the Java platform, uncaught exceptions and errors will cause the virtual machine's current thread to exit. As the Java Card virtual machine is single-threaded, uncaught exceptions or errors will cause the virtual machine to halt. Further response to uncaught exceptions or errors after halting the virtual machine is an implementation-specific policy, and is not mandated in this document.

Some error conditions are known to be unrecoverable at the time they are thrown. Throwing a runtime exception or error that cannot be caught will also cause the virtual machine to halt. As with uncaught exceptions, implementations may take further responses after halting the virtual machine. Uncatchable exceptions and errors which are supported by the Java Card platform may not be reflected in the Java Card API, though the Java Card platform will correctly detect the error condition.

2.3.3.2 Checked Exceptions

Exception	Supported	Not Supported
`ClassNotFoundException`		●
`CloneNotSupportedException`		●
`IllegalAccessException`		●
`InstantiationException`		●
`InterruptedException`		●
`NoSuchFieldException`		●
`NoSuchMethodException`		●

TABLE 2-3 Support of Java checked exceptions

2.3.3.3 Runtime Exceptions

Runtime Exception	Supported	Not Supported
ArithmeticException	●	
ArrayStoreException	●	
ClassCastException	●	
IllegalArgumentException		●
IllegalThreadStateException		●
NumberFormatException		●
IllegalMonitorStateException		●
IllegalStateException		●
IndexOutOfBoundsException	●	
ArrayIndexOutOfBoundsException	●	
StringIndexOutOfBoundsException		●
NegativeArraySizeException	●	
NullPointerException	●	
SecurityException	●	

TABLE 2-4 Support of Java runtime exceptions

2.3.3.4 Errors

Error	Supported	Not Supported
LinkageError	●	
ClassCircularityError	●	
ClassFormatError	●	
ExceptionInInitializerError	●	
IncompatibleClassChangeError	●	
AbstractMethodError	●	
IllegalAccessError	●	
InstantiationError	●	
NoSuchFieldError	●	
NoSuchMethodError	●	
NoClassDefFoundError	●	
UnsatisfiedLinkError	●	
VerifyError	●	
ThreadDeath		●
VirtualMachineError	●	
InternalError	●	
OutOfMemoryError	●	
StackOverflowError	●	
UnknownError	●	

TABLE 2-5 Support of Java errors

Appendix JCVM01

CHAPTER 3

Structure of the Java Card Virtual Machine

The specification of the Java Card virtual machine is in many ways quite similar to that of the Java Virtual Machine. This similarity is of course intentional, as the design of the Java Card virtual machine was based on that of the Java Virtual Machine. Rather than reiterate all the details of this specification which are shared with that of the Java Virtual Machine, this chapter will mainly refer to its counterpart in the *Java Virtual Machine Specification, 1st Edition*, providing new information only where the Java Card virtual machine differs.

3.1 Data Types and Values

The Java Card virtual machine supports the same two kinds of data types as the Java Virtual Machine: *primitive types* and *reference types*. Likewise, the same two kinds of values are used: *primitive values* and *reference values*.

The primitive data types supported by the Java Card virtual machine are the *numeric types* and the `returnAddress` type. The numeric types consist only of the *integral types*:

- `byte`, whose values are 8-bit signed two's complement integers
- `short`, whose values are 16-bit signed two's complement integers

Some Java Card virtual machine implementations may also support an additional integral type:

- `int`, whose values are 32-bit signed two's complement integers

Support for `reference` types is identical to that in the Java Virtual Machine.

3.2 Words

The Java Card virtual machine is defined in terms of an abstract storage unit called a *word*. This specification does not mandate the actual size in bits of a word on a specific platform. A word is large enough to hold a value of type `byte`, `short`, `reference` or `returnAddress`. Two words are large enough to hold a value of type `int`.

The actual storage used for values in an implementation is platform-specific. There is enough information present in the descriptor component of a CAP file to allow an implementation to optimize the storage used for values in variables and on the stack.

3.3 Runtime Data Areas

The Java Card virtual machine can support only a single thread of execution. Any runtime data area in the Java Virtual Machine which is duplicated on a per-thread basis will have only one global copy in the Java Card virtual machine.

The Java Card virtual machine's heap is not required to be garbage collected. Objects allocated from the heap will not necessarily be reclaimed.

This specification does not include support for `native` methods, so there are no native method stacks.

Otherwise, the runtime data areas are as documented for the Java Virtual Machine.

3.4 Contexts

Each applet running on a Java Card virtual machine is associated with an execution *context*. The Java Card virtual machine uses the context of the current frame to enforce security policies for inter-applet operations.

There is a one-to-one mapping between contexts and packages in which applets are defined. An easy way to think of a context is as the runtime equivalent of a package, since Java packages are compile-time constructs and have no direct representation at runtime. As a consequence, all applets managed by applet instances of applet classes from the same package will share the same context.

The Java Card Runtime Environment also has its own context. Framework objects execute in this *JCRE context*.

The context of the currently executing method is known as the *current context*. Every object in a Java Card virtual machine is owned by a particular context. The *owning context* is the context that was current when the object was created.

When a method in one context successfully invokes a method on an object in another context, the Java Card virtual machine performs a *context switch*. Afterwards the invoked method's context becomes the current context. When the invoked method returns, the current context is switched back to the previous context.

3.5 Frames

Java Card virtual machine *frames* are very similar to those defined for the Java Virtual Machine. Each frame has a set of local variables and an operand stack. Frames also contain a reference to a constant pool, but since all constant pools for all classes in a package are merged, the reference is to the constant pool for the current class' package.

Each frame also includes a reference to the context in which the current method is executing.

3.6 Representation of Objects

The Java Card virtual machine does not mandate a particular internal structure for objects or a particular layout of their contents. However, the core components in a CAP file are defined assuming a default structure for certain runtime structures (such as descriptions of classes), and a default layout for the contents of dynamically allocated objects. Information from the descriptor component of the CAP file can be used to format objects in whatever way an implementation requires.

3.7 Special Initialization Methods

The Java Card virtual machine supports *instance initialization methods* exactly as does the Java Virtual Machine.

The Java Card virtual machine includes only limited support for *class or interface initialization methods*. There is no general mechanism for executing `<clinit>` methods on a Java Card virtual machine. Instead, a CAP file includes information for initializing class data as defined in Chapter 2, “A Subset of the Java Virtual Machine.”

3.8 Exceptions

Exception support in the Java Card virtual machine is identical to support for exceptions in the Java Virtual Machine.

3.9 Binary File Formats

This specification defines two binary file formats which enable platform-independent development, distribution and execution of Java Card software.

The CAP file format describes files that contain executable code and can be downloaded and installed onto a Java Card enabled device. A CAP file is produced by a Java Card Converter tool, and contains a converted form of an entire package of Java classes. This file format's relationship to the Java Card virtual machine is analogous to the relationship of the `class` file format to the Java Virtual Machine.

The `export` file format describes files that contain the public linking information of Java Card packages. A package's `export` file is used when converting client packages of that package.

3.10 Instruction Set Summary

The Java Card virtual machine instruction set is quite similar to the Java Virtual Machine instruction set. Individual instructions consist of a one-byte *opcode* and zero or more *operands*. The pseudo-code for the Java Card virtual machine's instruction fetch-decode-execute loop is the same. Multi-byte operand data is also encoded in *big-endian* order.

There are a number of ways in which the Java Card virtual machine instruction set diverges from that of the Java Virtual Machine. Most of the differences are due to the Java Card virtual machine's more limited support for data types. Another source of

divergence is that the Java Card virtual machine is intended to run on 8-bit and 16-bit architectures, whereas the Java Virtual Machine was designed for a 32-bit architecture. The rest of the differences are all oriented in one way or another toward optimizing the size or performance of either the Java Card virtual machine or Java Card programs. These changes include inlining constant pool data directly in instruction opcodes or operands, adding multiple versions of a particular instruction to deal with different datatypes, and creating composite instructions for operations on the current object.

3.10.1 Types and the Java Card Virtual Machine

The Java Card virtual machine supports only a subset of the types supported by the Java Virtual Machine. This subset is described in Chapter 2, “A Subset of the Java Virtual Machine.” Type support is reflected in the instruction set, as instructions encode the data types on which they operate.

Given that the Java Card virtual machine supports fewer types than the Java Virtual Machine, there is an opportunity for better support for smaller data types. Lack of support for large numeric data types frees up space in the instruction set. This extra instruction space has been used to directly support arithmetic operations on the `short` data type.

Some of the extra instruction space has also been used to optimize common operations. Type information is directly encoded in field access instructions, rather than being obtained from an entry in the constant pool.

TABLE 3-1 summarizes the type support in the instruction set of the Java Card virtual machine. Only instructions that exist for multiple types are listed. Wide and composite forms of instructions are not listed either. A specific instruction, with type information, is built by replacing the *T* in the instruction template in the opcode column by the letter representing the type in the type column. If the type column for some instruction is blank, then no instruction exists supporting that operation on that type. For instance, there is a load instruction for type `short`, *sload*, but there is no load instruction for type `byte`.

opcode	byte	short	int	reference
Tspush	*bspush*	*sspush*		
Tipush	*bipush*	*sipush*	*iipush*	
Tconst		*sconst*	*iconst*	*aconst*
Tload		*sload*	*iload*	*aload*
Tstore		*sstore*	*istore*	*astore*
Tinc		*sinc*	*iinc*	
Taload	*baload*	*saload*	*iaload*	*aaload*
Tastore	*bastore*	*sastore*	*iastore*	*aastore*
Tadd		*sadd*	*iadd*	
Tsub		*ssub*	*isub*	
Tmul		*smul*	*imul*	
Tdiv		*sdiv*	*idiv*	
Trem		*srem*	*irem*	
Tneg		*sneg*	*ineg*	
Tshl		*sshl*	*ishl*	
Tshr		*sshr*	*ishr*	
Tushr		*sushr*	*iushr*	
Tand		*sand*	*iand*	
Tor		*sor*	*ior*	
Txor		*sxor*	*ixor*	
s2T	*s2b*		*s2i*	
i2T	*i2b*	*i2s*		
Tcmp			*icmp*	
if_TcmpOP		*if_scmpOP*		*if_acmpOP*
Tlookupswitch		*slookupswitch*	*ilookupswitch*	
Ttableswitch		*stableswitch*	*itableswitch*	
Treturn		*sreturn*	*ireturn*	*areturn*
getstatic_T	*getstatic_b*	*getstatic_s*	*getstatic_i*	*getstatic_a*
putstatic_T	*putstatic_b*	*putstatic_s*	*putstatic_i*	*putstatic_a*
getfield_T	*getfield_b*	*getfield_s*	*getfield_i*	*getfield_a*
putfield_T	*putfield_b*	*putfield_s*	*putfield_i*	*putfield_a*

TABLE 3-1 Type support in the Java Card Virtual Machine Instruction Set

The mapping between Java storage types and Java Card virtual machine computational types is summarized in TABLE 3-2.

Java (Storage) Type	Size in Bits	Computational Type
`byte`	8	`short`
`short`	16	`short`
`int`	32	`int`

TABLE 3-2 Storage types and computational types

Chapter 7, “Java Card Virtual Machine Instruction Set,” describes the Java Card virtual machine instruction set in detail.

Appendix JCVM01

CHAPTER 4

Binary Representation

This chapter presents information about the binary representation of Java Card programs. Java Card binaries are usually contained in files, therefore this chapter addresses binary representation in terms of this common case.

Several topics relating to binary representation are covered. The first section describes the basic organization of program representation in `export` and `CAP` files, as well as the use of the JAR file containers. The second section covers how Java Card applets and packages are named using unique identifiers. The third section presents the scheme used for naming and linking items within Java Card packages. The fourth and fifth sections describe the constraints for upward compatibility between different versions of a Java Card binary program file, and versions assigned based upon that compatibility.

4.1 Java Card File Formats

Java programs are represented in compiled, binary form as `class` files. Java `class` files are used not only to execute programs on a Java virtual machine, but also to provide type and name information to a Java compiler. In the latter role, a `class` file is essentially used to document the API of its class to client code. That client code is compiled into its own `class` file, including symbolic references used to dynamically link to the API class at runtime.

Java Card technology uses a different strategy for binary representation of programs. Executable binaries and interface binaries are represented in two separate files. These files are respectively called `CAP` files (for converted applet) and `export` files.

4.1.1 `Export` File Format

`Export` files are not used directly on a device that implements a Java Card virtual machine. However, the information in an `export` file is critical to the operation of the virtual machine on a device. An `export` file can be produced by a Java Card converter when a package is converted. This package's `export` file can be used later to convert another package that imports classes from the first package. Information in the `export` file is included in the `CAP` file of the second package, then is used on the device to link the contents of the second package to items imported from the first package.

A Java Card `export` file contains the public interface information for an entire package of classes. This means that an `export` file only contains information about the public API of a package, and does not include information used to link classes within a package.

The name of an `export` file is the last portion of the package specification followed by the extension '`.exp`'. For example, the name of the `export` file of the `javacard.framework` package must be `framework.exp`. Operating systems that impose limitations on file name lengths may transform an `export` file's name according to their own conventions.

For a complete description of the Java Card `export` file format, see Chapter 5.

4.1.2 `CAP` File Format

A Java Card `CAP` file contains a binary representation of a package of classes that can be installed on a device and used to execute the package's classes on a Java Card virtual machine.

A `CAP` file is produced by a Java Card converter when a package of classes is converted. A `CAP` file can contain a user library, or one or more applet definitions. A `CAP` file consists of a set of components, each of which describes a different aspect of the contents. The set of components in a `CAP` file can vary, depending on whether the file contains a library or applet definition(s).

For a complete description of the Java Card `CAP` File format, see Chapter 6.

4.1.3 JAR File Container

The JAR file format is used as the container format for `CAP` files. What this specification calls a "`CAP` file" is just a JAR file that contains the required set of `CAP` components (see Chapter 6).

CAP component files in a JAR file are located in a subdirectory called javacard that is in a directory representing the package. For example, the CAP component files of the package com.sun.framework are located in the directory com/sun/framework/javacard.

An export file may also be contained in a JAR file, whether that JAR file contains CAP component files or not. If an export file is included, it must be located in the same directory as the CAP component files for that package would be.

The name of a JAR file containing CAP component files is not defined as part of this specification. Other files, including other CAP files, may also reside in a JAR file that contains CAP component files.

4.2 AID-based Naming

This section describes the mechanism used for naming applets and packages in Java Card CAP files and export files, and custom components in Java Card CAP files. Java class files use Unicode strings to name Java packages. As the Java Card platform does not include support for strings, an alternative mechanism for naming is provided.

ISO 7816 is a multipart standard that describes a broad range of technology for building smart card systems. ISO 7816-5 defines the AID (application identifier) data format to be used for unique identification of card applications (and certain kinds of files in card file systems). The Java Card platform uses the AID data format to identify applets and packages. AIDs are administered by the International Standards Organization (ISO), so they can be used as unique identifiers.

4.2.1 The AID Format

This section presents a minimal description of the AID data format used in Java Card technology. For complete details, refer to ISO 7816-5, AID Registration Category ‘D’ format.

The AID format used by the Java Card platform is an array of bytes that can be interpreted as two distinct pieces, as shown in FIGURE 4-1. The first piece is a 5-byte value known as a RID (resource identifier). The second piece is a variable length value known as a PIX (proprietary identifier extension). A PIX can be from 0 to 11 bytes in length. Thus an AID can be from 5 to 16 bytes in total length.

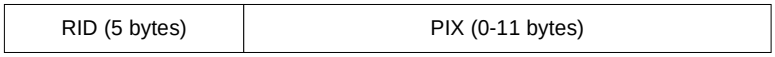


FIGURE 4-1 AID Format

ISO controls the assignment of RIDs to companies, with each company obtaining its own unique RID from the ISO. Companies manage assignment of PIXs for AIDs using their own RIDs.

4.2.2 AID Usage

In the Java platform, packages are uniquely identified using Unicode strings and a naming scheme based on internet domain names. In the Java Card platform, packages and applets are identified using AIDs.

Any package that is represented in an `export` file must be assigned a unique AID. The AID for a package is constructed from the concatenation of the company's RID and a PIX for that package. This AID corresponds to the string name for the package, as shown in FIGURE 4-2.

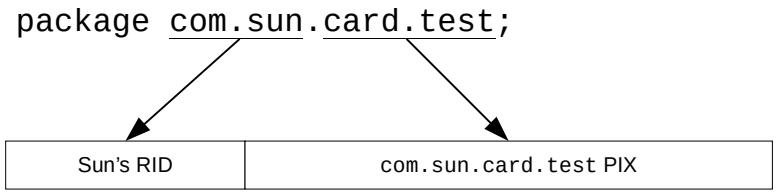


FIGURE 4-2 Mapping package identifiers to AIDs

Each applet installed on a Java Card technology enabled device must also have a unique AID. This AID is constructed similarly to a package AID. It is a concatenation of the applet provider's RID and PIX for that applet. An applet AID must not have the same value as the AID of any package or the AID of any other applet. If a `CAP` file defines multiple applets, all applet AIDs in that `CAP` file must have the same RID.

Custom components defined in a `CAP` file are also identified using AIDs. Like AIDs for applets and packages, component AIDs are formed by concatenating a RID and a PIX. All AIDs of new components must have the same RID as the AID for the package defined in the `CAP` file.

4.3 Token-based Linking

This section describes a scheme that allows downloaded software to be linked against APIs on a Java Card technology enabled device. The scheme represents referenced items as opaque tokens, instead of Unicode strings as are used in Java class files. The two basic requirements of this linking scheme are that it allows linking on the device, and that it does not require internal implementation details of APIs to be revealed to clients of those APIs. Secondary requirements are that the scheme be efficient in terms of resource use on the device, and have acceptable performance for linking. And of course, it must preserve the semantics of the Java language.

4.3.1 Externally Visible Items

Classes (including Interfaces) in Java packages may be declared with public or package visibility. A class's methods and fields may be declared with public, protected, package or private visibility. For purposes of this document, we define public classes, public or protected fields, and public or protected methods to be *externally visible* from the package. All externally visible items are described in a package's `export` file.

Each externally visible item must have a token associated with it to enable references from other packages to the item to be resolved on a device. There are six kinds of items in a package that require external identification.

- Classes (including Interfaces)
- Static Fields
- Static Methods
- Instance Fields
- Virtual Methods
- Interface Methods

4.3.2 Private Tokens

Items that are not externally visible are *internally visible*. Internally visible items are not described in a package's `export` file, but some such items use *private tokens* to represent internal references. External references are represented by *public tokens.* There are two kinds of items that can be assigned private tokens.

- Instance Fields
- Virtual Methods

4.3.3 The `Export` File and Conversion

Each externally visible item in a package has an entry in the package's `export` file. Each entry holds the item's name and its token. Some entries may include additional information as well. For detailed information on the `export` file format, see Chapter 5, "The Export File Format."

The `export` file is used to map names for imported items to tokens during package conversion. The Java Card converter uses these tokens to represent references to items in an imported package.

For example, during the conversion of the class files of applet A, the `export` file of `javacard.framework` is used to find tokens for items in the API that are used by the applet. Applet A creates a new instance of framework class `OwnerPIN`. The framework `export` file contains an entry for `javacard.framework.OwnerPIN` that holds the token for this class. The converter places this token in the `CAP` file's constant pool to represent an unresolved reference to the class. The token value is later used to resolve the reference on a device.

4.3.4 References – External and Internal

In the context of a `CAP` file, references to items are made indirectly through a package's constant pool. References to items in other packages are called *external*, and are represented in terms of tokens. References to items in the same `CAP` file are called *internal*, and are represented either in terms of tokens, or in a different internal format.

An external reference to a class is composed of a package token and a class token. Together those tokens specify a certain class in a certain package. An internal reference to a class is a 15-bit value that is a pointer to the class structure's location within the `CAP` file.

An external reference to a static class member, either a field or method, consists of a package token, a class token, and a token for the static field or static method. An internal reference to a static class member is a 16-bit value that is a pointer to the item's location in the `CAP` file.

References to instance fields, virtual methods and interface methods consist of a class reference and a token of the appropriate type. The class reference determines whether the reference is external or internal.

4.3.5 Installation and Linking

External references in a CAP file can be resolved on a device from token form into the internal representation used by the virtual machine.

A token can only be resolved in the context of the package that defines it. Just as the `export` file maps from a package's externally visible names to tokens, there is a set of link information for each package on the device that maps from tokens to resolved references.

4.3.6 Token Assignment

Tokens for an API are assigned by the API's developer and published in the package `export` file(s) for that API. Since the name-to-token mappings are published, an API developer may choose any order for tokens (subject to the constraints listed below).

A particular device platform can resolve tokens into whatever internal representation is most useful for that implementation of a Java Card virtual machine. Some tokens may be resolved to indices. For example, an instance field token may be resolved to an index into a class instance's fields. In such cases, the token value is distinct from and unrelated to the value of the resolved index.

4.3.7 Token Details

Each kind of item in a package has its own independent scope for tokens of that kind. The token range and assignment rules for each kind are listed in TABLE 4-1.

Token Type	Range	Type	Scope
Package	0 - 127	Private	CAP File
Class	0 - 255	Public	Package
Static Field	0 - 255	Public	Class
Static Method	0 - 255	Public	Class
Instance Field	0 - 255	Public or Private	Class
Virtual Method	0 - 127	Public or Private	Class Hierarchy
Interface Method	0 - 127	Public	Class

TABLE 4-1 Token Range, Type and Scope

4.3.7.1 Package

All package references from within a `CAP` file are assigned private *package tokens*; package tokens will never appear in an `export` file. Package token values must be in the range from 0 to 127, inclusive. The tokens for all the packages referenced from classes in a `CAP` file are numbered consecutively starting at zero. The ordering of package tokens is not specified.

4.3.7.2 Classes and Interfaces

All externally visible classes in a package are assigned public *class tokens*. Package-visible classes are not assigned tokens. Class token values must be in the range from 0 to 255, inclusive. The tokens for all the public classes in a package are numbered consecutively starting at zero. The ordering of class tokens is not specified.

4.3.7.3 Static Fields

All externally visible static fields in a package are assigned public *static field tokens.* Package-visible and private static fields are not assigned tokens. No tokens are assigned for final static fields that are initialized to primitive, compile-time constants, as these fields are never linked on a device. The tokens for all other externally visible static fields in a class are numbered consecutively starting at zero. Static fields token values must be in the range from 0 to 255, inclusive. The ordering of static field tokens is not specified.

4.3.7.4 Static Methods

All externally visible static methods in a package are assigned public *static method tokens*, including statically bound instance methods. Static method token values must be in the range from 0 to 255, inclusive. Package-visible and private static methods are not assigned tokens. The tokens for all the externally visible static methods in a class are numbered consecutively starting at zero. The ordering of static method tokens is not specified.

4.3.7.5 Instance Fields

All instance fields defined in a package are assigned either public or private *instance field tokens*. Instance field token values must be in the range from 0 to 255, inclusive. Public and private tokens for instance fields are assigned from the same namespace. The tokens for all the instance fields in a class are numbered consecutively starting at zero, except that the token after an `int` field is skipped and the token for the following field is numbered two greater than the token of the `int` field. Tokens for

externally visible fields must be numbered less than the tokens for package and private fields. For public tokens, the tokens for reference type fields must be numbered greater than the tokens for primitive type fields. For private tokens, the tokens for reference type fields must be numbered less than the tokens for primitive type fields. Beyond that the ordering of instance field tokens in a class is not specified.

Visibility	Category	Type	Token Value
public and protected fields (public tokens)	primitive	`boolean`	0
		`byte`	1
		`short`	2
	references	`byte[]`	3
		`Applet`	4
package and private fields (private tokens)	references	`short[]`	5
		`Object`	6
	primitive	`int`	7
		`short`	9

FIGURE 4-3 Tokens for Instance Fields

4.3.7.6 Virtual Methods

All virtual methods defined in a package are assigned either public or private *virtual method tokens*. Virtual method token values must be in the range from 0 to 127, inclusive. Public and private tokens for virtual methods are assigned from different namespaces. The high bit of the byte containing a virtual method token is set to one if the token is a private token.

Public tokens for the externally visible introduced virtual methods in a class are numbered consecutively starting at one greater than the highest numbered public virtual method token of the class's superclass. If a method overrides a method implemented in the class's superclass, that method uses the same token number as the method in the superclass. The high bit of the byte containing a public virtual method token is always set to zero, to indicate it is a public token. The ordering of public virtual method tokens in a class is not specified.

Private virtual method tokens are assigned differently from public virtual method tokens. If a class and its superclass are defined in the same package, the tokens for the package-visible introduced virtual methods in that class are numbered consecutively starting at one greater than the highest numbered private virtual method token of the class's superclass. If the class and its superclass are defined in different packages, the tokens for the package-visible introduced virtual methods in that class are numbered consecutively starting at zero. If a method overrides a method implemented in the class's superclass, that method uses the same token

number as the method in the superclass. The definition of the Java programming language specifies that overriding a package-visible virtual method is only possible if both the class and its superclass are defined in the same package. The high bit of the byte containing a virtual method token is always set to one, to indicate it is a private token. The ordering of private virtual method tokens in a class is not specified.

4.3.7.7 Interface Methods

All interface methods defined in a package are assigned public *interface method tokens*, as interface methods are always public. Interface methods tokens values must be in the range from 0 to 127, inclusive. The tokens for all the interface methods defined in or inherited by an interface are numbered consecutively starting at zero. The token value for an interface method in a given interface is unrelated to the token values of that same method in any of the interface's superinterfaces. The high bit of the byte containing an interface method token is always set to zero, to indicate it is a public token. The ordering of interface method tokens is not specified.

4.4 Binary Compatibility

In the Java programming language the granularity of binary compatibility can be between classes since binaries are stored in individual `class` files. In Java Card systems Java packages are processed as a single unit, and therefore the granularity of binary compatibility is between packages. In Java Card systems the *binary* of a package is represented in a `CAP` file, and the API of a package is represented in an `export` file.

In a Java Card system, a change to a type in a Java package results in a new `CAP` file. A new `CAP` file is *binary compatible with* (equivalently, does not *break compatibility with*) a preexisting `CAP` file if another `CAP` file converted using the `export` file of the preexisting `CAP` file can link with the new `CAP` file without errors.

FIGURE 4-4 shows an example of binary compatible `CAP` files, `p1` and `p1'`. The preconditions for the example are: the package `p1` is converted to create the `p1 CAP` file and `p1 export` file, and package `p1` is modified and converted to create the `p1' CAP` file. Package `p2` imports package `p1`, and therefore when the `p2 CAP` file is

created the `export` file of `p1` is used. In the example, `p2` is converted using the original `p1` `export` file. Because `p1'` is binary compatible with `p1`, `p2` may be linked with either the `p1` `CAP` file or the `p1'` `CAP` file.

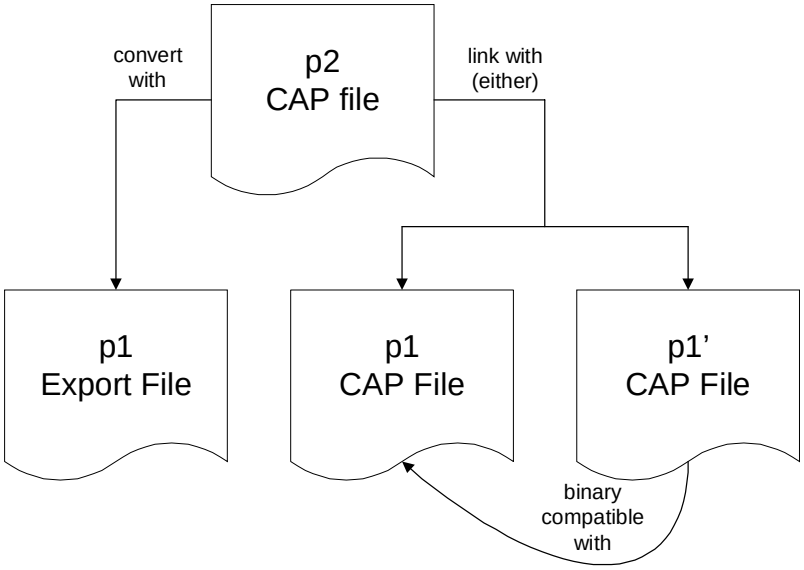


FIGURE 4-4 Binary compatibility example

Any modification that causes binary incompatibility in the Java programming language also causes binary incompatibility in Java Card systems. These modifications are described as causing a potential error in *The Java™ Language Specification*. Any modification that does not cause binary incompatibility in the Java programming language does not cause binary incompatibility in a Java Card system, except under the following conditions:

- the value of a token assigned to an element in the API of a package is changed;
- the value of an externally visible `final` `static` field (compile-time constant) is changed;
- an externally visible virtual method that does not override a preexisting method is added to a non-`final` `public` class.

Tokens are used to resolve references to imported elements of a package. If a token value is modified, a linker on a device is unable to associate the new token value with the previous token value of the element, and therefore is unable to resolve the reference correctly.

Compile-time constants are not stored as fields in `CAP` files. Instead their values are recorded in `export` files and placed inline in the bytecodes in `CAP` files. These values are said to be pre-linked in a `CAP` file of a package that imports those constants.

During execution, information is not available to determine whether the value of an inlined constant is the same as the value defined by the binary of the imported package.

As described above, tokens assigned to `public` and `protected` virtual methods are scoped to the hierarchy of a class. Tokens assigned to `public` and `protected` virtual methods introduced in a subclass have values starting at one greater than the maximum token value assigned in a superclass. If a new, non-override, `public` or `protected` virtual method is introduced in a superclass it is assigned a token value that would otherwise have been assigned in a subclass. Therefore, two unique virtual methods could be assigned the same token value within the same class hierarchy, making resolution of a reference to one of the methods ambiguous.

4.5 Package Versions

Each implementation of a package in a Java Card system is assigned a pair of major and minor version numbers. These version numbers are used to indicate binary compatibility or incompatibility between successive implementations of a package.

4.5.1 Assigning

The major and minor versions of a package are assigned by the package provider. It is recommended that the initial implementation of a package be assigned a major version of 1 and a minor version of 0. However, any values may be chosen. It is also recommended that when either a major or a minor version is incremented, it is incremented exactly by 1.

A major version must be changed when a new implementation of a package is not binary compatible with the previous implementation. The value of the new major version must be greater than the major version of the previous implementation. When a major version is changed, the associated minor version must be assigned the value of 0.

When a new implementation of a package is binary compatible with the previous implementation, it must be assigned a major version equal to the major version of the previous implementation. The minor version assigned to the new implementation must be greater than the minor version of the previous implementation.

4.5.2 Linking

Both an `export` file and a `CAP` file contain the major and minor version numbers of the package described. When a `CAP` file is installed on a Java Card enabled device a *resident image* of the package is created, and the major and minor version numbers are recorded as part of that image. When an `export` file is used during preparation of a `CAP` file, the version numbers indicated in the `export` file are recorded in the `CAP` file.

During installation, references from the package of the `CAP` file being installed to an imported package can be resolved only when the version numbers indicated in the `export` file used during preparation of the `CAP` file are compatible with the version numbers of the resident image. They are compatible when the major version numbers are equal and the minor version of the `export` file is less than or equal to the minor version of the resident image.

Appendix JCVM01

CHAPTER 5

The `Export` File Format

This chapter describes the Java Card virtual machine `export` file format. Compliant Java Card Converters must be capable of producing and consuming all `export` files that conform to the specification provided in this chapter. (Refer to Chapter 4, "Binary Representation.")

An `export` file consists of a stream of 8-bit bytes. All 16-bit and 32-bit quantities are constructed by reading in two and four consecutive 8-bit bytes, respectively. Multibyte data items are always stored in big-endian order, where the high-order bytes come first.

This chapter defines its own set of data types representing Java Card `export` file data: The types `u1`, `u2`, and `u4` represent an unsigned one-, two-, and four-byte quantities, respectively.

The Java Card `export` file format is presented using pseudo structures written in a C-like structure notation. To avoid confusion with the fields of Java Card virtual machine classes and class instances, the contents of the structures describing the Java Card `export` file format are referred to as *items*. Unlike the fields of a C structure, successive items are stored in the Java Card file sequentially, without padding or alignment.

Variable-sized *tables*, consisting of variable-sized items, are used in several `export` file structures. Although we will use C-like array syntax to refer to table items, the fact that tables are streams of varying-sized structures means that it is not possible to directly translate a table index into a byte offset into the table.

In a data structure that is referred to as an *array*, the elements are equal in size.

5.1 `Export` File Name

As described in §4.1.1, the name of a `export` file must be the last portion of the package specification followed by the extension '`.exp`'. For example, the name of the `export` file of the `javacard.framework` package must be `framework.exp`. Operating systems that impose limitations on file name lengths may transform an `export` file's name according to its conventions.

5.2 Containment in a Jar File

As described in §4.1.3, Java Card `CAP` files are contained in a JAR file. If an `export` file is also stored in a JAR file, it must also be located in a directory called `javacard` that is a subdirectory package's directory. For example, the `framework.exp` file would be located in the subdirectory `javacard/framework/javacard`.

5.3 `Export` File

An `export` file is defined by the following structure:

```
ExportFile {
       u4 magic
       u1 minor_version
       u1 major_version
       u2 constant_pool_count
       cp_info constant_pool[constant_pool_count]
       u2 this_package
       u1 export_class_count
       class_info classes[export_class_count]
}
```

The items in the `ExportFile` structure are as follows:

`magic`

The `magic` item contains the magic number identifying the `ExportFile` format; it has the value 0x00FACADE.

`minor_version, major_version`

The `minor_version` and `major_version` items are the minor and major version numbers of this `export` file. An implementation of a Java Card virtual machine supports `export` files having a given major version number and minor version numbers in the range 0 through some particular `minor_version`.

If a Java Card virtual machine encounters an `export` file with the supported major version but an unsupported minor version, the Java Card virtual machine must not attempt to interpret the content of the `export` file. However, it will be feasible to upgrade a Java Card virtual machine to support the newer minor version.

A Java Card virtual machine must not attempt to interpret a `export` file with a different major version. A change of the major version number indicates a major incompatibility change, one that requires a fundamentally different Java Card virtual machine.

In this specification, the major version of the `export` file has the value 2 and the minor version has the value 1. Only Sun Microsystems, Inc. may define the meaning and values of new `export` file versions.

`constant_pool_count`

The `constant_pool_count` item is a non-zero, positive value that indicates the number of constants in the constant pool.

`constant_pool[]`

The `constant_pool` is a table of variable-length structures representing various string constants, class names, field names and other constants referred to within the `ExportFile` structure.

Each of the `constant_pool` table entries, including entry zero, is a variable-length structure whose format is indicated by its first “tag” byte.

There are no ordering constrains on entries in the `constant_pool` table.

`this_package`

The value of `this_package` must be a valid index into the `constant_pool` table. The `constant_pool` entry at that index must be a `CONSTANT_Package_info` (§5.4.1) structure representing the package defined by this `ExportFile`.

`export_class_count`

The value of the `export_class_count` item gives the number of elements in the `classes` table.

`classes[]`

Each value of the `classes` table is a variable-length `class_info` structure (§5.5) giving the description of a publicly accessible class or interface declared in this package. If the `ACC_LIBRARY` flag item in the `CONSTANT_Package_info` (§5.4.1) structure indicated by the `this_package` item is set, the `classes` table has an entry for each `public` class and interface declared in this package. If the `ACC_LIBRARY` flag item is not set, the `classes` table has an entry for each shareable interface declared in this package.[1]

5.4 Constant Pool

All `constant_pool` table entries have the following general format:

```
cp_info {
       u1 tag
       u1 info[]
}
```

Each item in the `constant_pool` must begin with a 1-byte `tag` indicating the kind of `cp_info` entry. The content of the `info` array varies with the value of `tag`. The valid tags and their values are listed in TABLE 5-1. Each tag byte must be followed by two or more bytes giving information about the specific constant. The format of the additional information varies with the tag value.

Constant Type	Value
`CONSTANT_Package`	13
`CONSTANT_Interfaceref`	7
`CONSTANT_Integer`	3
`CONSTANT_Utf8`	1

TABLE 5-1 Export file constant pool tags

1. This restriction of exporting only shareable interfaces in non-library packages is imposed by the firewall defined in the Java Card™ Runtime Environment (JCRE) 2.1 Specification.

5.4.1 CONSTANT_Package

The `CONSTANT_Package_info` structure is used to represent a package:

```
CONSTANT_Package_info {
       u1 tag
       u1 flags
       u2 name_index
       u1 minor_version
       u1 major_version
       u1 aid_length
       u1 aid[aid_length]
}
```

The items of the `CONSTANT_Package_info` structure are the following:

`tag`

The `tag` item has the value of `CONSTANT_Package` (13).

`flags`

The `flags` item is a mask of modifiers that apply to this package. The `flags` modifiers are shown in the following table.

Flags	Value
ACC_LIBRARY	0x01

TABLE 5-2 Export file package flags

The `ACC_LIBRARY` flag has the value of one if this package does not define and declare any applets. In this case it is called a *library package*. Otherwise `ACC_LIBRARY` has the value of zero.

If the package is not a library package this `export` file can only contain shareable interfaces.[1] A shareable interface is either the `javacard.framework.Shareable` interface or an interface that extends the `javacard.framework.Shareable` interface.

All other flag values are reserved by the Java Card virtual machine. Their values must be zero.

1. This restriction is imposed by the firewall defined in the Java Card™ Runtime Environment (JCRE) 2.1 Specification.

`name_index`

The value of the `name_index` item must be a valid index into the `constant_pool` table. The `constant_pool` entry at that index must be a `CONSTANT_Utf8_info` (§5.4.4) structure representing a valid Java package name.

As in Java class files, ASCII periods (‘.’) that normally separate the identifiers in a package name are replaced by ASCII forward slashes (‘/’). For example, the package name `javacard.framework` is represented in a `CONSTANT_Utf8_info` structure as `javacard/framework`.

`minor_version, major_version`

The `minor_version` and `major_version` items are the minor and major version numbers of this package. These values uniquely identify the particular implementation of this package and indicate the binary compatibility between packages. See §4.5 for a description of assigining and using package version numbers.

`aid_length`

The value of the `aid_length` item gives the number of bytes in the `aid` array. Valid values are between 5 and 16, inclusive.

`aid[]`

The `aid` array contains the ISO AID of this package (§4.2).

5.4.2 CONSTANT_Interfaceref

The `CONSTANT_Interfaceref_info` structure is used to represent an interface:

```
CONSTANT_Interfaceref_info {
       u1 tag
       u2 name_index
}
```

The items of the `CONSTANT_Interfaceref_info` structure are the following:

`tag`

The `tag` item has the value of `CONSTANT_Interface` (7).

`name_index`

The value of the `name_index` item must be a valid index into the `constant_pool` table. The `constant_pool` entry at that index must be a `CONSTANT_Utf8_info` (§5.4.4) structure representing a valid fully qualified Java interface name. These names are fully qualified because they may be defined in a package other than the one described in the `export` file.

As in Java class files, ASCII periods (‘.’) that normally separate the identifiers in a class or interface name are replaced by ASCII forward slashes (‘/’). For example, the interface name `javacard.framework.Shareable` is represented in a `CONSTANT_Utf8_info` structure as `javacard/framework/Shareable`.

5.4.3 CONSTANT_Integer

The `CONSTANT_Integer_info` structure is used to represent four-byte numeric (int) constants:

```
CONSTANT_Integer_info {
       u1 tag
       u4 bytes
}
```

The items of the CONSTANT_Integer_info structure are the following:

`tag`

The `tag` item has the value of `CONSTANT_Integer` (3).

`bytes`

The `bytes` item of the `CONSTANT_Integer_info` structure contains the value of the `int` constant. The bytes of the value are stored in big-endian (high byte first) order.

5.4.4 CONSTANT_Utf8

The `CONSTANT_Utf8_info` structure is used to represent constant string values. UTF-8 strings are encoded in the same way as described in *The Java™ Virtual Machine Specification* (§ 4.4.7).

The `CONSTANT_Utf8_info` structure is:

```
CONSTANT_Utf8_info {
       u1 tag
       u2 length
       u1 bytes[length]
}
```

The items of the `CONSTANT_Utf8_info` structure are the following:

`tag`

The `tag` item has the value of `CONSTANT_Utf8` (1).

`length`

The value of the `length` item gives the number of bytes in the `bytes` array (not the length of the resulting string). The strings in the `CONSTANT_Utf8_info` structure are not null-terminated.

`bytes[]`

The `bytes` array contains the bytes of the string. No byte may have the value `(byte)0` or `(byte)0xF0-(byte)0xFF`.

5.5 Classes and Interfaces

Each class and interface is described by a variable-length `class_info` structure. The format of this structure is:

```
class_info {
       u1 token
       u2 access_flags
       u2 name_index
       u2 export_interfaces_count
       u2 interfaces[export_interfaces_count]
       u2 export_fields_count
       field_info fields[export_fields_count]
       u2 export_methods_count
       method_info methods[export_methods_count]
}
```

The items of the `class_info` structure are as follows:

`token`

The value of the `token` item is the class token (§4.3.7.2) assigned to this class or interface.

`access_flags`

The value of the `access_flags` item is a mask of modifiers used with class and interface declarations. The `access_flags` modifiers are shown in the fol-

lowing table.

Name	Value	Meaning	Used By
ACC_PUBLIC	0x0001	Is public; may be accessed from outside its package	Class, interface
ACC_FINAL	0x0010	Is final; no subclasses allowed.	Class
ACC_INTERFACE	0x0200	Is an interface	Interface
ACC_ABSTRACT	0x0400	Is abstract; may not be instantiated	Class, interface
ACC_SHAREABLE	0x0800	Is shareable, may be shared between Java Card applets.	Class, interface

TABLE 5-3 Export file class access and modifier flags

The ACC_SHAREABLE flag indicates whether this class or interface is shareable.[1] A class is shareable if it implements (directly or indirectly) the `javacard.framework.shareable` interface. An interface is shareable if it is or implements (directly or indirectly) the `javacard.framework.Shareable` interface.

All other class access and modifier flags are defined in the same way and with the same restrictions as described in *The Java™ Virtual Machine Specification*.

The Java Card virtual machine reserves all other flag values. Their values must be zero.

`name_index`

The value of the `name_index` item must be a valid index into the `constant_pool` table. The `constant_pool` entry at that index must be a `CONSTANT_Utf8_info (§5.4.4)` structure representing a valid Java class name stored as a simple (not fully qualified) name, that is, as a Java identifier.[2]

`export_interfaces_count`

The value of the `export_interface_count` item indicates the number of entries in the `interfaces` array.

1. The ACC_SHAREABLE flag is defined to enable Java Card virtual machines to implement the firewall restrictions defined by the *Java Card™ 2.1 Runtime Environment (JCRE) Specification.*

2. In Java class files class names are fully qualified. In Java Card `export` files all classes and interfaces enumerated are defined in the package of the `export` file making it unnecessary for class names to be fully qualified.

`interfaces[]`

The `interfaces` array contains an entry for each public interface implemented by this class or interface. It does not include package visible interfaces. It does include all public superinterfaces in the hierarchy of public interfaces implemented by this class or interface.

Each value in the `interfaces` array must be a valid index into the `constant_pool` table. The `constant_pool` entry at each value of `interfaces[i]`, where 0 <= i < `export_interfaces_count`, must be a `CONSTANT_Interfaceref_info` structure representing an interface which is an public superinterface of this class or interface type, in the left-to-right order given in the source for the type and its superclasses or superinterfaces.

`export_fields_count`

The value of the `export_fields_count` item gives the number of entries in the `fields` table.

`fields[]`

Each value in the `fields` table is a variable-length `field_info` (§5.6) structure. The `field_info` contains an entry for each publicly accessible field, both class variables and instance variables, declared by this class or interface. It does not include items representing fields that are inherited from superclasses or superinterfaces.

`export_methods_count`

The value of the `export_methods_count` item gives the number of entries in the `methods` table.

`methods[]`

Each value in the `methods` table is a `method_info` (§5.7) structure. The `method_info` structure contains an entry for each publicly accessible class (static or constructor) method defined by this class, and each publicly accessible instance method defined by this class or its superclasses, or defined by this interface or its super-interfaces.

5.6 Fields

Each field is described by a variable-length `field_info` structure. The format of this structure is:

```
field_info {
       u1 token
       u2 access_flags
       u2 name_index
       u2 descriptor_index
       u2 attributes_count
       attribute_info attributes[attributes_count]
}
```

The items of the `field_info` structure are as follows:

`token`

The `token` item is the token assigned to this field. There are three scopes for field tokens: `final static` fields of primitive types (compile-time constants), all other `static` fields, and instance fields.

If this field is a compile-time constant, the value of the `token` item is 0xFFFF. Compile-time constants are represented in `export` files, but are not assigned token values suitable for late binding. Instead Java Card Converters must replace bytecodes that reference `final static` fields with bytecodes that load the constant value of the field.[1]

If this field is `static`, but is not a compile-time constant, the token item represents a static field token (§4.3.7.3).

If this field is an instance field, the token item represents an instance field token (§4.3.7.5).

1. Although Java compilers ordinarily replace references to final static fields of primitive types with primitive constants, this functionality is not required.

`access_flags`

The value of the `access_flags` item is a mask of modifiers used with fields. The `access_flags` modifiers are shown in the following table.

Name	Value	Meaning	Used By
`ACC_PUBLIC`	`0x0001`	Is public; may be accessed from outside its package.	Any field
`ACC_PROTECTED`	`0x0004`	Is protected; may be accessed within subclasses.	Class field
`ACC_STATIC`	`0x0008`	Is static.	Class field
`ACC_FINAL`	`0x0010`	Is final; no further overriding or assignment after initialization.	Any field

TABLE 5-4 Export file field access and modifier flags

Field access and modifier flags are defined in the same way and with the same restrictions as described in *The Java™ Virtual Machine Specification*.

The Java Card virtual machine reserves all other flag values. Their values must be zero.

`name_index`

The value of the `name_index` item must be a valid index into the `constant_pool` table. The `constant_pool` entry at that index must be a `CONSTANT_Utf8_info` (§5.4.4) structure representing a valid Java field name stored as a simple (not fully qualified) name, that is, as a Java identifier.

`descriptor_index`

The value of the `descriptor_index` item must be a valid index into the `constant_pool` table. The `constant_pool` entry at that index must be a `CONSTANT_Utf8_info` (§5.4.4) structure representing a valid Java field descriptor.

Representation of a field descriptor in an `export` file is the same as in a Java `class` file. See the specification described in *The Java™ Virtual Machine Specification (*§ 4.3.2).

`attributes_count`

The value of the `attributes_count` item indicates the number of additional attributes of this field. The only `field_info` attribute currently defined is the `ConstantValue` attribute (§5.8.1). For `static final` fields of primitive types, the value must be 1; that is, when both the `ACC_STATIC` and `ACC_FINAL` bits in the flags item are set an attribute must be present. For all other fields the value

of the `attributes_count` item must be 0.

`attributes[]`

The only attribute defined for the `attributes` table of a `field_info` structure by this specification is the `ConstantValue` attribute (§5.8.1). This must be defined for `static final` fields of primitives (`boolean`, `byte`, `short`, and `int`).

5.7 Methods

Each method is described by a variable-length `method_info` structure. The format of this structure is:

```
method_info {
       u1 token
       u2 access_flags
       u2 name_index
       u2 descriptor_index
}
```

The items of the `method_info` structure are as follows:

`token`

The `token` item is the token assigned to this method. If this method is a static method or constructor, the `token` item represents a static method token (§4.3.7.4). If this method is a virtual method, the `token` item represents a virtual method token (§4.3.7.6).

`access_flags`

The value of the `access_flags` item is a mask of modifiers used with methods. The `access_flags` modifiers are shown in the following table.

Name	Value	Meaning	Used By
ACC_PUBLIC	0x0001	Is public; may be accessed from outside its package.	Any method
ACC_PROTECTED	0x0004	Is protected; may be accessed within subclasses.	Class/ instance method
ACC_STATIC	0x0008	Is static.	Class/ instance method
ACC_FINAL	0x0010	Is final; no further overriding or assignment after initialization.	Class/ instance method
ACC_ABSTRACT	0x0400	Is abstract; no implementation is provided	Any method

TABLE 5-5 Export file method access and modifier flags

Method access and modifier flags are defined in the same way and with the same restrictions as described in *The Java™ Virtual Machine Specification.*

Unlike in Java class files, the `ACC_NATIVE` flag is not supported in `export` files. Whether a method is native is an implementation detail that is not relevant to importing packages. The Java Card virtual machine reserves all other flag values. Their values must be zero.

`name_index`

The value of the `name_index` item must be a valid index into the `constant_pool` table. The `constant_pool` entry at that index must be a `CONSTANT_Utf8_info` (§5.4.4) structure representing either the special internal method name for constructors, `<init>`, or a valid Java method name stored as a simple (not fully qualified) name.

`descriptor_index`

The value of the `descriptor_index` item must be a valid index into the `constant_pool` table. The `constant_pool` entry at that index must be a `CONSTANT_Utf8_info` (§5.4.4) structure representing a valid Java method descriptor.

Representation of a method descriptor in an `export` file is the same as in a Java class file. See the specification described in *The Java™ Virtual Machine Specification* (§ 4.3.3).

5.8 Attributes

Attributes are used in the `field_info` (§5.6) structure of the `export` file format. All attributes have the following general format:

```
attribute_info {
       u2 attribute_name_index
       u4 attribute_length
       u1 info[attribute_length]
}
```

5.8.1 ConstantValue Attribute

The `ConstantValue` attribute is a fixed-length attribute used in the `attributes` table of the `field_info` structures. A `ConstantValue` attribute represents the value of a `final static` field (compile-time constant); that is, both the `ACC_STATIC` and `ACC_FINAL` bits in the `flags` item of the `field_info` structure must be set. There can be no more than one `ConstantValue` attribute in the `attributes` table of a given `field_info` structure.

The `ConstantValue` attribute has the format:

```
ConstantValue_attribute {
       u2 attribute_name_index
       u4 attribute_length
       u2 constantvalue_index
}
```

The items of the `ConstantValue_attribute` structure are as follows:

`attribute_name_index`

The value of the `attribute_name_index` item must be a valid index into the `constant_pool` table. The `constant_pool` entry at that index must be a `CONSTANT_Utf8_info` (§5.4.4) structure representing the string “ConstantValue.”

`attribute_length`

The value of the `attribute_length` item of a `ConstantValue_attribute` structure must be 2.

`constantvalue_index`

The value of the `constantvalue_index` item must be a valid index into the

`constant_pool` table. The `constant_pool` entry at that index must give the constant value represented by this attribute.

The `constant_pool` entry must be of a type `CONSTANT_Integer` (§5.4.3).

CHAPTER 6

The CAP File Format

This chapter describes the Java Card CAP (converted applet) file format. Each CAP file contains all of the classes and interfaces defined in one Java package. Java Card Converters must be capable of producing CAP files that conform to the specification provided in this chapter.

A CAP file consists of a stream of 8-bit bytes. All 16-bit and 32-bit quantities are constructed by reading in two and four consecutive 8-bit bytes, respectively. Multibyte data items are always stored in big-endian order, where the high-order bytes come first. The first bit read of an 8-bit quantity is considered the *high bit*.

This chapter defines its own set of data types representing Java Card CAP file data: The types u1, and u2 represent an unsigned one-, and two-byte quantities, respectively. Some u1 types are represented as *bitfield* structures, consisting of arrays of bits. The zeroeth bit in each bit array represents the most significant bit, or *high bit*.

The Java Card CAP file format is presented using pseudo structures written in a C-like structure notation. To avoid confusion with the fields of Java Card virtual machine classes and class instances, the contents of the structures describing the Java Card CAP file format are referred to as *items*. Unlike the fields of a C structure, successive items are stored in the Java Card file sequentially, without padding or alignment.

Variable-sized *tables*, consisting of variable-sized items, are used in several CAP file data structures. Although we will use C-like array syntax to refer to table items, the fact that tables are streams of variable-sized structures means that it is not possible to directly translate a table index into a byte offset into the table.

A data structure referred to as an *array* consists of items equal in size.

Some items in the structures of the CAP file format are describe using a C-like *union* notation. The bytes contained in a union structure have one of the two formats. Selection of the two formats is based on the value of the high bit of the structure.

6.1 Component Model

A Java Card CAP file consists of a set of components. Each component describes a set of elements in the Java package defined, or an aspect of the CAP file. A complete CAP file must contain all of the required components specified in this chapter. Two components are optional: the Applet Component (§6.5) and Export Component (§6.12). The Applet Component is included only if one or more Applets are defined in the package. The Export Component is included only if classes in other packages may import elements in the package defined.

The content of each component defined in a CAP file must conform to the corresponding format specified in this chapter. All components have the following general format:

```
component {
        u1 tag
        u2 size
        u1 info[]
}
```

Each component begins with a 1-byte `tag` indicating the kind of component. Valid tags and their values are listed in TABLE 6-1. The `size` item indicates the number of bytes in the info array of the component, not including the `tag` and `size` items.

The content and format of the `info` array varies with the type of component.

Component Type	Value
COMPONENT_Header	1
COMPONENT_Directory	2
COMPONENT_Applet	3
COMPONENT_Import	4
COMPONENT_ConstantPool	5
COMPONENT_Class	6
COMPONENT_Method	7
COMPONENT_StaticField	8
COMPONENT_ReferenceLocation	9
COMPONENT_Export	10
COMPONENT_Descriptor	11

TABLE 6-1 CAP file component tags

Sun may define additional components in future versions of this Java Card vitural machine specification. It is guaranteed that additional components will have tag values between 12 and 127, inclusive.

6.1.1 Containment in a JAR File

All CAP file components are stored in individual files contained in a JAR File. The component file names are enumerated in TABLE 6-2. These names are not case sensitive.

Component Type	File Name
COMPONENT_Header	Header.cap
COMPONENT_Directory	Directory.cap
COMPONENT_Applet	Applet.cap
COMPONENT_Import	Import.cap
COMPONENT_ConstantPool	ConstantPool.cap
COMPONENT_Class	Class.cap
COMPONENT_Method	Method.cap
COMPONENT_StaticField	StaticField.cap
COMPONENT_ReferenceLocation	RefLocation.cap
COMPONENT_Export	Export.cap
COMPONENT_Descriptor	Descriptor.cap

TABLE 6-2 CAP file component file names

As described in §4.1.3, the path to the CAP file component files in a JAR file consists of a directory called javacard that is in a subdirectory representing the package's directory. For example, the CAP file component files of the package javacard.framework are located in the subdirectory javacard/framework/javacard.

The name of a JAR file containing CAP file component files is not defined as part of this specification. Other files, including other CAP files, may also reside in a JAR file that contains CAP file component files.

6.1.2 Defining New Components

Java Card CAP files are permitted to contain new, or custom, components. All new components not defined as part of this specification must not affect the semantics of the specified components, and Java Card virtual machines must be able to accept CAP files that do not contain new components. Java Card virtual machine implementations are required to silently ignore components they do not recognize.

New components are identified in two ways: they are assigned both an ISO 7816-5 AID (§4.2) and a tag value. Valid tag values are between 128 and 255, inclusive. Both of these identifiers are recorded in the custom_component item of the Directory Component (§6.4).

The new component must conform to the general component format defined in this chapter, with a `tag` value, a `size` value indicating the number of bytes in the component (excluding the `tag` and `size` items), and an `info` item containing the content of the new component.

A new component file is stored in a JAR file, following the same restrictions as those specified in §4.1.3. That is, the file containing the new component must be located in the `<package_directory>/javacard` subdirectory of the JAR file and must have the extension '`.cap`'.

6.2 Installation

Installing a CAP file onto a Java Card enabled device entails communication between a Java Card enabled terminal and that device. While it is beyond the scope of this specification to define an installation protocol between a terminal and a device, the CAP file component order shown in TABLE 6-3 is a reference load order suitable for an implementation with a simple memory management model on a limited memory device.

Component Type
COMPONENT_Header
COMPONENT_Directory
COMPONENT_Import
COMPONENT_Applet
COMPONENT_Class
COMPONENT_Method
COMPONENT_StaticField
COMPONENT_Export
COMPONENT_ConstantPool
COMPONENT_ReferenceLocation
COMPONENT_Descriptor (optional)

TABLE 6-3 Reference component install order

6.3 Header Component

The Header Component contains general information about this CAP file and the package it defines. It is described by the following variable-length structure:

```
header_component {
       u1 tag
       u2 size
       u4 magic
       u1 minor_version
       u1 major_version
       u1 flags
       package_info this_package
}
```

The items in the header_component structure are as follows:

tag

The tag item has the value COMPONENT_Header (1).

size

The size item indicates the number of bytes in the header_component structure, excluding the tag and size items. The value of the size item must be greater than zero.

magic

The magic item supplies the magic number identifying the Java Card CAP file format; it has the value 0xDECAFFED.

minor_version, major_version

The minor_version and major_version items are the minor and major version numbers of this CAP file. An implementation of a Java Card virtual machine must support CAP files having a specific major version number and minor version numbers in the range of 0 through some particular minor_version.

If a Java Card virtual machine encounters a CAP file with the supported major version but an unsupported minor version, the Java Card virtual machine must not attempt to interpret the content of the CAP file. However, it will be feasible to upgrade a Java Card virtual machine to support the newer minor version.

A Java Card virtual machine must not attempt to interpret a CAP file with a different major version. A change of the major version number indicates a major incompatibility change, one that requires a fundamentally different Java Card

virtual machine.

In this specification, the major version of the CAP file has the value 2 and the minor version has the value 1. Only Sun Microsystems, Inc. may define the meaning and values of new CAP file versions.

flags

The flags item is a mask of modifiers that apply to this package. The flags modifiers are shown in the following table.

Flags	Value
ACC_INT	0x01
ACC_EXPORT	0x02
ACC_APPLET	0x04

TABLE 6-4 CAP file package flags

The ACC_INT flag has the value of one if the Java int type is used in this package. The int type is used if one or more of the following is present:

- a parameter to a method of type int,
- a local variable of type int,
- a field of type int,
- a field of type int array, or
- an instruction of type int.

Otherwise the ACC_INT flag has the value of 0.

The ACC_EXPORT flag has the value of one if an Export Component (§6.12) is included in this CAP file. Otherwise it has the value of 0.

The ACC_APPLET flag has the value of one if an Applet Component (§6.5) is included in this CAP file. Otherwise it has the value of 0.

All other bits in the flags item not defined in TABLE 6-4 are reserved for future use. Their values must be zero and they must be ignored by Java Card virtual machines.

this_package

The this_package item describes the package defined in this CAP file. It is represented as a package_info structure:

```
package_info {
       u1 minor_version
       u1 major_version
       u1 AID_length
       u1 AID[AID_length]
}
```

The items in the package_info structure are as follows:

minor_version, major_version
: The minor_version and major_version items are the minor and major version numbers of this package. These values uniquely identify the particular implementation of this package and indicate the binary compatibility between packages. See §4.5 for a description of assigining and using package version numbers.

AID_length
: The AID_length item represents the number of bytes in the AID item. Valid values are between 5 and 16, inclusive.

AID[]
: The AID item represents the Java Card name of the package. See ISO 7816-5 for the definition of an AID (§4.2).

6.4 Directory Component

The Directory Component lists the size of each of the components defined in this CAP file. When an optional component is not included, such as the Applet Component (§6.5) or Export Component (§6.12), it is represented in the Directory Component with size equal to zero. The Directory Component also includes entries for new (or custom) components.

The Directory Component is described by the following variable-length structure:

```
directory_component {
        u1 tag
        u2 size
        u2 component_sizes[11]
        static_field_size_info static_field_size
        u1 import_count
        u1 applet_count
        u1 custom_count
        custom_component_info custom_components[custom_count]
}
```

The items in the directory_component structure are as follows:

tag
: The tag item has the value COMPONENT_Directory (2).

`size`

The `size` item indicates the number of bytes in the `directory_component` structure, excluding the `tag` and `size` items. The value of the `size` item must be greater than zero.

`component_sizes[]`

The `component_sizes` item is an array representing the number of bytes in each of the components in this `CAP` file. All of the 11 components defined in this chapter are represented in the `component_sizes` array. The value of an index into the array is equal to the value of the tag of the component represented at that entry, minus 1.

The value in each entry in the `component_sizes` array is that same as the `size` item in the corresponding component. It represents the number of bytes in the component, excluding the `tag` and `size` items.

The value of an entry in the `component_sizes` array is zero for components not included in this `CAP` file. Components that may not be included are the Applet Component (§6.5) and the Export Component (§6.12). For all other components the value is greater than zero.

`static_field_size`

The `static_field_size` item is a `static_field_size_info` structure. The structure is defined as:

```
static_field_size_info {
       u2 image_size
       u2 array_init_count
       u2 array_init_size
}
```

The items in the `static_field_size_info` structure are the following:

`image_size`

The `image_size` item has the same value as the `image_size` item in the Static Field Component (§6.10). It represents the total number of bytes in the `static` fields defined in this package, excluding `final static` fields of primitive types.

`array_init_count`

The `array_init_count` item has the same value as the `array_init_count` item in the Static Field Component (§6.10). It represents the number of arrays initialized in all of the `<clinit>` methods in this package.

`array_init_size`

The `array_init_size` item represents the sum of the `count` items in

the array_init table item of the Static Field Component (§6.10). It is the total number of bytes in all of the arrays initialized in all of the <clinit> methods in this package.

import_count

The import_count item indicates the number of packages imported by classes and interfaces in this package. This item has the same value as the count item in the Import Component (§6.6).

applet_count

The applet_count item indicates the number of applets defined in this package. If an Applet Component (§6.5) is not included in this CAP file, the value of the applet_count item is zero. Otherwise the value of the applet_count item is the same as the value of the count item in the Applet Component (§6.5).

custom_count

The custom_count item indicates the number of entries in the custom_components table. Valid values are between 0 and 127, inclusive.

custom_components[]

The custom_components item is a table of variable-length custom_component_info structures. Each new component defined in this CAP file must be represented in the table. These components are not defined in this standard.

The custom_component_info structure is defined as:

```
custom_component_info {
       u1 component_tag
       u1 size
       u1 AID_length
       u1 AID[AID_length]
}
```

The items in entries of the custom_component_info structure are:

component_tag

The component_tag item represents the tag of the component. Valid values are between 128 and 255, inclusive.

size

The size item represents the number of bytes in the component, excluding the tag and size items.

AID_length

The AID_length item represents the number of bytes in the AID item.

Valid values are between 5 and 16, inclusive.

`AID[]`

The `AID` item represents the Java Card name of the component. See ISO 7816-5 for the definition of an AID (§4.2).

Each component is assigned an AID conforming to the ISO 7816-5 standard. The RID (first 5 bytes) of all of the custom component AIDs must have the same value. In addition, the RID of the custom component AIDs must have the same value as the RID of the package defined in this `CAP` file.

6.5 Applet Component

The Applet Component contains an entry for each of the applets defined in this package. Applets are defined by implementing a non-abstract subclass, direct or indirect, of the `javacard.framework.Applet` class.[1] If no applets are defined, this component must not be present in this `CAP` file.

The Applet Component is described by the following variable-length structure:

```
applet_component {
       u1 tag
       u2 size
       u1 count
       { u1 AID_length
         u1 AID[AID_length]
         u2 install_method_offset
       } applets[count]
}
```

The items in the `applet_component` structure are as follows:

`tag`

The `tag` item has the value `COMPONENT_Applet` (3).

`size`

The `size` item indicates the number of bytes in the `applet_component` structure, excluding the `tag` and `size` items. The value of the `size` item must be greater than zero.

1. Restrictions placed on an applet definition are imposed by the Java Card Runtime Environment (JCRE) 2.1 specification.

`count`

The `count` item indicates the number of applets defined in this package.

`applets[]`

The `applets` item represents a table of variable-length structures each describing an applet defined in this package.

The items in each entry of the `applets` table are defined as follows:

`AID_length`

The `AID_length` item represents the number of bytes in the `AID` item. Valid values are between 5 and 16, inclusive.

`AID[]`

The `AID` item represents the Java Card name of the applet.

Each applet is assigned an AID conforming to the ISO 7816-5 standard (§4.2). The RID (first 5 bytes) of all of the applet AIDs must have the same value. In addition, the RID of each applet AIDs must have the same value as the RID of the package defined in this `CAP` file.

`install_method_offset`

The value of the `install_method_offset` item must be a 16-bit offset into the `info` item of the Method Component (§6.9). The item at that offset must be a `method_info` structure that represents the static `install(byte[],short,byte)` method of the applet.[1] The `install(byte[],short,byte)` method must be defined in a class that extends the `javacard.framework.applet` class, directly or indirectly. The `install(byte[],short,byte)` method is called to initialize the applet.

1. Restrictions placed on the `install(byte[],short,byte)` method of an applet are imposed by the Java Card Runtime Environment (JCRE) 2.1 specification.

6.6 Import Component

The Import Component lists the set of packages imported by the classes in this package. It does not include an entry for the package defined in this CAP file. The Import Component is represented by the following structure:

```
import_component {
       u1 tag
       u2 size
       u1 count
       package_info packages[count]
}
```

The items in the import_component structure are as follows:

tag

The tag item has the value COMPONENT_Import (4).

size

The size item indicates the number of bytes in the import_component structure, excluding the tag and size items. The value of the size item must be greater than zero.

count

The count item indicates the number of items in the packages table. The value of the count item must be between 0 and 127, inclusive.

packages[]

The packages item represents a table of variable-length package_info structures as defined for this_package under §6.3. The table contains an entry for each of the packages referenced in the CAP file, not including the package defined.

The major and minor version numbers specified in the package_info structure are equal to the major and minor versions specified in the imported package's export file. See §4.5 for a description of assigining and using package version numbers.

Components of this CAP file refer to an imported package by using a index in this packages table. The index is called a *package token* (§4.3.7.1).

6.7 Constant Pool Component

The Constant Pool Component contains an entry for each of the classes, methods, and fields referenced by elements in the Method Component (§6.9) of this CAP file. The referencing elements in the Method Component may be instructions in the methods or exception handler catch types in the exception handler table.

Entries in the Constant Pool Component reference elements in the Class Component (§6.8), Method Component (§6.9), and Static Field Component (§6.10). The Import Component (§6.6) is also accessed using a package token (§4.3.7.1) to describe references to classes, methods and fields defined in imported packages. Entries in the Constant Pool Component do not reference other entries internal to itself.

The Constant Pool Component is described by the following structure:

```
constant_pool_component {
       u1 tag
       u2 size
       u2 count
       cp_info constant_pool[count]
}
```

The items in the `constant_pool_component` structure are as follows:

`tag`

The `tag` item has the value `COMPONENT_ConstantPool` (5).

`size`

The `size` item indicates the number of bytes in the `constant_pool_component` structure, excluding the `tag` and `size` items. The value of the `size` item must be greater than zero.

`count`

The `count` item represents the number entries in the `constant_pool` array. Valid values are between 0 and 65535, inclusive.

`constant_pool`

The `constant_pool` item represents an array of `cp_info` structures:

```
cp_info {
       u1 tag
       u1 info[3]
}
```

Each item in the `constant_pool` array is a 4-byte structure. Each structure

must begin with a 1-byte `tag` indicating the kind of `cp_info` entry. The content and format of the 3-byte `info` array varies with the value of the tag. The valid tags and their values are listed in the following table.

Constant Type	Tag
`CONSTANT_Classref`	1
`CONSTANT_InstanceFieldref`	2
`CONSTANT_VirtualMethodref`	3
`CONSTANT_SuperMethodref`	4
`CONSTANT_StaticFieldref`	5
`CONSTANT_StaticMethodref`	6

TABLE 6-5 CAP file constant pool tags

Java Card constant types are more specific than those in Java `class` files. The categories indicate not only the type of the item referenced, but also the manner in which it is referenced.

For example, in the Java constant pool there is one constant type for method references, while in the Java Card constant pool there are three constant types for method references: one for virtual method invocations using the *invokevirtual* bytecode, one for super method invocations using the *invokespecial* bytecode, and one for static method invocations using either the *invokestatic* or *invokespecial* bytecode.[1] The additional information provided by a constant type in Java Card technologies simplifies resolution of references.

There are no ordering constraints on constant pool entries. It is recommended, however, that `CONSTANT_InstanceFieldref` (§6.7.2) constants occur early in the array to permit using *getfield_T* and *putfield_T* bytecodes instead of *getfield_T_w* and *putfield_T_w* bytecodes. The former have 1-byte constant pool index parameters while the latter have 2-byte constant pool index parameters.

1. The constant pool index parameter of an *invokespecial* bytecode is to a `CONSTANT_StaticMethodref` when the method referenced is a constructor or a private virtual method. In these cases the method invoked is fully known when the `CAP` file is created. In the cases of virtual method and super method references, the method invoked is dependent upon an instance of a class and its hierarchy, both of which may be partially unknown when the `CAP` file is created.

6.7.1 CONSTANT_Classref

The `CONSTANT_Classref_info` structure is used to represent a reference to a class or an interface. The class or interface may be defined in this package or in an imported package.

```
CONSTANT_Classref_info {
       u1 tag
       union {
              u2 internal_class_ref
              { u1 package_token
                u1 class_token
              } external_class_ref
       } class_ref
       u1 padding
}
```

The items in the `CONSTANT_Classref_info` structure are the following:

`tag`

The `tag` item has the value `CONSTANT_Classref` (1).

`class_ref`

The `class_ref` item represents a reference to a class or interface. If the class or interface is defined in this package the structure represents an `internal_class_ref` and the high bit of the structure is zero. If the class or interface is defined in another package the structure represents an `external_class_ref` and the high bit of the structure is one.

`internal_class_ref`

The `internal_class_ref` structure represents a 16-bit offset into the `info` item of the Class Component (§6.8) to an `interface_info` or `class_info` structure. The `interface_info` or `class_info` structure must represent the referenced class or interface.

The value of the `internal_class_ref` item must between 0 and 32767, inclusive, making the high bit equal to zero.

`external_class_ref`

The `external_class_ref` structure represents a reference to a class or interface defined in an imported package. The high bit of this structure is one.

`package_token`

The `package_token` item represents a package token (§4.3.7.1) defined in the Import Component (§6.6) of this `CAP` file. The value of this token must be a valid index into the

`packages` table item of the `import_component` structure. The package represented at that index must be the imported package.

The value of the package token must be between 0 and 127, inclusive.

The high bit of the `package_token` item is equal to one.

`class_token`

The `class_token` item represents the token of the class or interface (§4.3.7.2) of the referenced class or interface. It has the value of the class token of the class as defined in the `Export` file of the imported package.

`padding`

The `padding` item has the value zero. It is present to make the size of a `CONSTANT_Classref_info` structure the same as all other constants in the `constant_pool` array.

6.7.2 CONSTANT_InstanceFieldref, CONSTANT_VirtualMethodref, and CONSTANT_SuperMethodref

References to instance fields, and virtual methods are represented by similar structures:

```
CONSTANT_InstanceFieldref_info {
       u1 tag
       class_ref class
       u1 token
}

CONSTANT_VirtualMethodref_info {
       u1 tag
       class_ref class
       u1 token
}

CONSTANT_SuperMethodref_info {
       u1 tag
       class_ref class
       u1 token
}
```

The items in these structures are as follows:

`tag`

The tag item of a `CONSTANT_InstanceFieldref_info` structure has the value `CONSTANT_InstanceFieldref` (2).

The tag item of a `CONSTANT_VirtualMethodref_info` structure has the value `CONSTANT_VirtualMethodref` (3).

The tag item of a `CONSTANT_SuperMethodref_info` structure has the value `CONSTANT_SuperMethodref` (4).

`class`

The `class` item represents the class associated with the referenced instance field, virtual method, or `super` method invocation. It is a `class_ref` structure (§6.7.1). If the referenced class is defined in this package the high bit is equal to zero. If the reference class is defined in an imported package the high bit of this structure is equal to one.

The class referenced in the `CONSTANT_InstanceField_info` structure must be the class that contains the declaration of the instance field.

The class referenced in the `CONSTANT_VirtualMethodref_info` structure must be a class that contains a declaration or definition of the virtual method.

The class referenced in the `CONSTANT_SuperMethodref_info` structure must always be internal to the class that defines the method that contains the Java language-level `super` invocation. The class must be defined in this package.

`token`

The `token` item in the `CONSTANT_InstanceFieldref_info` structure represents an instance field token (§4.3.7.5) of the referenced field. The value of the instance field token is defined within the scope of the class indicated by the `class` item.

The `token` item of the `CONSTANT_VirtualMethodref_info` structure represents the virtual method token (§4.3.7.6) of the referenced method. The virtual method token is defined within the scope of the hierarchy of the class indicated by the `class` item. If the referenced method is `public` or `protected` the high bit of the `token` item is zero. If the referenced method is package-visible the high bit of the `token` item is one. In this case the `class` item must represent a reference to a class defined in this package.

The `token` item of the `CONSTANT_SuperMethodref_info` structure represents the virtual method token (§4.3.7.6) of the referenced method. Unlike in the CONSTANT_VirtualMethodref_info structure, the virtual method token is defined within the scope of the hierarchy of the superclass of the class indicated by the `class` item. If the referenced method is `public` or `protected` the

high bit of the `token` item is zero. If the referenced method is package-visible the high bit of the `token` item is one. In the latter case the `class` item must represent a reference to a class defined in this package and at least one super-class of the class that contains a defintion of the virtual method must also be defined in this package.

6.7.3 CONSTANT_StaticFieldref and CONSTANT_StaticMethodref

References to static fields and methods are represented by similar structures:

```
CONSTANT_StaticFieldref_info {
       u1 tag
       union {
              { u1 padding
                u2 offset
              } internal_ref
              { u1 package_token
                u1 class_token
                u1 token
              } external_ref
       } static_field_ref
}

CONSTANT_StaticMethodref_info {
       u1 tag
       union {
              { u1 padding
                u2 offset
              } internal_ref
              { u1 package_token
                u1 class_token
                u1 token
              } external_ref
       } static_method_ref
}
```

The items in these structures are as follows:

`tag`

The `tag` item of a CONSTANT_StaticFieldref_info structure has the value CONSTANT_StaticFieldref (5).

The `tag` item of a CONSTANT_StaticMethodref_info structure has the value CONSTANT_StaticMethodref (6).

static_field_ref and static_method_ref

The static_field_ref and static_method_ref item represents a reference to a static field or static method, respectively. Static method references include references to static methods, constructors, and private virtual methods.

If the referenced item is defined in this package the structure represents an internal_ref and the high bit of the structure is zero. If the referenced item is defined in another package the structure represents an external_ref and the high bit of the structure is one.

internal_ref

The internal_ref item represents a reference to a static field or method defined in this package. The items in the structure are:

padding
: The padding item is equal to 0.

offset
: The offset item of a CONSTANT_StaticFieldref_info structure represents a 16-bit offset into the Static Field Image defined by the Static Field component (§6.10) to this static field.

  The offset item of a CONSTANT_StaticMethodref_info structure represents a 16-bit offset into the info item of the Method Component (§6.9) to a method_info structure. The method_info structure must represent the referenced method.

external_ref

The external_ref item represents a reference to a static field or method defined in an imported package. The items in the structure are:

package_token
: The package_token item represents a package token (§4.3.7.1) defined in the Import Component (§6.6) of this CAP file. The value of this token must be a valid index into the packages table item of the import_component structure. The package represented at that index must be the imported package.

  The value of the package token must be between 0 and 127, inclusive.

  The high bit of the package_token item is equal to one.

`class_token`

The `class_token` item represents the token (§4.3.7.2) of the class of the referenced class. It has the value of the class token of the class as defined in the `Export` file of the imported package.

The class indicated by the `class_token` item must define the referenced field or method.

`token`

The `token` item of a `CONSTANT_StaticFieldref_info` structure represents a static field token (§4.3.7.3) as defined in the `Export` file of the imported package. It has the value of the token of the referenced field.

The `token` item of a `CONSTANT_StaticMethodref_info` structure represents a static method token (§4.3.7.4) as defined in the `Export` file of the imported package. It has the value of the token of the referenced method.

6.8 Class Component

The Class Component describes each of the classes and interfaces defined in this package. It does not contain complete access information and content details for each class and interface. Instead, the information included is limited to that required to execute operations associated with a particular class or interface, without performing verification. Complete details regarding the classes and interfaces defined in this package are included in the Descriptor Component (§6.13).

The information included in the Class Component for each interface is sufficient to uniquely identify the interface and to test whether or not a cast to that interface is valid.

The information included in the Class Component for each class is sufficient to resolve operations associated with instances of a class. The operations include creating an instance, testing whether or not a cast of the instance is valid, dispatching virtual method invocations, and dispatching interface method invocations. Also included is sufficient information to locate instance fields of type `reference`, including arrays.

The classes represented in the Class Component reference other entries in the Class Component in the form of superclass, superinterface and implemented interface references. When a superclass, superinterface or implemented interface is defined in an imported package the Import Component is used in the representation of the reference.

The classes represented in the Class Component also contain references to virtual methods defined in the Method Component (§6.9) of this CAP file. References to virtual methods defined in imported packages are not explicitly described. Instead such methods are located through a superclass within the hierarchy of the class, where the superclass is defined in the same imported package as the virtual method.

The Constant Pool Component (§6.7), Export Component (§6.12) and Descriptor Component (§6.13) reference classes and interfaces defined in the Class Component. No other CAP file components reference the Class Component.

The Class Component is represented by the following structure:

```
class_component {
       u1 tag
       u2 size
       interface_info interfaces[]
       class_info classes[]
}
```

The items in the class_component structure are as follows:

tag

The tag item has the value COMPONENT_Class (6).

size

The size item indicates the number of bytes in the class_component structure, excluding the tag and size items. The value of the size item must be greater than zero.

interfaces[]

The interfaces item represents an array of interface_info structures. Each interface defined in this package is represented in the array. The entries are ordered based on hierarchy such that a superinterface has a lower index than any of its subinterfaces.

classes[]

The classes item represents a table of variable-length class_info structures. Each class defined in this package is represented in the array. The entries are ordered based on hierarchy such that a superclass has a lower index than any of its subclasses.

6.8.1 interface_info and class_info

The `interface_info` and `class_info` structures represent interfaces and classes, respectively. The two are differentiated by the value of the high bit in the structures. They are defined as follows:

```
interface_info {
  u1 bitfield {
    bit[4] flags
    bit[4] interface_count
  }
  class_ref superinterfaces[interface_count]
}

class_info {
  u1 bitfield {
    bit[4] flags
    bit[4] interface_count
  }
  class_ref super_class_ref
  u1 declared_instance_size
  u1 first_reference_index
  u1 reference_count
  u1 public_method_table_base
  u1 public_method_table_count
  u1 package_method_table_base
  u1 package_method_table_count
  u2 public_virtual_method_table[public_method_table_count]
  u2 package_virtual_method_table[package_method_table_count]
  implemented_interface_info interfaces[interface_count]
}
```

The items of the `interface_info` and `class_info` structure are as follows:

`flags`

The flags item is a mask of modifiers used to describe this interface or class. Valid values are shown in the following table:

Name	Value
ACC_INTERFACE	0x8
ACC_SHAREABLE	0x4

TABLE 6-6 CAP file interface and class flags

The ACC_INTERFACE flag indicates whether this `interface_info` or `class_info` structure represents an interface or a class. The value must be 1 if it represents an `interface_info` structure and 0 if a `class_info` structure.

The ACC_SHAREABLE flag in an `interface_info` structure indicates whether

this interface is shareable. The value of this flag must be one if and only if the interface is `javacard.framework.Shareable` interface or implements that interface directly or indirectly.

The `ACC_SHAREABLE` flag in a `class_info` structure indicates whether this class is shareable.[1] The value of this flag must be one if and only if this class or any of its superclasses implements an interface that is shareable.

The Java Card virtual machine reserves all other flag values. Their values must be zero.

`interface_count`

The `interface_count` item of the `interface_info` structure indicates the number of entries in the `superinterfaces` table item. The value represents the number of immediate superinterfaces of this interface.It does not include superinterfaces of the superinterfaces. Valid values are between 0 and 15, inclusive.

The `interface_count` item of the `class_info` structure indicates the number of entries in the `interfaces` table item. The value represents the number of interfaces implemented by this class, including superinterfaces of those interfaces and potentially interfaces implemented by superclasses of this class. Valid values are between 0 and 15, inclusive.

`superinterfaces`

The `superinterfaces` item of the `interface_info` structure is an array of `class_ref` structures representing the superinterfaces of this interface. The `class_ref` structure is defined as part of the `CONSTANT_Classref_info` structure (§6.7.1). This array is empty if this interface has no superinterfaces. Only immediate superinterfaces are represented in the array. Superinterfaces of superinterfaces are not included, and class `Object` is not included either.

`super_class_ref`

The `super_class_ref` item of the `class_info` structure is a `class_ref` structure representing the superclass of this class. The `class_ref` structure is defined as part of the `CONSTANT_Classref_info` structure (§6.7.1).

The `super_class_ref` item has the value of 0xFFFF only if this class does not have a superclass. Otherwise the value of the `super_class_ref` item is limited only by the constraints of the `class_ref` structure.

`declared_instance_size`

The `declared_instance_size` item of the `class_info` structure represents the number of 16-bit cells required to represent the instance fields declared by

1. A Java Card virtual machine uses the `ACC_SHAREABLE` flag to implement the firewall restrictions defined by the Java Card Runtime Environment (JCRE) 2.1 specification.

this class. It does not include instance fields declared by superclasses of this class.

Instance fields of type `int` are represented in two 16-bit cells, while all other field types are represented in one 16-bit cell.

`first_reference_token`

The `first_reference_token` item of the `class_info` structure represents the instance field token (§4.3.7.5) value of the first `reference` type instance field defined by this class. It does not include instance fields defined by superclasses of this class.

If this class does not define any `reference` type instance fields, the value of the `first_reference_token` is 0xFF. Otherwise the value of the `first_reference_token` item must be within the range of the set of instance field tokens of this class.

`reference_count`

The `reference_count` item of the `class_info` structure represents the number of `reference` type instance field defined by this class. It does not include `reference` type instance fields defined by superclasses of this class.

Valid values of the `reference_count` item are between 0 and the maximum number of instance fields defined by this class.

`public_method_table_base`

The `public_method_table_base` item of the `class_info` structure is equal to the virtual method token value (§4.3.7.6) of the first method in the `public_virtual_method_table` array. If the `public_virtual_method_table` array is empty the value of the `public_method_table_base` item is equal to the `public_method_table_base` item of the `class_info` structure of this class' superclass plus the `public_method_table_count` item of the `class_info` structure of this class' superclass. If this class has no superclass and the `public_virtual_method_table` array is empty, the value of the `public_method_table_base` item is zero.

`public_method_table_count`

The `public_method_table_count` item of the `class_info` structure indicates the number of entries in the `public_virtual_method_table` array.

If this class does not define any `public` or `protected` override methods, the minimum valid value of `public_method_table_count` item is the number of `public` and `protected` virtual methods declared by this class. If this class defines one or more `public` or `protected` override methods, the minimum valid value of `public_method_table_count` item is the value of the largest `public` or `protected` virtual method token, minus the value of the smallest

public or protected virtual override method token, plus one.

The maximum valid value of the public_method_table_count item is the value of the largest public or protected virtual method token, plus one.

Any value for the public_method_table_count item between the minimum and maximum specified here is valid. However, the value must correspond to the number of entries in the public_virtual_method_table array.

package_method_table_base

The package_method_table_base item of the class_info structure is equal to the virtual method token value (§4.3.7.6) of the first entry in the package_virtual_method_table array. If the package_virtual_method_table array is empty the value of the package_method_table_base item is equal to the package_method_table_base item of the class_info structure of this class' superclass plus the package_method_table_count item of the class_info structure of this class' superclass. If this class has no superclass or inherits from a class defined in another package and the package_virtual_method_table array is empty, the value of the package_method_table_base item is zero.

package_method_table_count

The package_method_table_count item of the class_info structure indicates the number of entries in the package_virtual_method_table array.

If this class does not define any override methods, the minimum valid value of package_method_table_count item is the number of package visible virtual methods declared by this class. If this class defines one or more package visible override methods, the minimum valid value of package_method_table_count item is the value of the largest package visible virtual method token, minus the value of the smallest package visible virtual override method token, plus one.

The maximum valid value of the package_method_table_count item is the value of the largest package visible method token, plus one.

Any value for the package_method_table_count item between the minimum and maximum specified here are valid. However, the value must correspond to the number of entries in the package_virtual_method_table.

public_virtual_method_table

The public_virtual_method_table item of the class_info structure represents an array of public and protected virtual methods. These methods can be invoked on an instance of this class. The public_virtual_method_table array includes methods declared or defined by this class. It may also include methods declared or defined by any or all of its superclasses. The value of an index into this table must be equal to the value of the virtual method token of

the indicated method, minus the value of the `public_method_table_base` item.

Entries in the `public_virtual_method_table` array that represent methods defined or declared in this package contain offsets into the `info` item of the Method Component (§6.9) to the `method_info` structure representing the method. Entries that represent methods defined or declared in an imported package contain the value 0xFFFF.

Entries for methods that are declared abstract, not including those defined by interfaces, are represented in the `public_virtual_method_table` array in the same way as non-abstract methods.

`package_virtual_method_table`

The `package_virtual_method_table` item of the `class_info` structure represents an array of package-visible virtual methods. These methods can be invoked on an instance of this class. The `package_virtual_method_table` array includes methods declared or defined by this class. It may also include methods declared or defined by any or all of its superclasses that are defined in this package. The value of an index into this table must be equal to the value of the virtual method token of the indicated method & 0x7F, minus the value of the `package_method_table_base` item.

All entries in the `package_virtual_method_table` array represent methods defined or declared in this package. They contain offsets into the `info` item of the Method Component (§6.9) to the `method_info` structure representing the method.

Entries for methods that are declared abstract, not including those defined by interfaces, are represented in the `package_virtual_method_table` array in the same way as non-abstract methods.

`interfaces[]`

The `interfaces` item of the `class_info` structure represents a table of variable-length `implemented_interface_info` structures. The table must contain an entry for each of the implemented interfaces indicated in the declaration of this class and each of the interfaces in the hierarchies of those interfaces. Interfaces that occur more than once are represented by a single entry. Interfaces implemented by superclasses of this class may optionally be represented.

Given the declarations below, the number of entries for class c0 is 1 and the entry in the `interfaces` array is i0. The minimum number of entries for class c1 is 3 and the entries in the `interfaces` array are i1, i2, and i3. The entries for class c1 may also include interface i0, which is implemented by the superclass of c1.

```
interface i0 {}
interface i1 {}
interface i2 extends i1 {}
interface i3 {}
class c0 implements i0 {}
class c1 extends c0 implements i2, i3 {}
```

The `implemented_interface_info` structure is defined as follows:

```
implemented_interface_info {
       class_ref interface
       u1 count
       u1 index[count]
}
```

The items in the `implemented_interface_info` structure are defined as follows:

`interface`

The `interface` item has the form of a `class_ref` structure. The `class_ref` structure is defined as part of the `CONSTANT_Classref_info` structure (§6.7.1). The `interface_info` structure referenced by the `interface` item represents an interface implemented by this class.

`count`

The `count` item indicates the number of entries in the `index` array.

`index`

The `index` item is an array that maps declarations of interface methods to implementations of those methods in this class. It is a representation of a the set of methods declared by the interface and its superinterfaces.

Entries in the `index` array must be ordered such that the interface method token value (§4.3.7.7) of the interface method is equal to the index into the array. The interface method token value is assigned to the method within the scope of the interface definition and its superinterfaces, not within the scope of this class.

The values in the `index` array represent the virtual method tokens (§4.3.7.6) of the implementations of the interface methods. The virtual method token values are defined within the scope of the hierarchy of this class.

6.9 Method Component

The Method Component describes each of the methods declared in this package, excluding `<clinit>` methods and interface method declarations. The exception handlers associated with each method are also described.

The Method Component does not contain complete access information and descriptive details for each method. Instead, the information is limited to that required to execute each method, without performing verification. Complete details regarding the methods defined in this package are included in the Descriptor Component (§6.13).

Instructions and exception handler catch types in the Method Component reference entries in the Constant Pool Component (§6.7). No other `CAP` file components, including the Method Component, are referenced by the elements in the Method Component.

The Applet Component (§6.5), Constant Pool Component (§6.7), Export Component (§6.12), and Descriptor Component (§6.13) reference methods defined in the Method Component. The Reference Location Component (§6.11) references all constant pool indices contained in the Method Component. No other `CAP` file components reference the Method Component.

The Method Component is represented by the following structure:

```
method_component {
        u1 tag
        u2 size
        u1 handler_count
        exception_handler_info
        exception_handlers[handler_count]
        method_info methods[]
}
```

The items in the `method_component` structure are as follows:

`tag`

The `tag` item has the value `COMPONENT_Method` (7).

`size`

The `size` item indicates the number of bytes in the `method_component` structure, excluding the `tag` and `size` items. The value of the `size` item must be greater than zero.

`handler_count`

The `handler_count` item represents the number of entries in the `exception_handlers` array. Valid values are between 0 and 255, inclusive.

`exception_handlers[]`

The `exception_handlers` item represents an array of 8-byte `exception_handler_info` structures. Each `exception_handler_info` structure represents a `catch` or `finally` block defined in a method of this package.

Entries in the `exception_handlers` array are sorted in ascending order by the distance between the beginning of the Method Component to the endpoint of each exception handler range in the `methods` item.

`methods[]`

The `methods` item represents a table of variable-length `method_info` structures. Each entry represents a method declared in a class of this package. `<clinit>` methods and interface method declaration are not included; all other methods, including non-interface abstract methods, are.

6.9.1 exception_handler_info

The `exception_handler_info` structure is defined as follows:

```
exception_handler_info {
       u2 start_offset
       u2 active_length
       u2 handler_offset
       u2 catch_type_index
}
```

The items in the `exception_handler_info` structure are as follows:

`start_offset, active_length`

The `active_length` item is encoded to indicate whether the active range of this exception handler is nested within another exception handler. The high bit of the `active_length` item is equal to 1 if the active range is not contained within another exception handler, and this exception handler is the last handler applicable to the active range. The high bit is equal to 0 if the active range is contained within the active range of another exception handler, or there are successive handlers applicable to the same active range.

end_offset is defined as `start_offset` plus `active_length` & 0x7FFF.

The `start_offset` item and *end_offset* are byte offsets into the `info` item of

the Method Component. They indicate the ranges in a bytecode array at which the exception handler is active. The value of the `start_offset` must be a valid offset into a `bytecodes` array of a `method_info` structure to an opcode of an instruction. The value of the *end_offset* either must be a valid offset into a `bytecodes` array of a `method_info` structure to an opcode of an instruction or must be equal to a method's bytecode count, the length of the `bytecodes` array of a `method_info` structure. The value of the `start_offset` must be less than the value of the *end_offset*.

The `start_offset` is inclusive and the *end_offset* is exclusive; that is, the exception handler must be active while the execution address is within the interval [`start_offset`, *end_offset*).

`handler_offset`

The handler_offset item represents a byte offset into the `info` item of the Method Component. It indicates the start of the exception handler. The value of the item must be a valid offset into a `bytecodes` array of a `method_info` structure to an opcode of an instruction, and must be less than the value of the method's bytecode count.

`catch_type_index`

If the value of the `catch_type_index` item is non-zero, it must be a valid index into the `constant_pool` array of the Constant Pool Component (§6.7). The `constant_pool` entry at that index must be a `CONSTANT_Classref_info` structure, representing the class of the exception caught by this `exception_handlers` array entry.

If the `exception_handlers` table entry represents a finally block, the value of the `catch_type_index` item is zero. In this case the exception handler is called for all exceptions that are thrown within the `start_offset` and *end_offset* range.

6.9.2 method_info

The `method_info` structure is defined as follows:

```
method_info {
       method_header_info method_header
       u1 bytecodes[]
}
```

The items in the `method_info` structure are as follows:

`method_header`

The `method_header` item represents either a `method_header_info` or an

`extended_method_header_info` structure:

```
method_header_info {
       u1 bitfield {

         bit[4] flags
         bit[4] max_stack
       }
       u1 bitfield {
         bit[4] nargs
         bit[4] max_locals
       }
}

extended_method_header_info {
       u1 bitfield {
         bit[4] flags
         bit[4] padding
       }
       u1 max_stack
       u1 nargs

       u1 max_locals
}
```

The items of the `method_header_info` and extended_method_header_info structures are as follows:

`flags`

The flags item is a mask of modifiers defined for this method. Valid flag values are shown in the following table.

Flags	Values
ACC_EXTENDED	0x8
ACC_ABSTRACT	0x4

TABLE 6-7 CAP file method flags

The value of the `ACC_EXTENDED` flag must be one if the `method_header` is represented by an `extended_method_header_info` structure. Otherwise the value must be zero.

The value of the `ACC_ABSTRACT` flag must be one if this method is defined as abstract. In this case the `bytecodes` array must be empty. If this method is not abstract the value of the `ACC_ABSTRACT` flag must be zero.

The Java Card virtual machine reserves all other flag values. Their values must be zero.

`padding`

The `padding` item has the value of zero. This item is only defined for the `extended_method_header_info` structure.

`max_stack`

The `max_stack` item indicates the maximum number of 16-bit cells required on the operand stack during execution of this method.

Stack entries of type `int` are represented in two 16-bit cells, while all others are represented in one 16-bit cell.

`nargs`

The `nargs` item indicates the number of 16-bit cells required to represent the parameters passed to this method, including the `this` pointer if this method is a virtual method.

Parameters of type `int` are represented in two 16-bit cells, while all others are represented in one 16-bit cell.

`max_locals`

The `max_locals` item indicates the number of 16-bit cells required to represent the local variables declared by this method, not including the parameters passed to this method on invocation.[1]

Local variables of type `int` are represented in two 16-bit cells, while all others are represented in one 16-bit cell. The number of cells required for overloaded local variables is two if one or more of the overloaded variables is of type `int`.

`bytecodes[]`

The `bytecodes` item represents an array of Java Card bytecodes that implement this method. Valid instructions are defined in Chapter 7, “Java Card Virtual Machine Instruction Set”. The *impdep1* and *impdep2* bytecodes can not be present in the `bytecodes` array item.

If this method is abstract the `bytecodes` item must contain zero elements.

1. Unlike in Java Card `CAP` files, in Java `class` files the `max_locals` item includes both the local variables declared by the method and the parameters passed to the method.

6.10 Static Field Component

The Static Field Component contains all of the information required to create and initialize an image of all of the static fields defined in this package, referred to as the *static field image*. `Final static` fields of primitive types are not represented in the static field image. Instead these compile-time constants are placed in line in Java Card instructions.

The Static Field Component does not reference any other component in this `CAP` file. The Constant Pool Component (§6.7), Export Component (§6.12) and Descriptor Component (§6.13) reference fields defined in the Static Field Component.

The ordering constraints, or segments, associated with a static field image are shown in TABLE 6-8. `Reference` types occur first in the image. Arrays initialized through Java `<clinit>` methods occur first within the set of `reference` types. Primitive types occur last in the image, and primitive types initialized to non-default values occur last within the set of primitive types.

category	segment	content
`reference` types	1	arrays of primitive types initialized by `<clinit>` methods
	2	`reference` types initialized to `null`
primitive types	3	primitive types initialized to default values
	4	primitive types initialized to non-default values

TABLE 6-8 Segments of a static field image

The number of bytes used to represent each field type in the static field image is shown in the following table.

Type	Bytes
`boolean`	`1`
`byte`	`1`
`short`	`2`
`int`	`4`
`reference`, including arrays	`2`

TABLE 6-9 Static field sizes

The `static_field_component` structure is defined as:

```
static_field_component {
       u1 tag
       u2 size
       u2 image_size
       u2 reference_count
       u2 array_init_count
       array_init_info array_init[array_init_count]
       u2 default_value_count
       u2 non_default_value_count
       u1 non_default_values[non_default_values_count]
}
```

The items in the `static_field_component` structure are as follows:

`tag`

The `tag` item has the value `COMPONENT_StaticField` (8).

`size`

The `size` item indicates the number of bytes in the `static_field_component` structure, excluding the `tag` and `size` items. The value of the `size` item must be greater than zero.

`image_size`

The `image_size` item indicates the number of bytes required to represent the static fields defined in this package, excluding final static fields of primitive types. This value is the number of bytes in the static field image. The number of bytes required to represent each field type is shown in TABLE 6-9.

The value of the `image_size` item does not include the number of bytes require to represent the initial values of array instances enumerated in the Static Field Component.

`reference_count`

The `reference_count` item indicates the number of `reference` type static fields defined in this package. This is the number of fields represented in segments 1 and 2 of the static field image as described in TABLE 6-8.

The value of the `reference_count` item may be 0 if no `reference` type fields are defined in this package. Otherwise it must be equal to the number of `reference` type fields defined.

`array_init_count`

The `array_init_count` item indicates the number of elements in the `array_init` array. This is the number of fields represented in segment 1 of the static field image as described in TABLE 6-8. It represents the number of arrays

initialized in all of the <clinit> methods in this package.

If this CAP file defines a library package the value of array_init_count must be zero.

array_init[]

The array_init item represents an array of array_init_info structures that specify the initial array values of static fields of arrays of primitive types. These initial values are indicated in Java <clinit> methods. The array_init_info structure is defined as:

```
array_init_info {
       u1 type
       u2 count
       u1 values[count]
}
```

The items in the array_init_info structure are defined as follows:

type

The type item indicates the type of the primitive array. Valid values are shown in the following table.

Type	Value
boolean	2
byte	3
short	4
int	5

TABLE 6-10 Array types

count

The count item indicates the number of bytes in the values array. It does not represent the number of elements in the static field array (referred to as *length* in Java), since the values array is an array of bytes and the static field array may be a non-byte type. The Java length of the static field array is equal to the count item divided by the number of bytes required to represent the static field type (TABLE 6-9) indicated by the type item.

values

The values item represents a byte array containing the initial values of the static field array. The number of entries in the values array is equal to the size in bytes of the type indicated by the type item. The size in bytes of each type is shown in TABLE 6-9.

`default_value_count`

The `default_value_count` item indicates the number of bytes required to initialize the set of static fields represented in segment 3 of the static field image as described in TABLE 6-8. These static fields are primitive types initialized to default values. The number of bytes required to initialize each static field type is equal to the size in bytes of the type as shown in TABLE 6-9.

`non_default_value_count`

The `non_default_value_count` item represents the number bytes in the `non_default_values` array. This value is equal to the number of bytes in segment 4 of the static field image as described in TABLE 6-8. These static fields are primitive types initialized to non-default values.

`non_default_values[]`

The `non_default_values` item represents an array of bytes of non-default initial values. This is the exact image of segment 4 of the static field image as described in TABLE 6-8. The number of entries in the `non_default_values` array for each static field type is equal to the size in bytes of the type as shown in TABLE 6-9.

6.11 Reference Location Component

The Reference Location Component represents lists of offsets into the `info` item of the Method Component (§6.9) to operands that contain indices into the `constant_pool` array of the Constant Pool Component (§6.7). Some of the constant pool indices are represented in one-byte values while others are represented in two-byte values.

The Reference Location Component is not referenced by any other component in this `CAP` file.

The Reference Location Component structure is defined as:

```
reference_location_component {
       u1 tag
       u2 size
       u2 byte_index_count
       u1 offsets_to_byte_indices[byte_index_count]
       u2 byte2_index_count
       u1 offsets_to_byte2_indices[byte2_index_count]
}
```

The items of the `reference_location_component` structure are as follows:

`tag`

The tag item has the value COMPONENT_ReferenceLocation (9).

`size`

The `size` item indicates the number of bytes in the `reference_location_component` structure, excluding the `tag` and `size` items. The value of the `size` item must be greater than zero.

`byte_index_count`

The `byte_index_count` item represents the number of elements in the `offsets_to_byte_indices` array.

`offsets_to_byte_indices[]`

The `offsets_to_byte_indices` item represents an array of 1-byte jump offsets into the `info` item of the Method Component to each 1-byte `constant_pool` array index. Each entry represents the number of bytes (or *distance*) between the current index to the next. If the distance is greater than or equal to 255 then there are *n* entries equal to 255 in the array, where *n* is equal to the distance divided by 255. The *nth* entry of 255 is followed by an entry containing the value of the distance modulo 255.

An example of the jump offsets in an `offsets_to_byte_indices` array is shown in the following table.

Instruction	Offset to Operand	Jump Offset
`getfield_a 0`	10	10
`putfield_b 2`	65	55
		255
		255
`getfield_s 1`	580	5
		255
`putfield_a 0`	835	0
`getfield_i 3`	843	8

TABLE 6-11 One-byte reference location example

All 1-byte `constant_pool` array indices in the Method Component must be represented in `offsets_to_byte_indices` array.

`byte2_index_count`

The `byte2_index_count` item represents the number of elements in the `offsets_to_byte2_indices` array.

`offsets_to_byte2_indices[]`

The `offsets_to_byte2_indices` item represents an array of 1-byte jump off-

sets into the info item of the Method Component to each 2-byte `constant_pool` array index. Each entry represents the number of bytes (or *distance*) between the current index to the next. If the distance is greater than or equal to 255 then there are *n* entries equal to 255 in the array, where *n* is equal to the distance divided by 255. The *nth* entry of 255 is followed by an entry containing the value of the distance modulo 255.

An example of the jump offsets in an offsets_to_byte_indices array is shown in TABLE 6-11. The same example applies to the offsets_to_byte2_indices array if the instructions are changed to those with 2-byte `constant_pool` array indices.

All 2-byte `constant_pool` array indices in the Method Component must be represented in `offsets_to_byte2_indices` array, including those represented in `catch_type_index` items of the `exception_handler_info` array.

6.12 Export Component

The Export Component lists all static elements in this package that may be imported by classes in other packages. Instance fields and virtual methods are not represented in the Export Component.

If this `CAP` file does not include an Applet Component (§6.5) (called a *library* package) , the Export Component contains an entry for each `public` class and `public` interface defined in this package. Furthermore, for each `public` class there is an entry for each `public` or `protected static` field defined in that class, for each `public` or `protected static` method defined in that class, and for each `public` or protected constructor defined in that class. `Final static` fields of primitive types (compile-time constants) are not included.

If this `CAP` file includes an Applet Component (§6.5) (called an *applet* package) the Export Component includes entries only for all `public` interfaces that are shareable.[1] An interface is sharable if and only if it is the `javacard.framework.Shareable` interface or implements (directly or indirectly) that interface.

Elements in the Export Component reference elements in the Class Component (§6.8), Method Component (§6.9), and Static Field Component (§6.10). No other component in this `CAP` file references the Export Component.

1. The restriction on shareable functionality is imposed by the firewall as defined in the Java Card Runtime Environment (JCRE) 2.1 specification.

The Export Component is represented by the following structure:

```
export_component {
        u1 tag
        u2 size
        u1 class_count
        class_export_info {
                u2 class_offset
                u1 static_field_count
                u1 static_method_count
                u2 static_field_offsets[static_field_count]
                u2 static_method_offsets[static_method_count]
        } class_exports[class_count]
}
```

The items of the `export_component` structure are as follows:

`tag`

The `tag` item has the value `COMPONENT_Export` (10).

`size`

The `size` item indicates the number of bytes in the `export_component` structure, excluding the `tag` and `size` items. The value of the `size` item must be greater than zero.

`class_count`

The `class_count` item represents the number of entries in the `class_exports` table.

`class_exports[]`

The `class_exports` item represents a variable-length table of `class_export_info` structures. If this package is a library package, the table contains an entry for each of the `public` classes and `public` interfaces defined in this package. If this package is an applet package, the table contains an entry for each of the `public` shareable interfaces defined in this package.

An index into the table to a particular class or interface is equal to the token value of that class or interface (§4.3.7.2). The token value is published in the `Export` file (§5.5) of this package.

The items in the `class_export_info` structure are:

`class_offset`

The `class_offset` item represents a byte offset into the `info` item of the Class Component (§6.8). If this package defines a library package, the item at that offset must be either an `interface_info` or a `class_info` structure. The `interface_info` or `class_info` struc-

ture at that offset must represent the exported class or interface.

If this package defines an applet package, the item at the `class_offset` in the `info` item of the Class Component must be an `interface_info` structure. The `interface_info` structure at that offset must represent the exported, shareable interface. In particular, the `ACC_SHAREABLE` flag of the `interface_info` structure must be equal to 1.

`static_field_count`

The `static_field_count` item represents the number of elements in the `static_field_offsets` array. This value indicates the number of `public` and `protected static` fields defined in this class, excluding `final static` fields of primitive types.

If the `class_offset` item represents an offset to an `interface_info` structure, the value of the `static_field_count` item must be zero.

`static_method_count`

The `static_method_count` item represents the number of elements in the `static_method_offsets` array. This value indicates the number of `public` and `protected static` methods and constructors defined in this class.

If the `class_offset` item represents an offset to an `interface_info` structure, the value of the `static_method_count` item must be zero.

`static_field_offsets[]`

The `static_field_offsets` item represents an array of 2-byte offsets into the static field image defined by the Static Field Component (§6.10). Each offset must be to the beginning of the representation of the exported static field.

An index into the `static_field_offsets` array must be equal to the token value of the field represented by that entry. The token value is published in the `Export` file (§5.7) of this package.

`static_method_offsets[]`

The `static_method_offsets` item represents a table of 2-byte offsets into the `info` item of the Method Component (§6.9). Each offset must be to the beginning of a `method_info` structure. The `method_info` structure must represent the exported static method or constructor.

An index into the `static_method_offsets` array must be equal to the token value of the method represented by that entry.

6.13 Descriptor Component

The Descriptor Component provides sufficient information to parse and verify all elements of the CAP file. It references, and therefore describes, elements in the Constant Pool Component (§6.7), Class Component (§6.8), Method Component (§6.9), and Static Field Component (§6.10). No components in the CAP file reference the Descriptor Component.

The Descriptor Component is represented by the following structure:

```
descriptor_component {
       u1 tag
       u2 size
       u1 class_count
       class_descriptor_info classes[class_count]
       type_descriptor_info types
}
```

The items of the descriptor_component structure are as follows:

tag

The tag item has the value COMPONENT_Descriptor (11).

size

The size item indicates the number of bytes in the descriptor_component structure, excluding the tag and size items. The value of the size item must be greater than zero.

class_count

The class_count item represents the number of entries in the classes table.

classes[]

The classes item represents a table of variable-length class_descriptor_info structures. Each class and interface defined in this package is represented in the table.

types

The types item represents a type_descriptor_info structure. This structure lists the set of field types and method signatures of the fields and methods defined or referenced in this package. Those referenced are enumerated in the Constant Pool Component.

6.13.1 class_descriptor_info

The `class_descriptor_info` structure is used to describe a class or interface defined in this package:

```
class_descriptor_info {
       u1 token
       u1 access_flags
       class_ref this_class_ref
       u1 interface_count
       u2 field_count
       u2 method_count
       class_ref interfaces [interface_count]
       field_descriptor_info fields[field_count]
       method_descriptor_info methods[method_count]
}
```

The items of the `class_descriptor_info` structure are as follows:

`token`

The `token` item represents the class token (§4.3.7.2) of this class or interface. If this class or interface is package-visible it does not have a token assigned. In this case the value of the `token` item must be 0xFF.

`access_flags`

The `access_flags` item is a mask of modifiers used to describe the access permission to and properties of this class or interface. The `access_flags` modifiers for classes and interfaces are shown in the following table.

Name	Value
ACC_PUBLIC	0x01
ACC_FINAL	0x10
ACC_INTERFACE	0x40
ACC_ABSTRACT	0x80

TABLE 6-12 CAP file class descriptor flags

The class access and modifier flags defined in the table above are a subset of those defined for classes and interfaces in a Java `class` file. They have the same meaning, and are set under the same conditions, as the corresponding flags in a Java `class` file.

The Java Card virtual machine reserves all other flag values. Their values must be zero.

`this_class_ref`

The `this_class_ref` item is a `class_ref` structure indicating the location of the `class_info` structure in the Class Component (§6.8). The `class_ref` structure is defined as part of the `CONSTANT_Classref_info` structure (§6.7.1).

`interface_count`

The `interface_count` item represents the number of entries in the `interfaces` array.

`field_count`

The `field_count` item represents the number of entries in the `fields` array. If this `class_descriptor_info` structure represents an interface, the value of the `field_count` item is equal to zero.

`method_count`

The `method_count` item represents the number of entries in the `methods` array.

`interfaces[]`

The `interfaces` item represents an array of interfaces implemented by this class or interface. The elements in the array are `class_ref` structures indicating the location of the `class_info` structure in the Class Component (§6.8). The `class_ref` structure is defined as part of the `CONSTANT_Classref_info` structure (§6.7.1).

`fields[]`

The `fields` item represents an array of `field_descriptor_info` structures. Each field declared by this class is represented in the array.

`methods[]`

The `methods` item represents an array of `method_descriptor_info` structures. Each method declared or defined by this class or interface is represented in the array.

6.13.2 field_descriptor_info

The `field_descriptor_info` structure is used to describe a field defined in this package:

```
field_descriptor_info {
       u1 token
       u1 access_flags
       union {
              static_field_ref static_field
              instance_field_ref instance_field
       } field_ref
       union {
              u2 primitive_type
              u2 reference_type
       } type
}
```

The items of the `field_descriptor_info` structure is as follows:

`token`

The `token` item represents the token of this field. If this field is private or package-visible static field it does not have a token assigned. In this case the value of the `token` item must be 0xFF.

`access_flags`

The `access_flags` item is a mask of modifiers used to describe the access permission to and properties of this field. The `access_flags` modifiers for fields are shown in the following table.

Name	Value
ACC_PUBLIC	0x01
ACC_PRIVATE	0x02
ACC_PROTECTED	0x04
ACC_STATIC	0x08
ACC_FINAL	0x10

TABLE 6-13 CAP file field descriptor flagss

The field access and modifier flags defined in the table above are a subset of those defined for fields in a Java `class` file. They have the same meaning, and are set under the same conditions, as the corresponding flags in a Java `class` file.

The Java Card virtual machine reserves all other flag values. Their values must be zero.

`field_ref`

The `field_ref` item represents a reference to this field. If the `ACC_STATIC` flag is equal to 1, this item represents a `static_field_ref` as defined in the `CONSTANT_StaticFieldref` structure (§6.7.3).

If the `ACC_STATIC` flag is equal to 0, this item represents an `instance_field_ref` as defined in the `CONSTANT_InstanceFieldref` structure (§6.7.2).

`type`

The `type` item indicates the type of this field. directly or indirectly. If this field is a primitive type (`boolean`, `byte`, `short`, or `int`) the high bit of this item is equal to 1, otherwise the high bit of this item is equal to 0.

`primitive_type`

The `primitive_type` item represents the type of this field using the values in the table below. As noted above, the high bit of the `primitive_type` item is equal to 1.

Data Type	Value
`boolean`	0x0002
`byte`	0x0003
`short`	0x0004
`int`	0x0005

TABLE 6-14 Primitive type descriptor values

`reference_type`

The `reference_type` item represents a 15-bit offset into the `type_descriptor_info` structure. The item at the offset must represent the `reference` type of this field. As noted above, the high bit of the `reference_type` item is equal to 0.

6.13.3 method_descriptor_info

The `method_descriptor_info` structure is used to describe a method defined in this package:

```
method_descriptor_info {
       u1 token
       u1 access_flags
       u2 method_offset
       u2 type_offset
       u2 bytecode_count
       u2 exception_handler_count
       u2 exception_handler_index
}
```

The items of the `method_descriptor_info` structure are as follows:

`token`

The `token` item represents the static method token (§4.3.7.4) or virtual method token (§4.3.7.6) or interface method token (§4.3.7.7) of this method. If this method is a private or package-visible static method, a private or package-visible constructor, or a private virtual method it does not have a token assigned. In this case the value of the `token` item must be 0xFF.

`access_flags`

The `access_flags` item is a mask of modifiers used to describe the access permission to and properties of this method. The `access_flags` modifiers for methods are shown in the following table.

Name	Value
ACC_PUBLIC	0x01
ACC_PRIVATE	0x02
ACC_PROTECTED	0x04
ACC_STATIC	0x08
ACC_FINAL	0x10
ACC_ABSTRACT	0x40
ACC_INIT	0x80

TABLE 6-15 CAP file method descriptor flags

The method access and modifier flags defined in the table above, except the `ACC_INIT` flag, are a subset of those defined for methods in a Java `class` file. They have the same meaning, and are set under the same conditions, as the corresponding flags in a Java `class` file.

The `ACC_INIT` flag is set if the method descriptor identifies a constructor meth-

ods. In Java a constructor method is recognized by its name, `<init>`, but in Java Card the name is replaced by a token. As in the Java verifier, these methods require special checks by the Java Card verifier.

The Java Card virtual machine reserves all other flag values. Their values must be zero.

`method_offset`

If the `class_descriptor_info` structure that contains this `method_descriptor_info` structure represents a class, the `method_offset` item represents a byte offset into the `info` item of the Method Component (§6.9). The element at that offset must be the beginning of a `method_info` structure. The `method_info` structure must represent this method.

If the `class_descriptor_info` structure that contains this `method_descriptor_info` structure represents an interface, the value of the `method_offset` item must be zero.

`type_offset`

The `type_offset` item must be a valid offset into the `type_descriptor_info` structure. The type described at that offset represents the signature of this method.

`bytecode_count`

The `bytecode_count` item represents the number of bytecodes in this method. The value is equal to the length of the `bytecodes` array item in the `method_info` structure in the method component (§6.9) of this method.

`exception_handler_count`

The `exception_handler_count` item represents the number of exception handlers implemented by this method.

`exception_handler_index`

The `exception_handler_index` item represents the index to the first `exception_handlers` table entry in the method component (§6.9) implemented by this method. Succeeding `exception_handlers` table entries, up to the value of the exception_handler_count item, are also exception handlers implemented by this method.

The value of the `exception_handler_index` item is 0 if the value of the `exception_handler_count` item is 0.

6.13.4 type_descriptor_info

The `type_descriptor_info` structure represents the types of fields and signatures of methods defined in this package:

```
type_descriptor_info {
       u2 constant_pool_count
       u2 constant_pool_types[constant_pool_count]
       { u1 nibble_count;
         u1 type[(nibble_count+1) / 2];
       } type_desc[]
}
```

The `type_descriptor_info` structure contains the following elements:

`constant_pool_count`

The `constant_pool_count` item represents the number of entries in the `constant_pool_types` array. This value is equal to the number of entries in the `constant_pool` array of the Constant Pool Component (§6.7).

`constant_pool_types[]`

The `constant_pool_types` item is an array that describes the types of the fields and methods referenced in the Constant Pool Component. This item has the same number of entries as the `constant_pool` array of the Constant Pool Component, and each entry describes the type of the corresponding entry in the `constant_pool` array.

If the corresponding `constant_pool` array entry represents a class or interface reference, it does not have an associated type. In this case the value of the entry in the `constant_pool_types` array item is 0xFFFF.

If the corresponding `constant_pool` array entry represents a field or method, the value of the entry in the `constant_pool_types` array is an offset into the `type_descriptor_info` structure. The element at that offset must describe the type of the field or the signature of the method.

`type_desc[]`

The `type_desc` item represents a table of variable-length type descriptor structures. These descriptors represent the types of fields and signatures of methods. The elements in the structure are:

`nibble_count`

The `nibble_count` value represents the number of nibbles required to describe the type encoded in the `type` array. This is different from the length of the `type` array if the value of the `nibble_count` item is odd. In this case the length of the `type` array is one greater than the value of `nibble_count`.

`type[]`

The `type` array contains an encoded description of the type, composed of individual nibbles. If the `nibble_count` item is an odd number, the last nibble in the `type` array must be 0x0. The values of the type descriptor nibbles are defined in the following table.

Type	Value
`void`	0x1
`boolean`	0x2
`byte`	0x3
`short`	0x4
`int`	0x5
`reference`	0x6
array of `boolean`	0xA
array of `byte`	0xB
array of `short`	0xC
array of `int`	0xD
array of `reference`	0xE

TABLE 6-16 Type descriptor values

Class `reference` types are described using the `reference` nibble 0x6, followed by a 2-byte (4-nibble) `class_ref` structure. The `class_ref` structure is defined as part of the `CONSTANT_Classref_info` structure (§6.7.1). For example, a field of type `reference` to `p1.c1` in a `CAP` file defining package `p0` is described as:

Nibble	Value	Description
0	0x6	`reference`
1	<p1>	package token (high bit on)
2		
3	<c1>	class token
4		
5	0x0	`padding`

TABLE 6-17 Encoded `reference` type `p1.c1`

The following are examples of the array types:

Nibble	Value	Description
0	0xB	array of `byte`
1	0x0	`padding`

TABLE 6-18 Encoded `byte` array type

Nibble	Value	Description
0	0xE	array of `reference`
1	<p1>	package token (high bit on)
2		
3	<c1>	class token
4		
5	0x0	`padding`

TABLE 6-19 Encoded `reference` array type `p1.c1`

Method signatures are encoded in the same way, with the last nibble indicating the return type of the method. For example:

Nibble	Value	Description
0	0x1	`void`
1	0x0	`padding`

TABLE 6-20 Encoded method signature `()V`

Nibble	Value	Description
0	0x6	`reference`
1	<p1>	package token (high bit on)
2		
3	<c1>	class token
4		
5	0x4	`short`

TABLE 6-21 Encoded method signature `(Lp1.ci;)S`

CHAPTER 7

Java Card Virtual Machine Instruction Set

A Java Card virtual machine instruction consists of an opcode specifying the operation to be performed, followed by zero or more operands embodying values to be operated upon. This chapter gives details about the format of each Java Card virtual machine instruction and the operation it performs.

7.1 Assumptions: The Meaning of “Must”

The description of each instruction is always given in the context of Java Card virtual machine code that satisfies the static and structural constraints of Chapter 6, “The CAP File Format.”

In the description of individual Java Card virtual machine instructions, we frequently state that some situation “must” or “must not” be the case: “The *value2* must be of type `int`.” The constraints of Chapter 6, “The CAP File Format” guarantee that all such expectations will in fact be met. If some constraint (a “must” or “must not”) in an instruction description is not satisfied at run time, the behavior of the Java Card virtual machine is undefined.

7.2 Reserved Opcodes

In addition to the opcodes of the instructions specified later this chapter, which are used in Java Card `CAP` files (see Chapter 6, “The CAP File Format”), two opcodes are reserved for internal use by a Java Card virtual machine implementation. If Sun extends the instruction set of the Java Card virtual machine in the future, these reserved opcodes are guaranteed not to be used.

The two reserved opcodes, numbers 254 (0xfe) and 255 (0xff), have the mnemonics *impdep1* and *impdep2*, respectively. These instructions are intended to provide “back doors” or traps to implementation-specific functionality implemented in software and hardware, respectively.

Although these opcodes have been reserved, they may only be used inside a Java Card virtual machine implementation. They cannot appear in valid `CAP` files.

7.3 Virtual Machine Errors

A Java Card virtual machine may encounter internal errors or resource limitations that prevent it from executing correctly written Java programs. While the Java Virtual Machine Specification allows reporting and handling of virtual machine errors, it also states that they cannot ordinarily be handled by application code. This Java Card Virtual Machine Specification is more restrictive in that it does not allow for any reporting or handling of unrecoverable virtual machine errors at the application code level. A virtual machine error is considered unrecoverable if further execution could compromise the security or correct operation of the virtual machine or underlying system software. When an unrecoverable error occurs, the virtual machine will halt bytecode execution. Responses beyond halting the virtual machine are implementation-specific policies and are not mandated in this specification.

In the case where the virtual machine encounters a recoverable error, such as insufficient memory to allocate a new object, it will throw a `SystemException` with an error code describing the error condition. The Java Card Virtual Machine Specification cannot predict where resource limitations or internal errors may be encountered and does not mandate precisely when they can be reported. Thus, a `SystemException` may be thrown at any time during the operation of the Java Card virtual machine.

7.4 Security Exceptions

Instructions of the Java Card virtual machine throw an instance of the class `SecurityException` when a security violation has been detected. The Java Card virtual machine does not mandate the complete set of security violations that can or will result in an exception being thrown. However, there is a minimum set that must be supported.

In the general case, any instruction that de-references an object reference must throw a `SecurityException` if the context (§3.4) in which the instruction is executing is different than the owning context (§3.4) of the referenced object. The list of instructions includes the instance field get and put instructions, the array load and store instructions, as well as the *arraylength, invokeinterface, invokespecial, invokevirtual, checkcast, instanceof* and *athrow* instructions.

There are several exceptions to this general rule that allow cross-context use of objects or arrays. These exceptions are detailed in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*. An important detail to note is that any cross-context method invocation will result in a context switch (§3.4).

The Java Card virtual machine may also throw a `SecurityException` if an instruction violates any of the static constraints of Chapter 6, “The CAP File Format.” The Java Card Virtual Machine Specification does not mandate which instructions must implement these additional security checks, or to what level. Therefore, a `SecurityException` may be thrown at any time during the operation of the Java Card virtual machine.

7.5 The Java Card Virtual Machine Instruction Set

Java Virtual Machine instructions are represented in this chapter by entries of the form shown in the figure below, an example instruction page, in alphabetical order and each beginning on a new page.

mnemonic ***mnemonic***

Short description of the instruction

Format

mnemonic
operand1
operand2
…

Forms

mnemonic = opcode

Stack

…, *value1*, *value2* ⇒
…, *value3*

Description

A longer description detailing constraints on operand stack contents or constant pool entries, the operation performed, the type of the results, etc.

Runtime Exceptions

If any runtime exceptions can be thrown by the execution of an instruction they are set off one to a line, in the order in which they must be thrown.

Other than the runtime exceptions, if any, listed for an instruction, that instruction must not throw any runtime exceptions except for instances of `SystemException`.

Notes

Comments not strictly part of the specification of an instruction are set aside as notes at the end of the description.

FIGURE 7-1 An example instruction page

Each cell in the instruction format diagram represents a single 8-bit byte. The instruction's *mnemonic* is its name. Its opcode is its numeric representation and is given in both decimal and hexadecimal forms. Only the numeric representation is actually present in the Java Card virtual machine code in a `CAP` file.

Keep in mind that there are “operands” generated at compile time and embedded within Java Card virtual machine instructions, as well as “operands” calculated at run time and supplied on the operand stack. Although they are supplied from several different areas, all these operands represent the same thing: values to be operated upon by the Java Card virtual machine instruction being executed. By implicitly taking many of its operands from its operand stack, rather than representing them explicitly in its compiled code as additional operand bytes, register numbers, etc., the Java Card virtual machine’s code stays compact.

Some instructions are presented as members of a family of related instructions sharing a single description, format, and operand stack diagram. As such, a family of instructions includes several opcodes and opcode mnemonics; only the family mnemonic appears in the instruction format diagram, and a separate forms line lists all member mnemonics and opcodes. For example, the forms line for the *sconst_<s>* family of instructions, giving mnemonic and opcode information for the two instructions in that family (*sconst_0* and *sconst_1*), is

Forms *sconst_0* = 3 (0x3),
sconst_1 = 4 (0x4)

In the description of the Java Card virtual machine instructions, the effect of an instruction’s execution on the operand stack (§3.5) of the current frame (§3.5) is represented textually, with the stack growing from left to right and each word represented separately. Thus,

Stack…, *value1*, *value2* ⇒
…, *result*

shows an operation that begins by having a one-word *value2* on top of the operand stack with a one-word *value1* just beneath it. As a result of the execution of the instruction, *value1* and *value2* are popped from the operand stack and replaced by a one-word *result*, which has been calculated by the instruction. The remainder of the operand stack, represented by an ellipsis (…), is unaffected by the instruction’s execution.

The type `int` takes two words on the operand stack. In the operand stack representation, each word is represented separately using a dot notation:

Stack…, *value1.word1*, *value1.word2*, *value2.word1*, *value2.word2* ⇒
…, *result.word1*, *result.word2*

The Java Card Virtual Machine Specification does not mandate how the two words are used to represent the 32-bit `int` value; it only requires that a particular implementation be internally consistent.

aaload *aaload*

Load `reference` from array

Format

aaload

Forms

aaload = 36 (0x24)

Stack

..., arrayref, index ⇒
..., value

Description

The *arrayref* must be of type `reference` and must refer to an array whose components are of type `reference`. The *index* must be of type `short`. Both *arrayref* and *index* are popped from the operand stack. The `reference` *value* in the component of the array at *index* is retrieved and pushed onto the top of the operand stack.

Runtime Exceptions

If *arrayref* is `null`, *aaload* throws a `NullPointerException`.

Otherwise, if *index* is not within the bounds of the array referenced by *arrayref*, the *aaload* instruction throws an `ArrayIndexOutOfBoundsException`.

Notes

In some circumstances, the *aaload* instruction may throw a `SecurityException` if the current context (§3.4) is not the owning context (§3.4) of the array referenced by *arrayref*. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*.

aastore *aastore*

Store into `reference` array

Format

aastore

Forms

aastore = 55 (0x37)

Stack

..., arrayref, index, value ⇒
...

Description

The *arrayref* must be of type `reference` and must refer to an array whose components are of type `reference`. The *index* must be of type `short` and the *value* must be of type `reference`. The *arrayref*, *index* and *value* are popped from the operand stack. The `reference` *value* is stored as the component of the array at *index*.

The type of value must be assignment compatible with the type of the components of the array referenced by arrayref. Assignment of a value of reference type *S* (source) to a variable of reference type *T* (target) is allowed only when the type *S* supports all of the operations defined on type *T*. The detailed rules follow:

- If *S* is a class type, then:
  - If *T* is a class type, then *S* must be the same class as *T*, or *S* must be a subclass of *T*;
  - If *T* is an interface type, then *S* must implement interface *T*.
- If *S* is an interface type, then:
  - If *T* is a class type, then *T* must be `Object` (§2.2.2.4);
  - If *T* is an interface type, *T* must be the same interface as *S* or a superinterface of *S*.
- If *S* is an array type[1], namely the type *SC*`[]`, that is, an array of components of type *SC*, then:
  - If *T* is a class type, then *T* must be `Object`.
  - If *T* is an array type, namely the type *TC*`[]`, an array of components of type *TC*, then one of the following must be true:
    - *TC* and *SC* are the same primitive type (§3.1).
    - *TC* and *SC* are reference types (§3.1) with type *SC* assignable to *TC*, by these rules.

1. This version of the Java Card virtual machine specification does not allow for arrays of more than one dimension. Therefore, neither *S* or *T* can be an array type, and the rules for array types do not apply.

aastore (cont.) *aastore (cont.)*

- If *T* is an interface type, *T* must be one of the interfaces implemented by arrays[1].

Runtime Exceptions

If *arrayref* is `null`, *aastore* throws a `NullPointerException`.

Otherwise, if *index* is not within the bounds of the array referenced by *arrayref*, the *aastore* instruction throws an `ArrayIndexOutOfBoundsException`.

Otherwise, if *arrayref* is not `null` and the actual type of *value* is not assignment compatible with the actual type of the component of the array, *aastore* throws an `ArrayStoreException`.

Notes

In some circumstances, the *aastore* instruction may throw a `SecurityException` if the current context (§3.4) is not the owning context (§3.4) of the array referenced by *arrayref*. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*.

1. In the Java Card 2.1 API, arrays do not implement any interfaces. Therefore, *T* cannot be an interface type when *S* is an array type, and this rule does not apply.

aconst_null *aconst_null*

Push `null`

Format

aconst_null

Forms

aconst_null = 1 (0x1)

Stack

... ⇒
..., *null*

Description

Push the `null` object `reference` onto the operand stack.

aload *aload*

Load `reference` from local variable

Format

aload
index

Forms

aload = 21 (0x15)

Stack

… ⇒
…, *objectref*

Description

The *index* is an unsigned byte that must be a valid index into the local variables of the current frame (§3.5). The local variable at *index* must contain a `reference`. The *objectref* in the local variable at *index* is pushed onto the operand stack.

Notes

The *aload* instruction cannot be used to load a value of type `returnAddress` from a local variable onto the operand stack. This asymmetry with the *astore* instruction is intentional.

aload_<n> *aload_<n>*

Load `reference` from local variable

Format

aload_<n>

Forms

aload_0 = 24 (0x18)
aload_1 = 25 (0x19)
aload_2 = 26 (0x1a)
aload_3 = 27 (0x1b)

Stack

… ⇒
…, *objectref*

Description

The <*n*> must be a valid index into the local variables of the current frame (§3.5). The local variable at <*n*> must contain a `reference`. The *objectref* in the local variable at <*n*> is pushed onto the operand stack.

Notes

An *aload_*<*n*> instruction cannot be used to load a value of type `returnAddress` from a local variable onto the operand stack. This asymmetry with the corresponding *astore_*<*n*> instruction is intentional.

Each of the *aload_*<*n*> instructions is the same as *aload* with an *index* of <*n*>, except that the operand <*n*> is implicit.

anewarray *anewarray*

Create new array of `reference`

Format

anewarray
indexbyte1
indexbyte2

Forms

anewarray = 145 (0x91)

Stack

..., count ⇒
..., arrayref

Description

The *count* must be of type `short`. It is popped off the operand stack. The *count* represents the number of components of the array to be created. The unsigned *indexbyte1* and *indexbyte2* are used to construct an index into the constant pool of the current package (§3.5), where the value of the index is (*indexbyte1* << 8) | *indexbyte2*. The item at that index in the constant pool must be of type `CONSTANT_Classref` (§6.7.1), a reference to a class or interface type. The reference is resolved. A new array with components of that type, of length *count*, is allocated from the heap, and a `reference` *arrayref* to this new array object is pushed onto the operand stack. All components of the new array are initialized to `null`, the default value for `reference` types.

Runtime Exception

If *count* is less than zero, the *anewarray* instruction throws a `NegativeArraySizeException`.

areturn *areturn*

Return `reference` from method

Format

areturn

Forms

areturn = 119 (0x77)

Stack

…, *objectref* ⇒
[empty]

Description

The *objectref* must be of type `reference`. The *objectref* is popped from the operand stack of the current frame (§3.5) and pushed onto the operand stack of the frame of the invoker. Any other values on the operand stack of the current method are discarded.

The virtual machine then reinstates the frame of the invoker and returns control to the invoker.

arraylength *arraylength*

Get length of array

Format

arraylength

Forms

arraylength = 146 (0x92)

Stack

…, *arrayref* ⇒
…, *length*

Description

The *arrayref* must be of type `reference` and must refer to an array. It is popped from the operand stack. The *length* of the array it references is determined. That *length* is pushed onto the top of the operand stack as a `short`.

Runtime Exception

If *arrayref* is `null`, the *arraylength* instruction throws a `NullPointerException`.

Notes

In some circumstances, the *arraylength* instruction may throw a `SecurityException` if the current context (§3.4) is not the owning context (§3.4) of the array referenced by *arrayref*. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification.*

astore *astore*

Store `reference` into local variable

Format

astore
index

Forms

astore = 40 (0x28)

Stack

…, *objectref* ⇒
…

Description

The *index* is an unsigned byte that must be a valid index into the local variables of the current frame (§3.5). The *objectref* on the top of the operand stack must be of type `returnAddress` or of type `reference`. The *objectref* is popped from the operand stack, and the value of the local variable at *index* is set to *objectref*.

Notes

The *astore* instruction is used with an *objectref* of type `returnAddress` when implementing Java's `finally` keyword. The *aload* instruction cannot be used to load a value of type `returnAddress` from a local variable onto the operand stack. This asymmetry with the *astore* instruction is intentional.

astore_<n> *astore_<n>*

Store `reference` into local variable

Format

astore_<n>

Forms

astore_0 = 43 (0x2b)
astore_1 = 44 (0x2c)
astore_2 = 45 (0x2d)
astore_3 = 46 (0x2e)

Stack

…, *objectref* ⇒
…

Description

The <*n*> must be a valid index into the local variables of the current frame (§3.5). The *objectref* on the top of the operand stack must be of type `returnAddress` or of type `reference`. It is popped from the operand stack, and the value of the local variable at <*n*> is set to *objectref*.

Notes

An *astore_<n>* instruction is used with an *objectref* of type `returnAddress` when implementing Java's `finally` keyword. An *aload_<n>* instruction cannot be used to load a value of type `returnAddress` from a local variable onto the operand stack. This asymmetry with the corresponding *astore_<n>* instruction is intentional.

Each of the *aload_<n>* instructions is the same as *aload* with an *index* of <*n*>, except that the operand <*n*> is implicit.

athrow *athrow*

Throw exception or error

Format

athrow

Forms

athrow = 147 (0x93)

Stack

…, *objectref* ⇒
objectref

Description

The *objectref* must be of type `reference` and must refer to an object that is an instance of class `Throwable` or of a subclass of `Throwable`. It is popped from the operand stack. The *objectref* is then thrown by searching the current frame (§3.5) for the most recent `catch` clause that catches the class of *objectref* or one of its superclasses.

If a `catch` clause is found, it contains the location of the code intended to handle this exception. The `pc` register is reset to that location, the operand stack of the current frame is cleared, *objectref* is pushed back onto the operand stack, and execution continues. If no appropriate clause is found in the current frame, that frame is popped, the frame of its invoker is reinstated, and the *objectref* is rethrown.

If no `catch` clause is found that handles this exception, the virtual machine exits.

Runtime Exception

If *objectref* is `null`, *athrow* throws a `NullPointerException` instead of *objectref*.

Notes

In some circumstances, the *athrow* instruction may throw a `SecurityException` if the current context (§3.4) is not the owning context (§3.4) of the object referenced by *objectref*. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*.

baload *baload*

Load `byte` or `boolean` from array

Format

baload

Forms

baload = 37 (0x25)

Stack

..., arrayref, index ⇒
..., value

Description

The *arrayref* must be of type `reference` and must refer to an array whose components are of type `byte` or of type `boolean`. The *index* must be of type `short`. Both *arrayref* and *index* are popped from the operand stack. The `byte` *value* in the component of the array at *index* is retrieved, sign-extended to a `short` *value*, and pushed onto the top of the operand stack.

Runtime Exceptions

If *arrayref* is `null`, *baload* throws a `NullPointerException`.

Otherwise, if *index* is not within the bounds of the array referenced by *arrayref*, the *baload* instruction throws an `ArrayIndexOutOfBoundsException`.

Notes

In some circumstances, the *baload* instruction may throw a `SecurityException` if the current context (§3.4) is not the owning context (§3.4) of the array referenced by *arrayref*. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*.

bastore *bastore*

Store into `byte` or `boolean` array

Format

bastore

Forms

bastore = 56 (0x38)

Stack

…, *arrayref, index, value* ⇒
…

Description

The *arrayref* must be of type `reference` and must refer to an array whose components are of type `byte` or of type `boolean`. The *index* and *value* must both be of type `short`. The *arrayref, index* and *value* are popped from the operand stack. The `short` *value* is truncated to a `byte` and stored as the component of the array indexed by *index*.

Runtime Exceptions

If *arrayref* is `null`, *bastore* throws a `NullPointerException`.

Otherwise, if *index* is not within the bounds of the array referenced by *arrayref*, the *bastore* instruction throws an `ArrayIndexOutOfBoundsException`.

Notes

In some circumstances, the *bastore* instruction may throw a `SecurityException` if the current context (§3.4) is not the owning context (§3.4) of the array referenced by *arrayref*. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*.

bipush *bipush*

Push `byte`

Format

bipush
byte

Forms

bipush = 18 (0x12)

Stack

… ⇒
…, *value.word1*, *value.word2*

Description

The immediate *byte* is sign-extended to an `int`, and the resulting *value* is pushed onto the operand stack.

Notes

If a virtual machine does not support the `int` data type, the *bipush* instruction will not be available.

bspush *bspush*

Push `byte`

Format

bspush
byte

Forms

bspush = 16 (0x10)

Stack

... ⇒
..., *value*

Description

The immediate *byte* is sign-extended to a `short`, and the resulting *value* is pushed onto the operand stack.

checkcast *checkcast*

Check whether object is of given type

Format

checkcast
atype
indexbyte1
indexbyte2

Forms

checkcast = 148 (0x94)

Stack

…, *objectref* ⇒
…, *objectref*

Description

The unsigned byte *atype* is a code that indicates if the type against which the object is being checked is an array type or a class type. It must take one of the following values or zero:

Array Type	atype
`T_BOOLEAN`	`10`
`T_BYTE`	`11`
`T_SHORT`	`12`
`T_INT`	`13`
`T_REFERENCE`	`14`

If the value of *atype* is 10, 11, 12, or 13, the values of the *indexbyte1* and *indexbyte2* must be zero, and the value of *atype* indicates the array type against which to check the object. Otherwise the unsigned *indexbyte1* and *indexbyte2* are used to construct an index into the constant pool of the current package (§3.5), where the value of the index is (*indexbyte1* << 8) | *indexbyte2*. The item at that index in the constant pool must be of type `CONSTANT_Classref` (§6.7.1), a reference to a class or interface type. The reference is resolved. If the value of *atype* is 14, the object is checked against an array type that is an array of object references of the type of the resolved class. If the value of *atype* is zero, the object is checked against a class or interface type that is the resolved class.

The *objectref* must be of type `reference`. If *objectref* is `null` or can be cast to the specified array type or the resolved class or interface type, the operand stack is unchanged; otherwise the *checkcast* instruction throws a `ClassCastException`.

The following rules are used to determine whether an *objectref* that is not `null` can be cast to the resolved type: if *S* is the class of the object referred to by *objectref* and *T* is

checkcast (cont.) *checkcast (cont.)*

the resolved class, array or interface type, *checkcast* determines whether *objectref* can be cast to type *T* as follows:

- If *S* is a class type, then:
  - If *T* is a class type, then *S* must be the same class as *T*, or *S* must be a subclass of *T*;
  - If *T* is an interface type, then *S* must implement interface *T*.
- If *S* is an interface type, then:
  - If *T* is a class type, then *T* must be `Object` (§2.2.2.4);
  - If *T* is an interface type, *T* must be the same interface as *S* or a superinterface of *S*.
- If *S* is an array type, namely the type *SC*`[]`, that is, an array of components of type *SC*[1], then:
  - If *T* is a class type, then *T* must be `Object`.
  - If *T* is an array type, namely the type *TC*`[]`, an array of components of type *TC*, then one of the following must be true:
    - *TC* and *SC* are the same primitive type (§3.1).
    - *TC* and *SC* are reference types (§3.1) with type *SC* assignable to *TC*, by these rules.
  - If *T* is an interface type, *T* must be one of the interfaces implemented by arrays[2].

Runtime Exception

If *objectref* cannot be cast to the resolved class, array, or interface type, the *checkcast* instruction throws a `ClassCastException`.

Notes

The *checkcast* instruction is fundamentally very similar to the *instanceof* instruction. It differs in its treatment of `null`, its behavior when its test fails (*checkcast* throws an exception, *instanceof* pushes a result code), and its effect on the operand stack.

In some circumstances, the *checkcast* instruction may throw a `SecurityException` if the current context (§3.4) is not the owning context (§3.4) of the object referenced by *objectref*. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*.

---

1. This version of the Java Card virtual machine specification does not allow for arrays of more than one dimension. Therefore, neither *SC* or *TC* can be an array type.
2. In the Java Card 2.1 API, arrays do not implement any interfaces. Therefore, *T* cannot be an interface type when *S* is an array type, and this rule does not apply.

checkcast (cont.) *checkcast (cont.)*

If a virtual machine does not support the `int` data type, the value of *atype* may not be 13 (array type = `T_INT`).

dup *dup*

Duplicate top operand stack word

Format

dup

Forms

dup = 61 (0x3d)

Stack

…, *word* ⇒
…, *word*, *word*

Description

The top word on the operand stack is duplicated and pushed onto the operand stack.

The *dup* instruction must not be used unless *word* contains a 16-bit data type.

Notes

Except for restrictions preserving the integrity of 32-bit data types, the *dup* instruction operates on an untyped word, ignoring the type of data it contains.

dup_x *dup_x*

Duplicate top operand stack words and insert below

Format

dup_x
mn

Forms

dup_x = 63 (0x3f)

Stack

…, *wordN*, …, *wordM*, …, *word1* ⇒
…, *wordM*, …, *word1*, *wordN*, …, *wordM*, …, *word1*

Description

The unsigned byte *mn* is used to construct two parameter values. The high nibble, (*mn* & 0xf0) >> 4, is used as the value *m*. The low nibble, (*mn* & 0xf), is used as the value *n*. Permissible values for *m* are 1 through 4. Permissible values for *n* are 0 and *m* through *m*+4.

For positive values of *n*, the top *m* words on the operand stack are duplicated and the copied words are inserted *n* words down in the operand stack. When *n* equals 0, the top *m* words are copied and placed on top of the stack.

The *dup_x* instruction must not be used unless the ranges of words 1 through *m* and words *m*+1 through *n* each contain either a 16-bit data type, two 16-bit data types, a 32-bit data type, a 16-bit data type and a 32-bit data type (in either order), or two 32-bit data types.

Notes

Except for restrictions preserving the integrity of 32-bit data types, the *dup_x* instruction operates on untyped words, ignoring the types of data they contain.

If a virtual machine does not support the `int` data type, the permissible values for *m* are 1 or 2, and permissible values for *n* are 0 and *m* through *m*+2.

dup2 *dup2*

Duplicate top two operand stack words

Format

dup2

Forms

dup2 = 62 (0x3e)

Stack

…, *word2*, *word1* ⇒
…, *word2*, *word1*, *word2*, *word1*

Description

The top two words on the operand stack are duplicated and pushed onto the operand stack, in the original order.

The *dup2* instruction must not be used unless each of *word1* and *word2* is a word that contains a 16-bit data type or both together are the two words of a single 32-bit datum.

Notes

Except for restrictions preserving the integrity of 32-bit data types, the *dup2* instruction operates on untyped words, ignoring the types of data they contain.

getfield_<t> *getfield_<t>*

Fetch field from object

Format

getfield_<t>
index

Forms

getfield_a = 131 (0x83)
getfield_b = 132 (0x84)
getfield_s = 133 (0x85)
getfield_i = 134 (0x86)

Stack

…, *objectref* ⇒
…, *value*

OR

…, *objectref* ⇒
…, *value.word1*, *value.word2*

Description

The *objectref*, which must be of type `reference`, is popped from the operand stack. The unsigned *index* is used as an index into the constant pool of the current package (§3.5). The constant pool item at the index must be of type `CONSTANT_InstanceFieldref` (§6.7.2), a reference to a class and a field token. If the field is `protected`, then it must be either a member of the current class or a member of a superclass of the current class, and the class of *objectref* must be either the current class or a subclass of the current class.

The item must resolve to a field with a type that matches *t*, as follows:

- *a* field must be of type `reference`
- *b* field must be of type `byte` or type `boolean`
- *s* field must be of type `short`
- *i* field must be of type `int`

The width of a field in a class instance is determined by the field type specified in the instruction. The item is resolved, determining the field offset. The *value* at that offset into the class instance referenced by *objectref* is fetched. If the *value* is of type `byte` or type `boolean`, it is sign-extended to a short. The *value* is pushed onto the operand stack.

Runtime Exception

If *objectref* is `null`, the *getfield_<t>* instruction throws a `NullPointerException`.

getfield_<t> (cont.) *getfield_<t> (cont.)*

Notes

In some circumstances, the *getfield_<t>* instruction may throw a `SecurityException` if the current context (§3.4) is not the owning context (§3.4) of the object referenced by *objectref*. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*.

If a virtual machine does not support the `int` data type, the *getfield_i* instruction will not be available.

getfield_<t>_this *getfield_<t>_this*

Fetch field from current object

Format

getfield_<t>_this
index

Forms

getfield_a_this = 173 (0xad)
getfield_b_this = 174 (0xae)
getfield_s_this = 175 (0xaf)
getfield_i_this = 176 (0xb0)

Stack

... ⇒
..., value

OR

... ⇒
..., value.word1, value.word2

Description

The currently executing method must be an instance method. The local variable at index 0 must contain a `reference` *objectref* to the currently executing method's `this` parameter. The unsigned *index* is used as an index into the constant pool of the current package (§3.5). The constant pool item at the index must be of type `CONSTANT_InstanceFieldref` (§6.7.2), a reference to a class and a field token. If the field is `protected`, then it must be either a member of the current class or a member of a superclass of the current class, and the class of *objectref* must be either the current class or a subclass of the current class.

The item must resolve to a field with a type that matches *t*, as follows:

- *a* field must be of type `reference`
- *b* field must be of type `byte` or type `boolean`
- *s* field must be of type `short`
- *i* field must be of type `int`

The width of a field in a class instance is determined by the field type specified in the instruction. The item is resolved, determining the field offset. The *value* at that offset into the class instance referenced by *objectref* is fetched. If the *value* is of type `byte` or type `boolean`, it is sign-extended to a short. The *value* is pushed onto the operand stack.

getfield_<t>_this (cont.) *getfield_<t>_this (cont.)*

Runtime Exception

If *objectref* is `null`, the *getfield_<t>_this* instruction throws a `NullPointerException`.

Notes

In some circumstances, the *getfield_<t>_this* instruction may throw a `SecurityException` if the current context (§3.4) is not the owning context (§3.4) of the object referenced by *objectref*. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*.

If a virtual machine does not support the `int` data type, the *getfield_i_this* instruction will not be available.

getfield_<t>_w *getfield_<t>_w*

Fetch field from object (wide index)

Format

getfield_<t>_w
indexbyte1
indexbyte2

Forms

getfield_a_w = 169 (0xa9)
getfield_b_w = 170 (0xaa)
getfield_s_w = 171 (0xab)
getfield_i_w = 172 (0xac)

Stack

…, *objectref* ⇒
…, *value*

OR

…, *objectref* ⇒
…, *value.word1*, *value.word2*

Description

The *objectref*, which must be of type `reference`, is popped from the operand stack. The unsigned *indexbyte1* and *indexbyte2* are used to construct an index into the constant pool of the current package (§3.5), where the value of the index is (*indexbyte1* << 8) | *indexbyte2*. The constant pool item at the index must be of type `CONSTANT_InstanceFieldref` (§6.7.2), a reference to a class and a field token. The item must resolve to a field of type `reference`. If the field is `protected`, then it must be either a member of the current class or a member of a superclass of the current class, and the class of *objectref* must be either the current class or a subclass of the current class.

The item must resolve to a field with a type that matches *t*, as follows:

- *a* field must be of type `reference`
- *b* field must be of type `byte` or type `boolean`
- *s* field must be of type `short`
- *i* field must be of type `int`

The width of a field in a class instance is determined by the field type specified in the instruction. The item is resolved, determining the field offset. The *value* at that offset into the class instance referenced by *objectref* is fetched. If the *value* is of type `byte` or type `boolean`, it is sign-extended to a short. The *value* is pushed onto the operand stack.

getfield_<t>_w (cont.) *getfield_<t>_w (cont.)*

Runtime Exception

If *objectref* is `null`, the *getfield_<t>_w* instruction throws a `NullPointerException`.

Notes

In some circumstances, the *getfield_<t>_w* instruction may throw a `SecurityException` if the current context (§3.4) is not the owning context (§3.4) of the object referenced by *objectref*. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*.

If a virtual machine does not support the `int` data type, the *getfield_i_w* instruction will not be available.

getstatic_<t> *getstatic_<t>*

Get `static` field from class

Format

getstatic_<t>
indexbyte1
indexbyte2

Forms

getstatic_a = 123 (0x7b)
getstatic_b = 124 (0x7c)
getstatic_s = 125 (0x7d)
getstatic_i = 126 (0x7e)

Stack

… ⇒
…, *value*

OR

… ⇒
…, *value.word1*, *value.word2*

Description

The unsigned *indexbyte1* and *indexbyte2* are used to construct an index into the constant pool of the current package (§3.5), where the value of the index is (*indexbyte1* << 8) | *indexbyte2*. The constant pool item at the index must be of type `CONSTANT_StaticFieldref` (§6.7.3), a reference to a static field. If the field is `protected`, then it must be either a member of the current class or a member of a superclass of the current class.

The item must resolve to a field with a type that matches *t*, as follows:

- *a* field must be of type `reference`
- *b* field must be of type `byte` or type `boolean`
- *s* field must be of type `short`
- *i* field must be of type `int`

The width of a class field is determined by the field type specified in the instruction. The item is resolved, determining the field offset. The item is resolved, determining the class field. The *value* of the class field is fetched. If the *value* is of type `byte` or `boolean`, it is sign-extended to a `short`. The *value* is pushed onto the operand stack.

Notes

If a virtual machine does not support the `int` data type, the *getstatic_i* instruction will not be available.

goto *goto*

Branch always

Format

goto
branch

Forms

goto = 112 (0x70)

Stack

No change

Description

The value *branch* is used as a signed 8-bit offset. Execution proceeds at that offset from the address of the opcode of this *goto* instruction. The target address must be that of an opcode of an instruction within the method that contains this *goto* instruction.

goto_w *goto_w*

Branch always (wide index)

Format

goto_w
branchbyte1
branchbyte2

Forms

goto_w = 168 (0xa8)

Stack

No change

Description

The unsigned bytes *branchbyte1* and *branchbyte2* are used to construct a signed 16-bit *branchoffset*, where *branchoffset* is (*branchbyte1* << 8) | *branchbyte2*. Execution proceeds at that offset from the address of the opcode of this *goto* instruction. The target address must be that of an opcode of an instruction within the method that contains this *goto* instruction.

i2b *i2b*

Convert `int` to `byte`

Format

i2b

Forms

i2b = 93 (0x5d)

Stack

…, *value.word1*, *value.word2* ⇒
…, *result*

Description

The *value* on top of the operand stack must be of type `int`. It is popped from the operand stack and converted to a `byte` *result* by taking the low-order 16 bits of the `int` value, and discarding the high-order 16 bits. The low-order word is truncated to a `byte`, then sign-extended to a `short` *result*. The *result* is pushed onto the operand stack.

Notes

The *i2b* instruction performs a narrowing primitive conversion. It may lose information about the overall magnitude of *value*. The *result* may also not have the same sign as *value*.

If a virtual machine does not support the `int` data type, the *i2b* instruction will not be available.

i2s *i2s*

Convert `int` to `short`

Format

i2s

Forms

i2s = 94 (0x5e)

Stack

..., value.word1, value.word2 ⇒
..., result

Description

The *value* on top of the operand stack must be of type `int`. It is popped from the operand stack and converted to a `short` *result* by taking the low-order 16 bits of the `int` value and discarding the high-order 16 bits. The *result* is pushed onto the operand stack.

Notes

The *i2s* instruction performs a narrowing primitive conversion. It may lose information about the overall magnitude of *value*. The *result* may also not have the same sign as *value*.

If a virtual machine does not support the `int` data type, the *i2s* instruction will not be available.

iadd *iadd*

Add `int`

Format

iadd

Forms

iadd = 66 (0x42)

Stack

…, *value1.word1, value1.word2, value2.word1, value2.word2* ⇒
…, *result.word1, result.word2*

Description

Both *value1* and *value2* must be of type `int`. The values are popped from the operand stack. The `int` *result* is *value1* + *value2*. The *result* is pushed onto the operand stack.

If an i*add* instruction overflows, then the result is the low-order bits of the true mathematical result in a sufficiently wide two's-complement format. If overflow occurs, then the sign of the result may not be the same as the sign of the mathematical sum of the two values.

Notes

If a virtual machine does not support the `int` data type, the *iadd* instruction will not be available.

iaload *iaload*

Load `int` from array

Format

iaload

Forms

iaload = 39 (0x27)

Stack

..., arrayref, index ⇒
..., value.word1, value.word2

Description

The *arrayref* must be of type `reference` and must refer to an array whose components are of type `int`. The *index* must be of type `short`. Both *arrayref* and *index* are popped from the operand stack. The `int` *value* in the component of the array at *index* is retrieved and pushed onto the top of the operand stack.

Runtime Exceptions

If *arrayref* is `null`, *iaload* throws a `NullPointerException`.

Otherwise, if *index* is not within the bounds of the array referenced by *arrayref*, the *iaload* instruction throws an `ArrayIndexOutOfBoundsException`.

Notes

In some circumstances, the *iaload* instruction may throw a `SecurityException` if the current context (§3.4) is not the owning context (§3.4) of the array referenced by *arrayref*. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*.

If a virtual machine does not support the `int` data type, the *iaload* instruction will not be available.

iand *iand*

Boolean AND `int`

Format

iand

Forms

iand = 84 (0x54)

Stack

…, *value1.word1, value1.word2, value2.word1, value2.word2* ⇒
…, *result.word1, result.word2*

Description

Both *value1* and *value2* must be of type `int`. They are popped from the operand stack. An `int` *result* is calculated by taking the bitwise AND (conjunction) of *value1* and *value2*. The *result* is pushed onto the operand stack.

Notes

If a virtual machine does not support the `int` data type, the *iand* instruction will not be available.

iastore *iastore*

Store into `int` array

Format

iastore

Forms

iastore = 58 (0x3a)

Stack

..., arrayref, index, value.word1, value.word2 ⇒
...

Description

The *arrayref* must be of type `reference` and must refer to an array whose components are of type `int`. The *index* must be of type `short` and *value* must be of type `int`. The *arrayref*, *index* and *value* are popped from the operand stack. The `int` *value* is stored as the component of the array indexed by *index*.

Runtime Exception

If *arrayref* is `null`, *iastore* throws a `NullPointerException`.

Otherwise, if *index* is not within the bounds of the array referenced by *arrayref*, the *iastore* instruction throws an `ArrayIndexOutOfBoundsException`.

Notes

In some circumstances, the *iastore* instruction may throw a `SecurityException` if the current context (§3.4) is not the owning context (§3.4) of the array referenced by *arrayref*. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*.

If a virtual machine does not support the `int` data type, the *iastore* instruction will not be available.

icmp *icmp*

Compare `int`

Format

icmp

Forms

icmp = 95 (0x5f)

Stack

…, *value1.word1, value1.word2, value2.word1, value2.word2* ⇒
…, *result*

Description

Both *value1* and *value2* must be of type `int`. They are both popped from the operand stack, and a signed integer comparison is performed. If *value1* is greater than *value2*, the `short` value 1 is pushed onto the operand stack. If *value1* is equal to *value2*, the `short` value 0 is pushed onto the operand stack. If *value1* is less than *value2*, the `short` value –1 is pushed onto the operand stack.

Notes

If a virtual machine does not support the `int` data type, the *icmp* instruction will not be available.

iconst_<i> *iconst_<i>*

Push `int` constant

Format

iconst_<i>

Forms

iconst_m1 = 10 (0x09)
iconst_0 = 11 (0xa)
i*const_1* = 12 (0xb)
i*const_2* = 13 (0xc)
i*const_3* = 14 (0xd)
i*const_4* = 15 (0xe)
i*const_5* = 16 (0xf)

Stack

… ⇒
…, *<i>.word1*, *<i>.word2*

Description

Push the `int` constant *<i>* (*-1*, *0*, *1*, *2*, *3*, *4*, or *5*) onto the operand stack.

Notes

If a virtual machine does not support the `int` data type, the *iconst_<i>* instruction will not be available.

idiv *idiv*

Divide `int`

Format

idiv

Forms

idiv = 72 (0x48)

Stack

..., value1.word1, value1.word2, value2.word1, value2.word2 ⇒
..., result.word1, result.word2

Description

Both *value1* and *value2* must be of type `int`. The values are popped from the operand stack. The `int` *result* is the value of the Java expression *value1* / *value2*. The *result* is pushed onto the operand stack.

An `int` division rounds towards 0; that is, the quotient produced for `int` values in *n/d* is an `int` value *q* whose magnitude is as large as possible while satisfying $|d \cdot q| = |n|$. Moreover, *q* is a positive when $|n| = |d|$ and *n* and *d* have the same sign, but *q* is negative when $|n| = |d|$ and *n* and *d* have opposite signs.

There is one special case that does not satisfy this rule: if the dividend is the negative integer of the largest possible magnitude for the `int` type, and the divisor is *–1*, then overflow occurs, and the result is equal to the dividend. Despite the overflow, no exception is thrown in this case.

Runtime Exception

If the value of the divisor in an `int` division is 0, *idiv* throws an `ArithmeticException`.

Notes

If a virtual machine does not support the `int` data type, the *idiv* instruction will not be available.

if_acmp<cond> *if_acmp<cond>*

Branch if `reference` comparison succeeds

Format

if_acmp<cond>
branch

Forms

if_acmpeq = 104 (0x68)
if_acmpne = 105 (0x69)

Stack

..., value1, value2 ⇒
...

Description

Both *value1* and *value2* must be of type `reference`. They are both popped from the operand stack and compared. The results of the comparisons are as follows:

- *eq* succeeds if and only if *value1* = *value2*
- *ne* succeeds if and only if *value1* ≠ *value2*

If the comparison succeeds, *branch* is used as signed 8-bit offset, and execution proceeds at that offset from the address of the opcode of this *if_acmp<cond>* instruction. The target address must be that of an opcode of an instruction within the method that contains this *if_acmp<cond>* instruction.

Otherwise, execution proceeds at the address of the instruction following this *if_acmp<cond>* instruction.

if_acmp<cond>_w *if_acmp<cond>_w*

Branch if `reference` comparison succeeds (wide index)

Format

if_acmp<cond>_w
branchbyte1
branchbyte2

Forms

if_acmpeq_w = 160 (0xa0)
if_acmpne_w = 161 (0xa1)

Stack

..., value1, value2 ⇒
...

Description

Both *value1* and *value2* must be of type `reference`. They are both popped from the operand stack and compared. The results of the comparisons are as follows:

- *eq* succeeds if and only if *value1* = *value2*
- *ne* succeeds if and only if *value1* ≠ *value2*

If the comparison succeeds, the unsigned bytes *branchbyte1* and *branchbyte2* are used to construct a signed 16-bit *branchoffset*, where *branchoffset* is (*branchbyte1* << 8) | *branchbyte2*. Execution proceeds at that offset from the address of the opcode of this *if_acmp<cond>_w* instruction. The target address must be that of an opcode of an instruction within the method that contains this *if_acmp<cond>_w* instruction.

Otherwise, execution proceeds at the address of the instruction following this *if_acmp<cond>_w* instruction.

if_scmp<cond> *if_scmp<cond>*

Branch if `short` comparison succeeds

Format

if_scmp<cond>
branch

Forms

if_scmpeq = 106 (0x6a)
if_scmpne = 107 (0x6b)
if_scmplt = 108 (0x6c)
if_scmpge = 109 (0x6d)
if_scmpgt = 110 (0x6e)
if_scmple = 111 (0x6f)

Stack

…, *value1*, *value2* ⇒
…

Description

Both *value1* and *value2* must be of type `short`. They are both popped from the operand stack and compared. All comparisons are signed. The results of the comparisons are as follows:

- *eq* succeeds if and only if *value1* = *value2*
- *ne* succeeds if and only if *value1* ≠ *value2*
- *lt* succeeds if and only if *value1* < *value2*
- *le* succeeds if and only if *value1* ≤ *value2*
- *gt* succeeds if and only if *value1* > *value2*
- *ge* succeeds if and only if *value1* ≥ *value2*

If the comparison succeeds, *branch* is used as signed 8-bit offset, and execution proceeds at that offset from the address of the opcode of this *if_scmp<cond>* instruction. The target address must be that of an opcode of an instruction within the method that contains this *if_scmp<cond>* instruction.

Otherwise, execution proceeds at the address of the instruction following this *if_scmp<cond>* instruction.

if_scmp<cond>_w *if_scmp<cond>_w*

Branch if `short` comparison succeeds (wide index)

Format

if_scmp<cond>_w
branchbyte1
branchbyte2

Forms

if_scmpeq_w = 162 (0xa2)
if_scmpne_w = 163 (0xa3)
if_scmplt_w = 164 (0xa4)
if_scmpge_w = 165 (0xa5)
if_scmpgt_w = 166 (0xa6)
if_scmple_w = 167 (0xa7)

Stack

..., value1, value2 ⇒
...

Description

Both *value1* and *value2* must be of type `short`. They are both popped from the operand stack and compared. All comparisons are signed. The results of the comparisons are as follows:

- *eq* succeeds if and only if *value1* = *value2*
- *ne* succeeds if and only if *value1* ≠ *value2*
- *lt* succeeds if and only if *value1* < *value2*
- *le* succeeds if and only if *value1* ≤ *value2*
- *gt* succeeds if and only if *value1* > *value2*
- *ge* succeeds if and only if *value1* ≥ *value2*

If the comparison succeeds, the unsigned bytes *branchbyte1* and *branchbyte2* are used to construct a signed 16-bit *branchoffset*, where *branchoffset* is (*branchbyte1* << 8) | *branchbyte2*. Execution proceeds at that offset from the address of the opcode of this *if_scmp<cond>_w* instruction. The target address must be that of an opcode of an instruction within the method that contains this *if_scmp<cond>_w* instruction.

Otherwise, execution proceeds at the address of the instruction following this *if_scmp<cond>_w* instruction.

if<cond> *if<cond>*

Branch if `short` comparison with zero succeeds

Format

if<cond>
branch

Forms

ifeq = 96 (0x60)
ifne = 97 (0x61)
iflt = 98 (0x62)
ifge = 99 (0x63)
ifgt = 100 (0x64)
ifle = 101 (0x65)

Stack

…, *value* ⇒
…

Description

The *value* must be of type `short`. It is popped from the operand stack and compared against zero. All comparisons are signed. The results of the comparisons are as follows:

- *eq* succeeds if and only if *value* = 0
- *ne* succeeds if and only if *value* ≠ 0
- *lt* succeeds if and only if *value* < 0
- *le* succeeds if and only if *value* ≤ 0
- *gt* succeeds if and only if *value* > 0
- *ge* succeeds if and only if *value* ≥ 0

If the comparison succeeds, *branch* is used as signed 8-bit offset, and execution proceeds at that offset from the address of the opcode of this *if<cond>* instruction. The target address must be that of an opcode of an instruction within the method that contains this *if<cond>* instruction.

Otherwise, execution proceeds at the address of the instruction following this *if<cond>* instruction.

if<cond>_w *if<cond>_w*

Branch if `short` comparison with zero succeeds (wide index)

Format

if<cond>_w
branchbyte1
branchbyte2

Forms

ifeq_w = 152 (0x98)
ifne_w = 153 (0x99)
iflt_w = 154 (0x9a)
ifge_w = 155 (0x9b)
ifgt_w = 156 (0x9c)
ifle_w = 157 (0x9d)

Stack

…, *value* ⇒
…

Description

The *value* must be of type `short`. It is popped from the operand stack and compared against zero. All comparisons are signed. The results of the comparisons are as follows:

- *eq* succeeds if and only if *value* = 0
- *ne* succeeds if and only if *value* ≠ 0
- *lt* succeeds if and only if *value* < 0
- *le* succeeds if and only if *value* ≤ 0
- *gt* succeeds if and only if *value* > 0
- *ge* succeeds if and only if *value* ≥ 0

If the comparison succeeds, the unsigned bytes *branchbyte1* and *branchbyte2* are used to construct a signed 16-bit *branchoffset*, where *branchoffset* is (*branchbyte1* << 8) | *branchbyte2*. Execution proceeds at that offset from the address of the opcode of this *if<cond>_w* instruction. The target address must be that of an opcode of an instruction within the method that contains this *if<cond>_w* instruction.

Otherwise, execution proceeds at the address of the instruction following this *if<cond>_w* instruction.

ifnonnull *ifnonnull*

Branch if `reference` not `null`

Format

ifnonnull
branch

Forms

ifnonnull = 103 (0x67)

Stack

…, *value* ⇒
…

Description

The *value* must be of type `reference`. It is popped from the operand stack. If the *value* is not `null`, *branch* is used as signed 8-bit offset, and execution proceeds at that offset from the address of the opcode of this *ifnonnull* instruction. The target address must be that of an opcode of an instruction within the method that contains this *ifnonnull* instruction.

Otherwise, execution proceeds at the address of the instruction following this *ifnonnull* instruction.

ifnonnull_w *ifnonnull_w*

Branch if `reference` not `null` (wide index)

Format

ifnonnull_w
branchbyte1
branchbyte2

Forms

ifnonnull_w = 159 (0x9f)

Stack

..., value ⇒
...

Description

The *value* must be of type `reference`. It is popped from the operand stack. If the *value* is not `null`, the unsigned bytes *branchbyte1* and *branchbyte2* are used to construct a signed 16-bit *branchoffset*, where *branchoffset* is (*branchbyte1* << 8) | *branchbyte2*. Execution proceeds at that offset from the address of the opcode of this *ifnonnull_w* instruction. The target address must be that of an opcode of an instruction within the method that contains this *ifnonnull_w* instruction.

Otherwise, execution proceeds at the address of the instruction following this *ifnonnull_w* instruction.

ifnull *ifnull*

Branch if `reference` is `null`

Format

ifnull
branch

Forms

ifnull = 102 (0x66)

Stack

…, *value* ⇒
…

Description

The *value* must be of type `reference`. It is popped from the operand stack. If the *value* is `null`, *branch* is used as signed 8-bit offset, and execution proceeds at that offset from the address of the opcode of this *ifnull* instruction. The target address must be that of an opcode of an instruction within the method that contains this *ifnull* instruction.

Otherwise, execution proceeds at the address of the instruction following this *ifnull* instruction.

ifnull_w *ifnull_w*

Branch if `reference` is `null` (wide index)

Format

ifnull_w
branchbyte1
branchbyte2

Forms

ifnull_w = 158 (0x9e)

Stack

..., value ⇒
...

Description

The *value* must be of type `reference`. It is popped from the operand stack. If the *value* is `null`, the unsigned bytes *branchbyte1* and *branchbyte2* are used to construct a signed 16-bit *branchoffset*, where *branchoffset* is (*branchbyte1* << 8) | *branchbyte2*. Execution proceeds at that offset from the address of the opcode of this *ifnull_w* instruction. The target address must be that of an opcode of an instruction within the method that contains this *ifnull_w* instruction.

Otherwise, execution proceeds at the address of the instruction following this *ifnull_w* instruction.

iinc *iinc*

Increment local `int` variable by constant

Format

iinc
index
const

Forms

iinc = 90 (0x5a)

Stack

No change

Description

The *index* is an unsigned byte. Both *index* and *index* + 1 must be valid indices into the local variables of the current frame (§3.5). The local variables at *index* and *index* + 1 together must contain an `int`. The *const* is an immediate signed byte. The value *const* is first sign-extended to an `int`, then the `int` contained in the local variables at *index* and *index* + 1 is incremented by that amount.

Notes

If a virtual machine does not support the `int` data type, the *iinc* instruction will not be available.

iinc_w *iinc_w*

Increment local `int` variable by constant

Format

iinc_w
index
byte1
byte2

Forms

iinc_w = 151 (0x97)

Stack

No change

Description

The *index* is an unsigned byte. Both *index* and *index* + 1 must be valid indices into the local variables of the current frame (§3.5). The local variables at *index* and *index* + 1 together must contain an `int`. The immediate unsigned *byte1* and *byte2* values are assembled into an intermediate `short` where the value of the short is (*byte1* << 8) | *byte2*. The intermediate value is then sign-extended to an `int` *const*. The `int` contained in the local variables at *index* and *index* + 1 is incremented by *const*.

Notes

If a virtual machine does not support the `int` data type, the *iinc_w* instruction will not be available.

iipush *iipush*

Push `int`

Format

iipush
byte1
byte2
byte3
byte4

Forms

iipush = 20 (0x14)

Stack

... ⇒
..., *value1.word1*, *value1.word2*

Description

The immediate unsigned *byte1*, *byte2*, *byte3*, and *byte4* values are assembled into a signed `int` where the value of the int is (*byte1* << 24) | (*byte2* << 16) | (*byte3* << 8) | *byte4*. The resulting *value* is pushed onto the operand stack.

Notes

If a virtual machine does not support the `int` data type, the *iipush* instruction will not be available.

iload *iload*

Load `int` from local variable

Format

iload
index

Forms

iload = 23 (0x17)

Stack

… ⇒
…, *value1.word1*, *value1.word2*

Description

The *index* is an unsigned byte. Both *index* and *index* + 1 must be valid indices into the local variables of the current frame (§3.5). The local variables at *index* and *index* + 1 together must contain an `int`. The *value* of the local variables at *index* and *index* + 1 is pushed onto the operand stack.

Notes

If a virtual machine does not support the `int` data type, the *iload* instruction will not be available.

iload_<n> *iload_<n>*

Load `int` from local variable

Format

iload_<n>

Forms

iload_0 = 32 (0x20)
i*load_1* = 33 (0x21)
i*load_2* = 34 (0x22)
i*load_3* = 35 (0x23)

Stack

... ⇒
..., *value1.word1, value1.word2*

Description

Both <*n*> and <*n*> + 1 must be a valid indices into the local variables of the current frame (§3.5). The local variables at <*n*> and <*n*> + 1 together must contain an `int`. The *value* of the local variables at <*n*> and <*n*> + 1 is pushed onto the operand stack.

Notes

Each of the *iload_<n>* instructions is the same as *iload* with an *index* of <*n*>, except that the operand <*n*> is implicit.

If a virtual machine does not support the `int` data type, the *iload_<n>* instruction will not be available.

ilookupswitch *ilookupswitch*

Access jump table by key match and jump

Format

ilookupswitch
defaultbyte1
defaultbyte2
npairs1
npairs2
match-offset pairs…

Pair Format

matchbyte1
matchbyte2
matchbyte3
matchbyte4
offsetbyte1
offsetbyte2

Forms

ilookupswitch = 118 (0x76)

Stack

…, *key.word1*, *key.word2* ⇒
…

Description

An *ilookupswitch* instruction is a variable-length instruction. Immediately after the *ilookupswitch* opcode follow a signed 16-bit value *default*, an unsigned 16-bit value *npairs*, and then *npairs* pairs. Each pair consists of an `int` *match* and a signed 16-bit *offset*. Each *match* is constructed from four unsigned bytes as (*matchbyte1* << 24) | (*matchbyte2* << 16) | (*matchbyte3* << 8) | *matchbyte4*. Each *offset* is constructed from two unsigned bytes as (*offsetbyte1* << 8) | *offsetbyte2*.

The table *match-offset* pairs of the *ilookupswitch* instruction must be sorted in increasing numerical order by *match*.

The *key* must be of type `int` and is popped from the operand stack and compared against the *match* values. If it is equal to one of them, then a target address is calculated by adding the corresponding *offset* to the address of the opcode of this *ilookupswitch* instruction. If the *key* does not match any of the *match* values, the target address is calculated by adding *default* to the address of the opcode of this *ilookupswitch* instruction. Execution then continues at the target address.

ilookupswitch (cont.) *ilookupswitch (cont.)*

The target address that can be calculated from the offset of each *match-offset* pair, as well as the one calculated from *default*, must be the address of an opcode of an instruction within the method that contains this *ilookupswitch* instruction.

Notes

The *match-offset* pairs are sorted to support lookup routines that are quicker than linear search.

If a virtual machine does not support the `int` data type, the *ilookupswitch* instruction will not be available.

imul *imul*

Multiply `int`

Format

imul

Forms

imul = 70 (0x46)

Stack

…, *value1.word1, value1.word2, value2.word1, value2.word2* ⇒
…, *result.word1, result.word2*

Description

Both *value1* and *value2* must be of type `int`. The values are popped from the operand stack. The `int` *result* is *value1* * *value2*. The *result* is pushed onto the operand stack.

If an *imul* instruction overflows, then the result is the low-order bits of the mathematical product as an `int`. If overflow occurs, then the sign of the result may not be the same as the sign of the mathematical product of the two values.

Notes

If a virtual machine does not support the `int` data type, the *imul* instruction will not be available.

ineg *ineg*

Negate `int`

Format

ineg

Forms

ineg = 76 (0x4c)

Stack

..., value.word1, value.word2 ⇒
..., result.word1, result.word2

Description

The *value* must be of type `int`. It is popped from the operand stack. The `int` *result* is the arithmetic negation of *value*, *-value*. The *result* is pushed onto the operand stack.

For `int` values, negation is the same as subtraction from zero. Because the Java Card virtual machine uses two's-complement representation for integers and the range of two's-complement values is not symmetric, the negation of the maximum negative `int` results in that same maximum negative number. Despite the fact that overflow has occurred, no exception is thrown.

For all `int` values `x`, `-x` equals `(~x) + 1`.

Notes

If a virtual machine does not support the `int` data type, the *imul* instruction will not be available.

instanceof *instanceof*

Determine if object is of given type

Format

instanceof
atype
indexbyte1
indexbyte2

Forms

instanceof = 149 (0x95)

Stack

…, *objectref* ⇒
…, *result*

Description

The unsigned byte *atype* is a code that indicates if the type against which the object is being checked is an array type or a class type. It must take one of the following values or zero:

Array Type	atype
`T_BOOLEAN`	`10`
`T_BYTE`	`11`
`T_SHORT`	`12`
`T_INT`	`13`
`T_REFERENCE`	`14`

If the value of *atype* is 10, 11, 12, or 13, the values of the *indexbyte1* and *indexbyte2* must be zero, and the value of *atype* indicates the array type against which to check the object. Otherwise the unsigned *indexbyte1* and *indexbyte2* are used to construct an index into the constant pool of the current package (§3.5), where the value of the index is (*indexbyte1* << 8) | *indexbyte2*. The item at that index in the constant pool must be of type `CONSTANT_Classref` (§6.7.1), a reference to a class or interface type. The reference is resolved. If the value of *atype* is 14, the object is checked against an array type that is an array of object references of the type of the resolved class. If the value of *atype* is zero, the object is checked against a class or interface type that is the resolved class.

The *objectref* must be of type `reference`. It is popped from the operand stack. If *objectref* is not `null` and is an instance of the resolved class, array or interface, the *instanceof* instruction pushes a `short` *result* of *1* on the operand stack. Otherwise it pushes a `short` *result* of *0*.

instanceof (cont.) *instanceof (cont.)*

The following rules are used to determine whether an *objectref* that is not `null` is an instance of the resolved type: if *S* is the class of the object referred to by *objectref* and *T* is the resolved class, array or interface type, *instanceof* determines whether *objectref* is an instance of *T* as follows:

- If *S* is a class type, then:
  - If *T* is a class type, then *S* must be the same class as *T*, or *S* must be a subclass of *T*;
  - If *T* is an interface type, then *S* must implement interface *T*.
- If *S* is an interface type, then:
  - If *T* is a class type, then *T* must be `Object` (§2.2.2.4);
  - If *T* is an interface type, *T* must be the same interface as *S* or a superinterface of *S*.
- If *S* is an array type, namely the type *SC*`[]`, that is, an array of components of type *SC*[1], then:
  - If *T* is a class type, then *T* must be `Object`.
  - If *T* is an array type, namely the type *TC*`[]`, an array of components of type *TC*, then one of the following must be true:
    - *TC* and *SC* are the same primitive type (§3.1).
    - *TC* and *SC* are reference types (§3.1) with type *SC* assignable to *TC*, by these rules.
  - If *T* is an interface type, *T* must be one of the interfaces implemented by arrays[2].

Notes

The *instanceof* instruction is fundamentally very similar to the *checkcast* instruction. It differs in its treatment of `null`, its behavior when its test fails (*checkcast* throws an exception, *instanceof* pushes a result code), and its effect on the operand stack.

In some circumstances, the *instanceof* instruction may throw a `SecurityException` if the current context (§3.4) is not the owning context (§3.4) of the object referenced by *objectref*. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*.

If a virtual machine does not support the `int` data type, the value of *atype* may not be 13 (array type = `T_INT`).

---

1. This version of the Java Card virtual machine specification does not allow for arrays of more than one dimension. Therefore, neither *SC* or *TC* can be an array type.
2. In the Java Card 2.1 API, arrays do not implement any interfaces. Therefore, *T* cannot be an interface type when *S* is an array type, and this rule does not apply.

invokeinterface *invokeinterface*

Invoke interface method

Format

invokeinterface
nargs
indexbyte1
indexbyte2
method

Forms

invokeinterface = 142 (0x8e)

Stack

…, *objectref*, [*arg1*, [*arg2* …]] ⇒
…

Description

The unsigned *indexbyte1* and *indexbyte2* are used to construct an index into the constant pool of the current package (§3.5), where the value of the index is (*indexbyte1* << 8) | *indexbyte2*. The constant pool item at that index must be of type `CONSTANT_Classref` (§6.7.1), a reference to an interface class. The specified method is resolved. The interface method must not be `<init>`, an instance initialization method, or `<clinit>`, a class or interface initialization method.

The *nargs* operand is an unsigned byte that must not be zero. The *method* operand is an unsigned byte that is the interface method token for the method to be invoked. The *objectref* must be of type `reference` and must be followed on the operand stack by *nargs* – 1 words of arguments. The number of words of arguments and the type and order of the values they represent must be consistent with those of the selected interface method.

The interface table of the class of the type of *objectref* is determined. If *objectref* is an array type, then the interface table of class `Object` (§2.2.2.4) is used. The interface table is searched for the resolved interface. The result of the search is a table that is used to map the *method* token to a *index*.

The *index* is an unsigned byte that is used as an index into the method table of the class of the type of *objectref*. If the *objectref* is an array type, then the method table of class `Object` is used. The table entry at that index includes a direct reference to the method's code and modifier information.

The *nargs* – 1 words of arguments and *objectref* are popped from the operand stack. A new stack frame is created for the method being invoked, and *objectref* and the arguments are made the values of its first *nargs* words of local variables, with *arg1* in local variable at index 0, *arg1* in local variable at offset 2, *arg2* immediately following

invokeinterface (cont.) *invokeinterface (cont.)*

that, and so on. The new stack frame is then made current, and the Java Card virtual machine `pc` is set to the opcode of the first instruction of the method to be invoked. Execution continues with the first instruction of the method.

Runtime Exception

If *objectref* is `null`, the *invokeinterface* instruction throws a `NullPointerException`.

Notes

In some circumstances, the *invokeinterface* instruction may throw a `SecurityException` if the current context (§3.4) is not the context (§3.4) of the object referenced by *objectref*. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*. If the current context is not the object's context and the JCRE permits invocation of the method, the *invokeinterface* instruction will cause a context switch (§3.4) to the object's context before invoking the method, and will cause a return context switch to the previous context when the invoked method returns.

invokespecial *invokespecial*

Invoke instance method; special handling for superclass, private, and instance initialization method invocations

Format

invokespecial
indexbyte1
indexbyte2

Forms

invokespecial = 140 (0x8c)

Stack

…, *objectref*, [*arg1*, [*arg2* …]] ⇒
…

Description

The unsigned *indexbyte1* and *indexbyte2* are used to construct an *index* into the constant pool of the current package (§3.5), where the value of the index is (*indexbyte1* << 8) | *indexbyte2*. If the invoked method is a private instance method or an instance initialization method, the constant pool item at *index* must be of type `CONSTANT_StaticMethodref` (§6.7.3), a reference to a statically linked instance method. If the invoked method is a superclass method, the constant pool item at *index* must be of type `CONSTANT_SuperMethodref` (§6.7.2), a reference to an instance method of a specified class. The reference is resolved. The resolved method must not be `<clinit>`, a class or interface initialization method. If the method is `<init>`, an instance initialization method, then the method must only be invoked once on an uninitialized object, and before the first backward branch following the execution of the *new* instruction that allocated the object. Finally, if the method is `protected`, then it must be either a member of the current class or a member of a superclass of the current class, and the class of *objectref* must be either the current class or a subclass of the current class.

The resolved method includes the code for the method, an unsigned byte *nargs* that must not be zero, and the method's modifier information.

The *objectref* must be of type `reference`, and must be followed on the operand stack by *nargs* – 1 words of arguments, where the number of words of arguments and the type and order of the values they represent must be consistent with those of the selected instance method.

The *nargs* – 1 words of arguments and *objectref* are popped from the operand stack. A new stack frame is created for the method being invoked, and *objectref* and the arguments are made the values of its first *nargs* words of local variables, with *objectref* in local variable *0*, *arg1* in local variable *1*, and so on. The new stack frame is

invokespecial (cont.) *invokespecial (cont.)*

then made current, and the Java Card virtual machine `pc` is set to the opcode of the first instruction of the method to be invoked. Execution continues with the first instruction of the method.

Runtime Exception

If *objectref* is `null`, the *invokespecial* instruction throws a `NullPointerException`.

invokestatic *invokestatic*

Invoke a class (`static`) method

Format

invokestatic
indexbyte1
indexbyte2

Forms

invokestatic = 141 (0x8d)

Stack

…, [*arg1*, [*arg2* …]] ⇒
…

Description

The unsigned *indexbyte1* and *indexbyte2* are used to construct an index into the constant pool of the current package (§3.5), where the value of the index is (*indexbyte1* << 8) | *indexbyte2*. The constant pool item at that index must be of type `CONSTANT_StaticMethodref` (§6.7.3), a reference to a static method. The method must not be `<init>`, an instance initialization method, or `<clinit>`, a class or interface initialization method. It must be `static`, and therefore cannot be `abstract`. Finally, if the method is `protected`, then it must be either a member of the current class or a member of a superclass of the current class.

The resolved method includes the code for the method, an unsigned byte *nargs* that may be zero, and the method's modifier information.

The operand stack must contain *nargs* words of arguments, where the number of words of arguments and the type and order of the values they represent must be consistent with those of the resolved method .

The *nargs* words of arguments are popped from the operand stack. A new stack frame is created for the method being invoked, and the words of arguments are made the values of its first *nargs* words of local variables, with *arg1* in local variable *0*, *arg2* in local variable *1*, and so on. The new stack frame is then made current, and the Java Card virtual machine `pc` is set to the opcode of the first instruction of the method to be invoked. Execution continues with the first instruction of the method.

invokevirtual *invokevirtual*

Invoke instance method; dispatch based on class

Format

invokevirtual
indexbyte1
indexbyte2

Forms

invokevirtual = 139 (0x8b)

Stack

…, *objectref*, [*arg1*, [*arg2* …]] ⇒
…

Description

The unsigned *indexbyte1* and *indexbyte2* are used to construct an index into the constant pool of the current package (§3.5), where the value of the index is (*indexbyte1* << 8) | *indexbyte2*. The constant pool item at that index must be of type `CONSTANT_VirtualMethodref` (§6.7.2), a reference to a class and a virtual method token. The specified method is resolved. The method must not be `<init>`, an instance initialization method, or `<clinit>`, a class or interface initialization method. If the method is `protected`, then it must be either a member of the current class or a member of a superclass of the current class, and the class of *objectref* must be either the current class or a subclass of the current class.

The resolved method reference includes an unsigned *index* into the method table of the resolved class and an unsigned byte *nargs* that must not be zero.

The *objectref* must be of type `reference`. The *index* is an unsigned byte that is used as an index into the method table of the class of the type of *objectref*. If the *objectref* is an array type, then the method table of class `Object` (§2.2.2.4) is used. The table entry at that index includes a direct reference to the method's code and modifier information.

The *objectref* must be followed on the operand stack by *nargs* – 1 words of arguments, where the number of words of arguments and the type and order of the values they represent must be consistent with those of the selected instance method.

The *nargs* – 1 words of arguments and *objectref* are popped from the operand stack. A new stack frame is created for the method being invoked, and *objectref* and the arguments are made the values of its first *nargs* words of local variables, with *objectref* in local variable *0*, *arg1* in local variable *1*, and so on. The new stack frame is then made current, and the Java Card virtual machine `pc` is set to the opcode of the first instruction of the method to be invoked. Execution continues with the first instruction of the method.

invokevirtual (cont.) *invokevirtual (cont.)*

Runtime Exception

If *objectref* is `null`, the *invokevirtual* instruction throws a `NullPointerException`.

In some circumstances, the *invokevirtual* instruction may throw a `SecurityException` if the current context (§3.4) is not the context (§3.4) of the object referenced by *objectref*. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*. If the current context is not the object's context and the JCRE permits invocation of the method, the *invokevirtual* instruction will cause a context switch (§3.4) to the object's context before invoking the method, and will cause a return context switch to the previous context when the invoked method returns.

ior *ior*

Boolean OR `int`

Format

ior

Forms

ior = 86 (0x56)

Stack

..., value1.word1, value1.word2, value2.word1, value2.word2 ⇒
..., result.word1, result.word2

Description

Both *value1* and *value2* must be of type `int`. The values are popped from the operand stack. An `int` *result* is calculated by taking the bitwise inclusive OR of *value1* and *value2*. The *result* is pushed onto the operand stack.

Notes

If a virtual machine does not support the `int` data type, the *ior* instruction will not be available.

irem *irem*

Remainder `int`

Format

irem

Forms

irem = 74 (0x4a)

Stack

…, value1.word1, value1.word2, value2.word1, value2.word2 ⇒
…, result.word1, result.word2

Description

Both *value1* and *value2* must be of type `int`. The values are popped from the operand stack. The `int` *result* is the value of the Java expression *value1* – (*value1* / *value2*) * *value2*. The *result* is pushed onto the operand stack.

The result of the *irem* instruction is such that `(a/b)*b + (a%b)` is equal to `a`. This identity holds even in the special case that the dividend is the negative `int` of largest possible magnitude for its type and the divisor is –`1` (the remainder is `0`). It follows from this rule that the result of the remainder operation can be negative only if the dividend is negative and can be positive only if the dividend is positive. Moreover, the magnitude of the result is always less than the magnitude of the divisor.

Runtime Exception

If the value of the divisor for a `short` remainder operator is 0, *irem* throws an `ArithmeticException`.

Notes

If a virtual machine does not support the `int` data type, the *irem* instruction will not be available.

ireturn *ireturn*

Return `int` from method

Format

ireturn

Forms

ireturn = 121 (0x79)

Stack

..., value.word1, value.word2 ⇒
[empty]

Description

The *value* must be of type `int`. It is popped from the operand stack of the current frame (§3.5) and pushed onto the operand stack of the frame of the invoker. Any other values on the operand stack of the current method are discarded.

The virtual machine then reinstates the frame of the invoker and returns control to the invoker.

Notes

If a virtual machine does not support the `int` data type, the *ireturn* instruction will not be available.

ishl *ishl*

Shift left `int`

Format

ishl

Forms

ishl = 78 (0x4e)

Stack

…, value1.word1, value1.word2, value2.word1, value2.word2 ⇒
…, result.word1, result.word2

Description

Both *value1* and *value2* must be of type `int`. The values are popped from the operand stack. An `int` *result* is calculated by shifting *value1* left by *s* bit positions, where *s* is the value of the low five bits of *value2*. The *result* is pushed onto the operand stack.

Notes

This is equivalent (even if overflow occurs) to multiplication by 2 to the power *s*. The shift distance actually used is always in the range 0 to 31, inclusive, as if *value2* were subjected to a bitwise logical AND with the mask value 0x1f.

If a virtual machine does not support the `int` data type, the *ishl* instruction will not be available.

ishr *ishr*

Arithmetic shift right `int`

Format

ishr

Forms

ishr = 80 (0x50)

Stack

..., value1.word1, value1.word2, value2.word1, value2.word2 ⇒
..., result.word1, result.word2

Description

Both *value1* and *value2* must be of type `int`. The values are popped from the operand stack. An `int` *result* is calculated by shifting *value1* right by *s* bit positions, with sign extension, where *s* is the value of the low five bits of *value2*. The *result* is pushed onto the operand stack.

Notes

The resulting value is $\lfloor (value1) / 2^{s} \rfloor$, where *s* is *value2* & 0x1f. For nonnegative *value1*, this is equivalent (even if overflow occurs) to truncating `int` division by 2 to the power *s*. The shift distance actually used is always in the range 0 to 31, inclusive, as if *value2* were subjected to a bitwise logical AND with the mask value 0x1f.

Notes

If a virtual machine does not support the `int` data type, the *ishr* instruction will not be available.

istore *istore*

Store `int` into local variable

Format

istore
index

Forms

istore = 42 (0x2a)

Stack

..., value.word1, value.word2 ⇒
...

Description

The *index* is an unsigned byte. Both *index* and *index* + 1 must be a valid index into the local variables of the current frame (§3.5). The *value* on top of the operand stack must be of type `int`. It is popped from the operand stack, and the local variables at *index* and *index* + 1 are set to *value*.

Notes

If a virtual machine does not support the `int` data type, the *istore* instruction will not be available.

istore_<n> *istore_<n>*

Store `int` into local variable

Format

istore_<n>

Forms

istore_0 = 51 (0x33)
i*store_1* = 52 (0x34)
i*store_2* = 53 (0x35)
i*store_3* = 54 (0x36)

Stack

…, *value.word1*, *value.word2* ⇒
…

Description

Both <*n*> and <*n*> + 1 must be a valid indices into the local variables of the current frame (§3.5). The *value* on top of the operand stack must be of type `int`. It is popped from the operand stack, and the local variables at *index* and *index* + 1 are set to *value*.

Notes

If a virtual machine does not support the `int` data type, the *istore_<n>* instruction will not be available.

isub *isub*

Subtract `int`

Format

isub

Forms

isub = 68 (0x44)

Stack

…, value1.word1, value1.word2, value2.word1, value2.word2 ⇒
…, result.word1, result.word2

Description

Both *value1* and *value2* must be of type `int`. The values are popped from the operand stack. The `int` *result* is *value1* - *value2*. The *result* is pushed onto the operand stack.

For `int` subtraction, `a – b` produces the same result as `a + (–b)`. For `int` values, subtraction from zeros is the same as negation.

Despite the fact that overflow or underflow may occur, in which case the *result* may have a different sign than the true mathematical result, execution of an *isub* instruction never throws a runtime exception.

Notes

If a virtual machine does not support the `int` data type, the *isub* instruction will not be available.

itableswitch *itableswitch*

Access jump table by `int` index and jump

Format

itableswitch
defaultbyte1
defaultbyte2
lowbyte1
lowbyte2
lowbyte3
lowbyte4
highbyte1
highbyte2
highbyte3
highbyte4
jump offsets…

Offset Format

offsetbyte1
offsetbyte2

Forms

itableswitch = 116 (0x74)

Stack

…, *index* ⇒
…

Description

An *itableswitch* instruction is a variable-length instruction. Immediately after the *itableswitch* opcode follow a signed 16-bit value *default*, a signed 32-bit value *low*, a signed 32-bit value *high*, and then *high* – *low* + 1 further signed 16-bit offsets. The value *low* must be less than or equal to *high*. The *high* – *low* + 1 signed 16-bit offsets are treated as a 0-based jump table. Each of the signed 16-bit values is constructed from two unsigned bytes as (*byte1* << 8) | *byte2*. Each of the signed 32-bit values is constructed from four unsigned bytes as (*byte1* << 24) | (*byte2* << 16) | (*byte3* << 8) | *byte4*.

The *index* must be of type `int` and is popped from the stack. If *index* is less than *low* or *index* is greater than *high*, then a target address is calculated by adding *default* to the address of the opcode of this *itableswitch* instruction. Otherwise, the offset at position *index* – *low* of the jump table is extracted. The target address is calculated by adding that offset to the address of the opcode of this *itableswitch* instruction. Execution then continues at the target address.

itableswitch (cont.) *itableswitch (cont.)*

The target addresses that can be calculated from each jump table offset, as well as the one calculated from *default*, must be the address of an opcode of an instruction within the method that contains this *itableswitch* instruction.

Notes

If a virtual machine does not support the `int` data type, the *itableswitch* instruction will not be available.

iushr *iushr*

Logical shift right `int`

Format

iushr

Forms

iushr = 82 (0x52)

Stack

..., value1.word1, value1.word2, value2.word1, value2.word2 ⇒
..., result.word1, result.word2

Description

Both *value1* and *value2* must be of type `int`. The values are popped from the operand stack. An `int` *result* is calculated by shifting the result right by *s* bit positions, with zero extension, where *s* is the value of the low five bits of *value2*. The *result* is pushed onto the operand stack.

Notes

If *value1* is positive and *s* is *value2* & 0x1f, the result is the same as that of *value1* >> *s*; if *value1* is negative, the result is equal to the value of the expression (*value1* >> *s*) + (2 << ~*s*). The addition of the (2 << ~*s*) term cancels out the propagated sign bit. The shift distance actually used is always in the range 0 to 31, inclusive, as if *value2* were subjected to a bitwise logical AND with the mask value 0x1f.

If a virtual machine does not support the `int` data type, the *iushr* instruction will not be available.

ixor *ixor*

Boolean XOR `int`

Format

ixor

Forms

ixor = 88 (0x58)

Stack

…, *value1.word1, value1.word2, value2.word1, value2.word2* ⇒
…, *result.word1, result.word2*

Description

Both *value1* and *value2* must be of type `int`. The values are popped from the operand stack. An `int` *result* is calculated by taking the bitwise exclusive OR of *value1* and *value2*. The *result* is pushed onto the operand stack.

Notes

If a virtual machine does not support the `int` data type, the *ixor* instruction will not be available.

jsr *jsr*

Jump subroutine

Format

jsr
branchbyte1
branchbyte2

Forms

jsr = 113 (0x71)

Stack

… ⇒
…, *address*

Description

The *address* of the opcode of the instruction immediately following this *jsr* instruction is pushed onto the operand stack as a value of type `returnAddress`. The unsigned *branchbyte1* and *branchbyte2* are used to construct a signed 16-bit offset, where the offset is (*branchbyte1* << 8) | *branchbyte2*. Execution proceeds at that offset from the address of this *jsr* instruction. The target address must be that of an opcode of an instruction within the method that contains this *jsr* instruction.

Notes

The *jsr* instruction is used with the *ret* instruction in the implementation of the `finally` clause of the Java language. Note that *jsr* pushes the address onto the stack and *ret* gets it out of a local variable. This asymmetry is intentional.

new *new*

Create new object

Format

new
indexbyte1
indexbyte2

Forms

new = 143 (0x8f)

Stack

... ⇒
..., *objectref*

Description

The unsigned *indexbyte1* and *indexbyte2* are used to construct an index into the constant pool of the current package (§3.5), where the value of the index is (*indexbyte1* << 8) | *indexbyte2*. The item at that index in the constant pool must be of type `CONSTANT_Classref` (§6.7.1), a reference to a class or interface type. The reference is resolved and must result in a class type (it must not result in an interface type). Memory for a new instance of that class is allocated from the heap, and the instance variables of the new object are initialized to their default initial values. The *objectref*, a `reference` to the instance, is pushed onto the operand stack.

Notes

The *new* instruction does not completely create a new instance; instance creation is not completed until an instance initialization method has been invoked on the uninitialized instance.

newarray *newarray*

Create new array

Format

newarray
atype

Forms

newarray = 144 (0x90)

Stack

..., *count* ⇒
..., *arrayref*

Description

The *count* must be of type `short`. It is popped off the operand stack. The *count* represents the number of elements in the array to be created.

The unsigned byte *atype* is a code that indicates the type of array to create. It must take one of the following values:

Array Type	*atype*
`T_BOOLEAN`	`10`
`T_BYTE`	`11`
`T_SHORT`	`12`
`T_INT`	`13`

A new array whose components are of type *atype*, of length *count*, is allocated from the heap. A `reference` *arrayref* to this new array object is pushed onto the operand stack. All of the elements of the new array are initialized to the default initial value for its type.

Runtime Exception

If *count* is less than zero, the *newarray* instruction throws a `NegativeArraySizeException`.

Notes

If a virtual machine does not support the `int` data type, the value of *atype* may not be 13 (array type = `T_INT`).

nop *nop*

Do nothing

Format

nop

Forms

nop = 0 (0x0)

Stack

No change

Description

Do nothing.

pop *pop*

Pop top operand stack word

Format

pop

Forms

pop = 59 (0x3b)

Stack

…, *word* ⇒
…

Description

The top word is popped from the operand stack.

Notes

The *pop* instruction operates on an untyped word, ignoring the type of data it contains.

pop2 *pop2*

Pop top two operand stack words

Format

pop2

Forms

pop2 = 60 (0x3c)

Stack

…, *word2*, *word1* ⇒
…

Description

The top two words are popped from the operand stack.

The *pop2* instruction must not be used unless each of *word1* and *word2* is a word that contains a 16-bit data type or both together are the two words of a single 32-bit datum.

Notes

Except for restrictions preserving the integrity of 32-bit data types, the *pop2* instruction operates on an untyped word, ignoring the type of data it contains.

putfield_<t> *putfield_<t>*

Set field in object

Format

putfield_<t>
index

Forms

putfield_a = 135 (0x87)
putfield_b = 136 (0x88)
putfield_s = 137 (0x89)
putfield_i = 138 (0x8a)

Stack

…, objectref, value ⇒
…

OR

…, objectref, value.word1, value.word2 ⇒
…

Description

The unsigned *index* is used as an index into the constant pool of the current package (§3.5). The constant pool item at the index must be of type `CONSTANT_InstanceFieldref` (§6.7.2), a reference to a class and a field token. If the field is `protected`, then it must be either a member of the current class or a member of a superclass of the current class, and the class of *objectref* must be either the current class or a subclass of the current class.

The item must resolve to a field with a type that matches *t*, as follows:

- *a* field must be of type `reference`
- *b* field must be of type `byte` or type `boolean`
- *s* field must be of type `short`
- *i* field must be of type `int`

The width of a field in a class instance is determined by the field type specified in the instruction. The item is resolved, determining the field offset. The *objectref*, which must be of type `reference`, and the *value* are popped from the operand stack. If the field is of type `byte` or type `boolean`, the *value* is truncated to a `byte`. The field at the offset from the start of the object referenced by *objectref* is set to the *value*.

Runtime Exception

If *objectref* is `null`, the *putfield_<t>* instruction throws a `NullPointerException`.

putfield_<t> (cont.) *putfield_<t> (cont.)*

Notes

In some circumstances, the *putfield_<t>* instruction may throw a `SecurityException` if the current context (§3.4) is not the owning context (§3.4) of the object referenced by *objectref*. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*.

If a virtual machine does not support the `int` data type, the *putfield_i* instruction will not be available.

putfield_<t>_this *putfield_<t>_this*

Set field in current object

Format

putfield_<t>_this
index

Forms

putfield_a_this = 181 (0xb5)
putfield_b_this = 182 (0xb6)
putfield_s_this = 183 (0xb7)
putfield_i_this = 184 (0xb8)

Stack

…, *value* ⇒
…

OR

…, *value.word1*, *value.word2* ⇒
…

Description

The currently executing method must be an instance method that was invoked using the *invokevirtual*, *invokeinterface* or *invokespecial* instruction. The local variable at index 0 must contain a `reference` *objectref* to the currently executing method's `this` parameter. The unsigned *index* is used as an index into the constant pool of the current package (§3.5). The constant pool item at the index must be of type `CONSTANT_InstanceFieldref` (§6.7.2), a reference to a class and a field token. If the field is `protected`, then it must be either a member of the current class or a member of a superclass of the current class, and the class of *objectref* must be either the current class or a subclass of the current class.

The item must resolve to a field with a type that matches *t*, as follows:

- *a* field must be of type `reference`
- *b* field must be of type `byte` or type `boolean`
- *s* field must be of type `short`
- *i* field must be of type `int`

The width of a field in a class instance is determined by the field type specified in the instruction. The item is resolved, determining the field offset. The *value* is popped from the operand stack. If the field is of type `byte` or type `boolean`, the *value* is truncated to a `byte`. The field at the offset from the start of the object referenced by *objectref* is set to the *value*.

putfield_<t>_this (cont.) *putfield_<t>_this (cont.)*

Runtime Exception

If *objectref* is `null`, the *putfield_<t>_this* instruction throws a `NullPointerException`.

Notes

In some circumstances, the *putfield_<t>_this* instruction may throw a `SecurityException` if the current context (§3.4) is not the owning context (§3.4) of the object referenced by *objectref*. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*.

If a virtual machine does not support the `int` data type, the *putfield_i_this* instruction will not be available.

putfield_<t>_w *putfield_<t>_w*

Set field in object (wide index)

Format

putfield<t>_w
indexbyte1
indexbyte2

Forms

putfield_a_w = 177 (0xb1)
putfield_b_w = 178 (0xb2)
putfield_s_w = 179 (0xb3)
putfield_i_w = 180 (0xb4)

Stack

…, *objectref*, *value* ⇒
…

OR

…, *objectref*, *value.word1*, *value.word2* ⇒
…

Description

The unsigned *indexbyte1* and *indexbyte2* are used to construct an index into the constant pool of the current package (§3.5), where the value of the index is (*indexbyte1* << 8) | *indexbyte2*. The constant pool item at the index must be of type `CONSTANT_InstanceFieldref` (§6.7.2), a reference to a class and a field token. If the field is `protected`, then it must be either a member of the current class or a member of a superclass of the current class, and the class of *objectref* must be either the current class or a subclass of the current class.

The item must resolve to a field with a type that matches *t*, as follows:

- *a* field must be of type `reference`
- *b* field must be of type `byte` or type `boolean`
- *s* field must be of type `short`
- *i* field must be of type `int`

The width of a field in a class instance is determined by the field type specified in the instruction. The item is resolved, determining the field offset. The *objectref*, which must be of type `reference`, and the *value* are popped from the operand stack. If the field is of type `byte` or type `boolean`, the *value* is truncated to a `byte`. The field at the offset from the start of the object referenced by *objectref* is set to the *value*.

putfield_<t>_w (cont.) *putfield_<t>_w (cont.)*

Runtime Exception

If *objectref* is `null`, the *putfield_<t>_w* instruction throws a `NullPointerException`.

Notes

In some circumstances, the *putfield_<t>_w* instruction may throw a `SecurityException` if the current context (§3.4) is not the owning context (§3.4) of the object referenced by *objectref*. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*.

If a virtual machine does not support the `int` data type, the *putfield_i_w* instruction will not be available.

putstatic_<t> *putstatic_<t>*

Set `static` field in class

Format

putstatic_<t>
indexbyte1
indexbyte2

Forms

putstatic_a = 127 (0x7f)
putstatic_b = 128 (0x80)
putstatic_s = 129 (0x81)
putstatic_i = 130 (0x82)

Stack

…, *value* ⇒
…

OR

…, *value.word1*, *value.word2* ⇒
…

Description

The unsigned *indexbyte1* and *indexbyte2* are used to construct an index into the constant pool of the current package (§3.5), where the value of the index is (*indexbyte1* << 8) | *indexbyte2*. The constant pool item at the index must be of type `CONSTANT_StaticFieldref` (§6.7.3), a reference to a static field. If the field is `protected`, then it must be either a member of the current class or a member of a superclass of the current class.

The item must resolve to a field with a type that matches *t*, as follows:

- *a* field must be of type `reference`
- *b* field must be of type `byte` or type `boolean`
- *s* field must be of type `short`
- *i* field must be of type `int`

The width of a class field is determined by the field type specified in the instruction. The item is resolved, determining the class field. The *value* is popped from the operand stack. If the field is of type `byte` or type `boolean`, the *value* is truncated to a `byte`. The field is set to the *value*.

putstatic_<t> (cont.) *putstatic_<t> (cont.)*

Notes

In some circumstances, the *putstatic_a* instruction may throw a `SecurityException` if the current context (§3.4) is not the owning context (§3.4) of the object being stored in the field. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*.

If a virtual machine does not support the `int` data type, the *putstatic_i* instruction will not be available.

ret *ret*

Return from subroutine

Format

ret
index

Forms

ret = 114 (0x72)

Stack

No change

Description

The *index* is an unsigned byte that must be a valid index into the local variables of the current frame (§3.5). The local variable at *index* must contain a value of type `returnAddress`. The contents of the local variable are written into the Java Card virtual machine's `pc` register, and execution continues there.

Notes

The *ret* instruction is used with the *jsr* instruction in the implementation of the `finally` keyword of the Java language. Note that *jsr* pushes the address onto the stack and *ret* gets it out of a local variable. This asymmetry is intentional.

The *ret* instruction should not be confused with the *return* instruction. A *return* instruction returns control from a Java method to its invoker, without passing any value back to the invoker.

return *return*

Return `void` from method

Format

return

Forms

return = 122 (0x7a)

Stack

... ⇒
[empty]

Description

Any values on the operand stack of the current method are discarded. The virtual machine then reinstates the frame of the invoker and returns control to the invoker.

s2b *s2b*

Convert `short` to `byte`

Format

s2b

Forms

s2b = 91 (0x5b)

Stack

..., value ⇒
..., result

Description

The *value* on top of the operand stack must be of type `short`. It is popped from the top of the operand stack, truncated to a `byte` *result*, then sign-extended to a `short` *result*. The *result* is pushed onto the operand stack.

Notes

The *s2b* instruction performs a narrowing primitive conversion. It may lose information about the overall magnitude of *value*. The *result* may also not have the same sign as *value*.

s2i *s2i*

Convert `short` to `int`

Format

s2i

Forms

s2i = 92 (0x5c)

Stack

…, *value* ⇒
…, *result.word1*, *result.word2*

Description

The *value* on top of the operand stack must be of type `short`. It is popped from the operand stack and sign-extended to an `int` *result*. The *result* is pushed onto the operand stack.

Notes

The *s2i* instruction performs a widening primitive conversion. Because all values of type `short` are exactly representable by type `int`, the conversion is exact.

If a virtual machine does not support the `int` data type, the *s2i* instruction will not be available.

sadd *sadd*

Add `short`

Format

sadd

Forms

sadd = 65 (0x41)

Stack

..., value1, value2 ⇒
..., result

Description

Both *value1* and *value2* must be of type `short`. The values are popped from the operand stack. The `short` *result* is *value1* + *value2*. The *result* is pushed onto the operand stack.

If a *sadd* instruction overflows, then the result is the low-order bits of the true mathematical result in a sufficiently wide two's-complement format. If overflow occurs, then the sign of the result may not be the same as the sign of the mathematical sum of the two values.

saload *saload*

Load `short` from array

Format

saload

Forms

saload = 38 (0x46)

Stack

…, *arrayref, index* ⇒
…, *value*

Description

The *arrayref* must be of type `reference` and must refer to an array whose components are of type `short`. The *index* must be of type `short`. Both *arrayref* and *index* are popped from the operand stack. The `short` *value* in the component of the array at *index* is retrieved and pushed onto the top of the operand stack.

Runtime Exceptions

If *arrayref* is `null`, *saload* throws a `NullPointerException`.

Otherwise, if *index* is not within the bounds of the array referenced by *arrayref*, the *saload* instruction throws an `ArrayIndexOutOfBoundsException`.

Notes

In some circumstances, the *saload* instruction may throw a `SecurityException` if the current context (§3.4) is not the owning context (§3.4) of the array referenced by *arrayref*. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*.

sand *sand*

Boolean AND `short`

Format

sand

Forms

sand = 83 (0x53)

Stack

…, *value1*, *value2* ⇒
…, *result*

Description

Both *value1* and *value2* are popped from the operand stack. A `short` *result* is calculated by taking the bitwise AND (conjunction) of *value1* and *value2*. The *result* is pushed onto the operand stack.

sastore *sastore*

Store into `short` array

Format

sastore

Forms

sastore = 57 (0x39)

Stack

…, *arrayref*, *index*, *value* ⇒
…

Description

The *arrayref* must be of type `reference` and must refer to an array whose components are of type `short`. The *index* and *value* must both be of type `short`. The *arrayref*, *index* and *value* are popped from the operand stack. The `short` *value* is stored as the component of the array indexed by *index*.

Runtime Exception

If *arrayref* is `null`, *sastore* throws a `NullPointerException`.

Otherwise, if *index* is not within the bounds of the array referenced by *arrayref*, the *sastore* instruction throws an `ArrayIndexOutOfBoundsException`.

Notes

In some circumstances, the *sastore* instruction may throw a `SecurityException` if the current context (§3.4) is not the owning context (§3.4) of the array referenced by *arrayref*. The exact circumstances when the exception will be thrown are specified in Chapter 6 of the *Java Card 2.1 Runtime Environment (JCRE) Specification*.

sconst_<s> *sconst_<s>*

Push `short` constant

Format

sconst_<s>

Forms

sconst_m1 = 2 (0x2)
sconst_0 = 3 (0x3)
sconst_1 = 4 (0x4)
sconst_2 = 5 (0x5)
sconst_3 = 6 (0x6)
sconst_4= 7 (0x7)
sconst_5 = 8 (0x8)

Stack

... ⇒
..., <*s*>

Description

Push the `short` constant <*s*> (*-1*, *0*, *1*, *2*, *3*, *4*, or *5*) onto the operand stack.

sdiv *sdiv*

Divide `short`

Format

sdiv

Forms

sdiv = 71 (0x47)

Stack

…, *value1*, *value2* ⇒
…, *result*

Description

Both *value1* and *value2* must be of type `short`. The values are popped from the operand stack. The `short` *result* is the value of the Java expression *value1* / *value2*. The *result* is pushed onto the operand stack.

A `short` division rounds towards 0; that is, the quotient produced for `short` values in *n/d* is a `short` value *q* whose magnitude is as large as possible while satisfying | *d* · *q* | = | *n* |. Moreover, *q* is a positive when | *n* | = | *d* | and *n* and *d* have the same sign, but *q* is negative when | *n* | = | *d* | and *n* and *d* have opposite signs.

There is one special case that does not satisfy this rule: if the dividend is the negative integer of the largest possible magnitude for the `short` type, and the divisor is *–1*, then overflow occurs, and the result is equal to the dividend. Despite the overflow, no exception is thrown in this case.

Runtime Exception

If the value of the divisor in a `short` division is 0, *sdiv* throws an `ArithmeticException`.

sinc *sinc*

Increment local `short` variable by constant

Format

sinc
index
const

Forms

sinc = 89 (0x59)

Stack

No change

Description

The *index* is an unsigned byte that must be a valid index into the local variable of the current frame (§3.5). The *const* is an immediate signed byte. The local variable at *index* must contain a `short`. The value *const* is first sign-extended to a `short`, then the local variable at *index* is incremented by that amount.

sinc_w *sinc_w*

Increment local `short` variable by constant

Format

sinc_w
index
byte1
byte2

Forms

sinc_w = 150 (0x96)

Stack

No change

Description

The *index* is an unsigned byte that must be a valid index into the local variable of the current frame (§3.5). The immediate unsigned *byte1* and *byte2* values are assembled into a `short` *const* where the value of *const* is (*byte1* << 8) | *byte2*. The local variable at *index*, which must contain a `short`, is incremented by *const*.

sipush *sipush*

Push `short`

Format

sipush
byte1
byte2

Forms

sipush = 19 (0x13)

Stack

… ⇒
…, *value1.word1, value1.word2*

Description

The immediate unsigned *byte1* and *byte2* values are assembled into a signed `short` where the value of the short is (*byte1* << 8) | *byte2*. The intermediate value is then sign-extended to an `int`, and the resulting *value* is pushed onto the operand stack.

Notes

If a virtual machine does not support the `int` data type, the *sipush* instruction will not be available.

sload *sload*

Load `short` from local variable

Format

sload
index

Forms

sload = 22 (0x16)

Stack

… ⇒
…, *value*

Description

The *index* is an unsigned byte that must be a valid index into the local variables of the current frame (§3.5). The local variable at *index* must contain a `short`. The *value* in the local variable at *index* is pushed onto the operand stack.

sload_<n> *sload_<n>*

Load `short` from local variable

Format

sload_<n>

Forms

sload_0 = 28 (0x1c)
sload_1 = 29 (0x1d)
sload_2 = 30 (0x1e)
sload_3 = 31 (0x1f)

Stack

... ⇒
..., *value*

Description

The <*n*> must be a valid index into the local variables of the current frame (§3.5). The local variable at <*n*> must contain a `short`. The *value* in the local variable at <*n*> is pushed onto the operand stack.

Notes

Each of the *sload_<n>* instructions is the same as *sload* with an *index* of <*n*>, except that the operand <*n*> is implicit.

slookupswitch *slookupswitch*

Access jump table by key match and jump

Format

slookupswitch
defaultbyte1
defaultbyte2
npairs1
npairs2
match-offset pairs…

Pair Format

matchbyte1
matchbyte2
offsetbyte1
offsetbyte2

Forms

slookupswitch = 117 (0x75)

Stack

…, *key* ⇒
…

Description

A *slookupswitch* instruction is a variable-length instruction. Immediately after the *slookupswitch* opcode follow a signed 16-bit value *default*, an unsigned 16-bit value *npairs*, and then *npairs* pairs. Each pair consists of a `short` *match* and a signed 16-bit *offset*. Each of the signed 16-bit values is constructed from two unsigned bytes as (*byte1* << 8) | *byte2*.

The table *match-offset* pairs of the *slookupswitch* instruction must be sorted in increasing numerical order by *match*.

The *key* must be of type `short` and is popped from the operand stack and compared against the *match* values. If it is equal to one of them, then a target address is calculated by adding the corresponding *offset* to the address of the opcode of this *slookupswitch* instruction. If the *key* does not match any of the *match* values, the target address is calculated by adding *default* to the address of the opcode of this *slookupswitch* instruction. Execution then continues at the target address.

The target address that can be calculated from the offset of each *match-offset* pair, as well as the one calculated from *default*, must be the address of an opcode of an instruction within the method that contains this *slookupswitch* instruction.

slookupswitch (cont.) *slookupswitch (cont.)*

Notes

The *match-offset* pairs are sorted to support lookup routines that are quicker than linear search.

smul *smul*

Multiply `short`

Format

smul

Forms

smul = 69 (0x45)

Stack

…, *value1*, *value2* ⇒
…, *result*

Description

Both *value1* and *value2* must be of type `short`. The values are popped from the operand stack. The `short` *result* is *value1* * *value2*. The *result* is pushed onto the operand stack.

If a *smul* instruction overflows, then the result is the low-order bits of the mathematical product as a `short`. If overflow occurs, then the sign of the result may not be the same as the sign of the mathematical product of the two values.

sneg *sneg*

Negate `short`

Format

sneg

Forms

sneg = 72 (0x4b)

Stack

..., value ⇒
..., result

Description

The *value* must be of type `short`. It is popped from the operand stack. The `short` *result* is the arithmetic negation of *value*, *-value*. The *result* is pushed onto the operand stack.

For `short` values, negation is the same as subtraction from zero. Because the Java Card virtual machine uses two's-complement representation for integers and the range of two's-complement values is not symmetric, the negation of the maximum negative `short` results in that same maximum negative number. Despite the fact that overflow has occurred, no exception is thrown.

For all `short` values `x`, `-x` equals `(~x) + 1`.

sor *sor*

Boolean OR `short`

Format

sor

Forms

sor = 85 (0x55)

Stack

…, *value1*, *value2* ⇒
…, *result*

Description

Both *value1* and *value2* must be of type `short`. The values are popped from the operand stack. A `short` *result* is calculated by taking the bitwise inclusive OR of *value1* and *value2*. The *result* is pushed onto the operand stack.

srem *srem*

Remainder `short`

Format

srem

Forms

srem = 73 (0x49)

Stack

…, *value1*, *value2* ⇒
…, *result*

Description

Both *value1* and *value2* must be of type `short`. The values are popped from the operand stack. The `short` *result* is the value of the Java expression *value1* – (*value1* / *value2*) * *value2*. The *result* is pushed onto the operand stack.

The result of the *irem* instruction is such that `(a/b)*b + (a%b)` is equal to `a`. This identity holds even in the special case that the dividend is the negative `short` of largest possible magnitude for its type and the divisor is `–1` (the remainder is `0`). It follows from this rule that the result of the remainder operation can be negative only if the dividend is negative and can be positive only if the dividend is positive. Moreover, the magnitude of the result is always less than the magnitude of the divisor.

Runtime Exception

If the value of the divisor for a `short` remainder operator is 0, *srem* throws an `ArithmeticException`.

sreturn *sreturn*

Return `short` from method

Format

sreturn

Forms

sreturn = 120 (0x78)

Stack

…, *value* ⇒
[empty]

Description

The *value* must be of type `short`. It is popped from the operand stack of the current frame (§3.5) and pushed onto the operand stack of the frame of the invoker. Any other values on the operand stack of the current method are discarded.

The virtual machine then reinstates the frame of the invoker and returns control to the invoker.

sshl *sshl*

Shift left `short`

Format

sshl

Forms

sshl = 77 (0x4d)

Stack

..., value1, value2 ⇒
..., result

Description

Both *value1* and *value2* must be of type `short`. The values are popped from the operand stack. A `short` *result* is calculated by shifting *value1* left by *s* bit positions, where *s* is the value of the low five bits of *value2*. The *result* is pushed onto the operand stack.

Notes

This is equivalent (even if overflow occurs) to multiplication by 2 to the power *s*. The shift distance actually used is always in the range 0 to 31, inclusive, as if *value2* were subjected to a bitwise logical AND with the mask value 0x1f.

sshr *sshr*

Arithmetic shift right `short`

Format

sshr

Forms

sshr = 79 (0x4f)

Stack

…, *value1*, *value2* ⇒
…, *result*

Description

Both *value1* and *value2* must be of type `short`. The values are popped from the operand stack. A `short` *result* is calculated by shifting *value1* right by *s* bit positions, with sign extension, where *s* is the value of the low five bits of *value2*. The *result* is pushed onto the operand stack.

Notes

The resulting value is $\lfloor (value1) / 2^{s} \rfloor$, where *s* is *value2* & 0x1f. For nonnegative *value1*, this is equivalent (even if overflow occurs) to truncating `short` division by 2 to the power *s*. The shift distance actually used is always in the range 0 to 31, inclusive, as if *value2* were subjected to a bitwise logical AND with the mask value 0x1f.

sspush *sspush*

Push `short`

Format

sspush
byte1
byte2

Forms

sspush = 17 (0x11)

Stack

… ⇒
…, *value*

Description

The immediate unsigned *byte1* and *byte2* values are assembled into a signed `short` where the value of the short is (*byte1* << 8) | *byte2*. The resulting *value* is pushed onto the operand stack.

sstore *sstore*

Store `short` into local variable

Format

sstore
index

Forms

sstore = 41 (0x29)

Stack

…, *value* ⇒
…

Description

The *index* is an unsigned byte that must be a valid index into the local variables of the current frame (§3.5). The *value* on top of the operand stack must be of type `short`. It is popped from the operand stack, and the value of the local variable at *index* is set to *value*.

sstore_<n> *sstore_<n>*

Store `short` into local variable

Format

sstore_<n>

Forms

sstore_0 = 47 (0x2f)
sstore_1 = 48 (0x30)
sstore_2 = 49 (0x31)
sstore_3 = 50 (0x32)

Stack

…, *value* ⇒
…

Description

The <*n*> must be a valid index into the local variables of the current frame (§3.5). The *value* on top of the operand stack must be of type `short`. It is popped from the operand stack, and the value of the local variable at <*n*> is set to *value*.

ssub *ssub*

Subtract `short`

Format

ssub

Forms

ssub = 67 (0x43)

Stack

…, *value1*, *value2* ⇒
…, *result*

Description

Both *value1* and *value2* must be of type `short`. The values are popped from the operand stack. The `short` *result* is *value1* - *value2*. The *result* is pushed onto the operand stack.

For `short` subtraction, `a – b` produces the same result as `a + (–b)`. For `short` values, subtraction from zeros is the same as negation.

Despite the fact that overflow or underflow may occur, in which case the *result* may have a different sign than the true mathematical result, execution of a *ssub* instruction never throws a runtime exception.

stableswitch *stableswitch*

Access jump table by `short` index and jump

Format

stableswitch
defaultbyte1
defaultbyte2
lowbyte1
lowbyte2
highbyte1
highbyte2
jump offsets…

Offset Format

offsetbyte1
offsetbyte2

Forms

stableswitch = 115 (0x73)

Stack

…, *index* ⇒
…

Description

A *stableswitch* instruction is a variable-length instruction. Immediately after the *stableswitch* opcode follow a signed 16-bit value *default*, a signed 16-bit value *low*, a signed 16-bit value *high*, and then *high* – *low* + 1 further signed 16-bit offsets. The value *low* must be less than or equal to *high*. The *high* – *low* + 1 signed 16-bit offsets are treated as a 0-based jump table. Each of the signed 16-bit values is constructed from two unsigned bytes as (*byte1* << 8) | *byte2*.

The *index* must be of type `short` and is popped from the stack. If *index* is less than *low* or *index* is greater than *high*, than a target address is calculated by adding *default* to the address of the opcode of this *stableswitch* instruction. Otherwise, the offset at position *index* – *low* of the jump table is extracted. The target address is calculated by adding that offset to the address of the opcode of this *stableswitch* instruction. Execution then continues at the target address.

The target addresses that can be calculated from each jump table offset, as well as the one calculated from *default*, must be the address of an opcode of an instruction within the method that contains this *stableswitch* instruction.

sushr *sushr*

Logical shift right `short`

Format

sushr

Forms

sushr = 81 (0x51)

Stack

…, *value1*, *value2* ⇒
…, *result*

Description

Both *value1* and *value2* must be of type `short`. The values are popped from the operand stack. A `short` *result* is calculated by sign-extending *value1* to 32 bits and shifting the result right by *s* bit positions, with zero extension, where *s* is the value of the low five bits of *value2*. The resulting value is then truncated to a 16-bit *result*. The *result* is pushed onto the operand stack.

Notes

If *value1* is positive and *s* is *value2* & 0x1f, the result is the same as that of *value1* >> *s*; if *value1* is negative, the result is equal to the value of the expression (*value1* >> *s*) + (2 << ~*s*). The addition of the (2 << ~*s*) term cancels out the propagated sign bit. The shift distance actually used is always in the range 0 to 31, inclusive, as if *value2* were subjected to a bitwise logical AND with the mask value 0x1f.

swap_x *swap_x*

Swap top two operand stack words

Format

swap_x
mn

Forms

swap_x = 64 (0x40)

Stack

..., wordM+N, ..., wordM+1, wordM, ..., word1 ⇒
..., wordM, ..., word1, wordM+N, ..., wordM+1

Description

The unsigned byte *mn* is used to construct two parameter values. The high nibble, (*mn* & 0xf0) >> 4, is used as the value *m*. The low nibble, (*mn* & 0xf), is used as the value *n*. Permissible values for both *m* and *n* are 1 and 2.

The top *m* words on the operand stack are swapped with the *n* words immediately below.

The *swap_x* instruction must not be used unless the ranges of words 1 through *m* and words *m*+1 through *n* each contain either a 16-bit data type, two 16-bit data types, a 32-bit data type, a 16-bit data type and a 32-bit data type (in either order), or two 32-bit data types.

Notes

Except for restrictions preserving the integrity of 32-bit data types, the *swap_x* instruction operates on untyped words, ignoring the types of data they contain.

If a virtual machine does not support the `int` data type, the only permissible value for both *m* and *n* is 1.

sxor *sxor*

Boolean XOR `short`

Format

sxor

Forms

sxor = 87 (0x57)

Stack

…, *value1*, *value2* ⇒
…, *result*

Description

Both *value1* and *value2* must be of type `short`. The values are popped from the operand stack. A `short` *result* is calculated by taking the bitwise exclusive OR of *value1* and *value2*. The *result* is pushed onto the operand stack.

Appendix JCVM01

CHAPTER **8**

Tables of Instructions

TABLE 8-1 Instructions by Opcode Value

dec	hex	mnemonic	dec	hex	mnemonic
0	00	nop	47	2F	sstore_0
1	01	aconst_null	48	30	sstore_1
2	02	sconst_m1	49	31	sstore_2
3	03	sconst_0	50	32	sstore_3
4	04	sconst_1	51	33	istore_0
5	05	sconst_2	52	34	istore_1
6	06	sconst_3	53	35	istore_2
7	07	sconst_4	54	36	istore_3
8	08	sconst_5	55	37	aastore
9	09	iconst_m1	56	38	bastore
10	0A	iconst_0	57	39	sastore
11	0B	iconst_1	58	3A	iastore
12	0C	iconst_2	59	3B	pop
13	0D	iconst_3	60	3C	pop2
14	0E	iconst_4	61	3D	dup
15	0F	iconst_5	62	3E	dup2
16	10	bspush	63	3F	dup_x
17	11	sspush	64	40	swap_x
18	12	bipush	65	41	sadd
19	13	sipush	66	42	iadd
20	14	iipush	67	43	ssub
21	15	aload	68	44	isub
22	16	sload	69	45	smul
23	17	iload	70	46	imul
24	18	aload_0	71	47	sdiv
25	19	aload_1	72	48	idiv
26	1A	aload_2	73	49	srem
27	1B	aload_3	74	4A	irem
28	1C	sload_0	75	4B	sneg
29	1D	sload_1	76	4C	ineg
30	1E	sload_2	77	4D	sshl
31	1F	sload_3	78	4E	ishl
32	20	iload_0	79	4F	sshr
33	21	iload_1	80	50	ishr
34	22	iload_2	81	51	sushr
35	23	iload_3	82	52	iushr
36	24	aaload	83	53	sand
37	25	baload	84	54	iand
38	26	saload	85	55	sor
39	27	iaload	86	56	ior
40	28	astore	87	57	sxor
41	29	sstore	88	58	ixor
42	2A	istore	89	59	sinc
43	2B	astore_0	90	5A	iinc
44	2C	astore_1	91	5B	s2b
45	2D	astore_2	92	5C	s2i
46	2E	astore_3	93	5D	i2b

Table 8-1 (continued) Instructions by Opcode Value

dec	hex	mnemonic	dec	hex	mnemonic
94	5E	i2s	141	8D	invokestatic
95	5F	icmp	142	8E	invokeinterface
96	60	ifeq	143	8F	new
97	61	ifne	144	90	newarray
98	62	iflt	145	91	anewarray
99	63	ifge	146	92	arraylength
100	64	ifgt	147	93	athrow
101	65	ifle	148	94	checkcast
102	66	ifnull	149	95	instanceof
103	67	ifnonnull	150	96	sinc_w
104	68	if_acmpeq	151	97	iinc_w
105	69	if_acmpne	152	98	ifeq_w
106	6A	if_scmpeq	153	99	ifne_w
107	6B	if_scmpne	154	9A	iflt_w
108	6C	if_scmplt	155	9B	ifge_w
109	6D	if_scmpge	156	9C	ifgt_w
110	6E	if_scmpgt	157	9D	ifle_w
111	6F	if_scmple	158	9E	ifnull_w
112	70	goto	159	9F	ifnonnull_w
113	71	jsr	160	A0	if_acmpeq_w
114	72	ret	161	A1	if_acmpne_w
115	73	stableswitch	162	A2	if_scmpeq_w
116	74	itableswitch	163	A3	if_scmpne_w
117	75	slookupswitch	164	A4	if_scmplt_w
118	76	ilookupswitch	165	A5	if_scmpge_w
119	77	areturn	166	A6	if_scmpgt_w
120	78	sreturn	167	A7	if_scmple_w
121	79	ireturn	168	A8	goto_w
122	7A	return	169	A9	getfield_a_w
123	7B	getstatic_a	170	AA	getfield_b_w
124	7C	getstatic_b	171	AB	getfield_s_w
125	7D	getstatic_s	172	AC	getfield_i_w
126	7E	getstatic_i	173	AD	getfield_a_this
127	7F	putstatic_a	174	AE	getfield_b_this
128	80	putstatic_b	175	AF	getfield_s_this
129	81	putstatic_s	176	B0	getfield_i_this
130	82	putstatic_i	177	B1	putfield_a_w
131	83	getfield_a	178	B2	putfield_b_w
132	84	getfield_b	179	B3	putfield_s_w
133	85	getfield_s	180	B4	putfield_i_w
134	86	getfield_i	181	B5	putfield_a_this
135	87	putfield_a	182	B6	putfield_b_this
136	88	putfield_b	183	B7	putfield_s_this
137	89	putfield_s	184	B8	putfield_i_this
138	8A	putfield_i			…
139	8B	invokevirtual	254	FE	impdep1
140	8C	invokespecial	255	FF	impdep2

TABLE 8-2 Instructions by Opcode Mnemonic

mnemonic	dec	hex	mnemonic	dec	hex
aaload	36	24	iand	84	54
aastore	55	37	iastore	58	3A
aconst_null	1	01	icmp	95	5F
aload	21	15	iconst_0	10	0A
aload_0	24	18	iconst_1	11	0B
aload_1	25	19	iconst_2	12	0C
aload_2	26	1A	iconst_3	13	0D
aload_3	27	1B	iconst_4	14	0E
anewarray	145	91	iconst_5	15	0F
areturn	119	77	iconst_m1	9	09
arraylength	146	92	idiv	72	48
astore	40	28	if_acmpeq	104	68
astore_0	43	2B	if_acmpeq_w	160	A0
astore_1	44	2C	if_acmpne	105	69
astore_2	45	2D	if_acmpne_w	161	A1
astore_3	46	2E	if_scmpeq	106	6A
athrow	147	93	if_scmpeq_w	162	A2
baload	37	25	if_scmpge	109	6D
bastore	56	38	if_scmpge_w	165	A5
bipush	18	12	if_scmpgt	110	6E
bspush	16	10	if_scmpgt_w	166	A6
checkcast	148	94	if_scmple	111	6F
dup	61	3D	if_scmple_w	167	A7
dup_x	63	3F	if_scmplt	108	6C
dup2	62	3E	if_scmplt_w	164	A4
getfield_a	131	83	if_scmpne	107	6B
getfield_a_this	173	AD	if_scmpne_w	163	A3
getfield_a_w	169	A9	ifeq	96	60
getfield_b	132	84	ifeq_w	152	98
getfield_b_this	174	AE	ifge	99	63
getfield_b_w	170	AA	ifge_w	155	9B
getfield_i	134	86	ifgt	100	64
getfield_i_this	176	B0	ifgt_w	156	9C
getfield_i_w	172	AC	ifle	101	65
getfield_s	133	85	ifle_w	157	9D
getfield_s_this	175	AF	iflt	98	62
getfield_s_w	171	AB	iflt_w	154	9A
getstatic_a	123	7B	ifne	97	61
getstatic_b	124	7C	ifne_w	153	99
getstatic_i	126	7E	ifnonnull	103	67
getstatic_s	125	7D	ifnonnull_w	159	9F
goto	112	70	ifnull	102	66
goto_w	168	A8	ifnull_w	158	9E
i2b	93	5D	iinc	90	5A
i2s	94	5E	iinc_w	151	97
iadd	66	42	iipush	20	14
iaload	39	27	iload	23	17

Table 8-2 (continued) Instructions by Opcode Mnemonic

mnemonic	dec	hex	mnemonic	dec	hex
iload_0	32	20	putstatic_s	129	81
iload_1	33	21	ret	114	72
iload_2	34	22	return	122	7A
iload_3	35	23	s2b	91	5B
ilookupswitch	118	76	s2i	92	5C
imul	70	46	sadd	65	41
ineg	76	4C	saload	38	26
instanceof	149	95	sand	83	53
invokeinterface	142	8E	sastore	57	39
invokespecial	140	8C	sconst_0	3	03
invokestatic	141	8D	sconst_1	4	04
invokevirtual	139	8B	sconst_2	5	05
ior	86	56	sconst_3	6	06
irem	74	4A	sconst_4	7	07
ireturn	121	79	sconst_5	8	08
ishl	78	4E	sconst_m1	2	02
ishr	80	50	sdiv	71	47
istore	42	2A	sinc	89	59
istore_0	51	33	sinc_w	150	96
istore_1	52	34	sipush	19	13
istore_2	53	35	sload	22	16
istore_3	54	36	sload_0	28	1C
isub	68	44	sload_1	29	1D
itableswitch	116	74	sload_2	30	1E
iushr	82	52	sload_3	31	1F
ixor	88	58	slookupswitch	117	75
jsr	113	71	smul	69	45
new	143	8F	sneg	75	4B
newarray	144	90	sor	85	55
nop	0	00	srem	73	49
pop	59	3B	sreturn	120	78
pop2	60	3C	sshl	77	4D
putfield_a	135	87	sshr	79	4F
putfield_a_this	181	B5	sspush	17	11
putfield_a_w	177	B1	sstore	41	29
putfield_b	136	88	sstore_0	47	2F
putfield_b_this	182	B6	sstore_1	48	30
putfield_b_w	178	B2	sstore_2	49	31
putfield_i	138	8A	sstore_3	50	32
putfield_i_this	184	B8	ssub	67	43
putfield_i_w	180	B4	stableswitch	115	73
putfield_s	137	89	sushr	81	51
putfield_s_this	183	B7	swap_x	64	40
putfield_s_w	179	B3	sxor	87	57
putstatic_a	127	7F			
putstatic_b	128	80			
putstatic_i	130	82			

Glossary

AID is an acronym for Application IDentifier as defined in ISO 7816-5.

API is an acronym for Application Programming Interface. The API defines calling conventions by which an application program accesses the operating system and other services.

Applet is the basic unit of selection, context, functionality, and security in Java Card technology.

Applet developer refers to a person creating a Java Card applet using the Java Card technology specifications.

Atomic operation is an operation that either completes in its entirety (if the operation succeeds) or no part of the operation completes at all (if the operation fails).

Atomicity refers to whether a particular operation is atomic or not and is necessary for proper data recovery in cases where power is lost or the card is unexpectedly removed from the CAD.

Cast is the explicit conversion from one data type to another.

Class is the prototype for an object in an object-oriented language. A class may also be considered a set of objects which share a common structure and behavior. The structure of a class is determined by the class variables which represent the state of an object of that class and the behavior is given by a set of methods associated with the class.

Classes are related in a class hierarchy. One class may be a specialization (a “subclass”) of another (one of its “superclasses”), it may be composed of other classes, or it may use other classes in a client-server relationship.

Context is the object space partition associated with a package. Applets within the same Java package belong to the same context. The firewall is the boundary between contexts (see Current context).

Current context. The JCRE keeps track of the current Java Card context. When a virtual method is invoked on an object, and a context switch is required and permitted, the current context is changed to correspond to the context of the applet that owns the object. When that method returns, the previous context is restored. Invocations of static methods have no effect on the current context. The current context and sharing status of an object together determine if access to an object is permissible.

Firewall is the mechanism in the Java Card technology by which the Java Card VM prevents an applet in one context from making unauthorized accesses to objects owned by an applet in another context or the JCRE context, and reports or otherwise addresses the violation.

Framework is the set of classes which implement the API. This includes core and extension packages. Responsibilities include dispatching of APDUs, applet selection, managing atomicity, and installing applets.

Garbage collection is the process by which dynamically allocated storage is automatically reclaimed during the execution of a program.

Instance variables (also known as *fields*) represent a portion of an object's internal state. Each object has its own set of instance variables. Objects of the same class will have the same instance variables, but each object can have different values.

Instantiation (in object-oriented programming) means to produce a particular object from its class template. This involves allocation of a data structure with the types specified by the template, and initialization of instance variables with either default values or those provided by the class's constructor function.

JAR is an acronym for Java Archive. JAR is a platform-independent file format that combines many files into one.

Java Card Runtime Environment (JCRE) consists of the Java Card Virtual Machine, the framework, and the associated native methods.

JCRE implementer refers to a person creating a vendor-specific framework using the Java Card 2.1 API.

JCVM is an acronym for the Java Card Virtual Machine. The JCVM executes byte code and manages classes and objects. It enforces separation between applets (firewalls) and enables secure data sharing.

Method is the name given to a procedure or routine, associated with one or more classes, in object-oriented languages.

Namespace is a set of names in which all names are unique.

Object-Oriented is a programming methodology based on the concept of an "object" which is a data structure encapsulated with a set of routines, called "methods," which operate on the data.

Objects, in object-oriented programming, are unique instances of a data structure defined according to the template provided by its class. Each object has its own values for the variables belonging to its class and can respond to the messages (methods) defined by its class.

Package is a namespace within the Java programming language and can have classes and interfaces. A package is the smallest unit within the Java programming language.

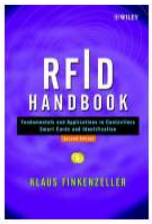
Appendix JCVM01

screenshot-catalog.libraries.psu.edu-2022.04.22-11_35_05
https://catalog.libraries.psu.edu/catalog/2447992/marc_view
22.04.2022

MARC View

LEADER 01663cam a22004094a 4500				
001 2447992				
003 SIRSI				
005 20151215052937.0				
008 021210t20032003enka b 001 0 eng				
010			a| 2002192439	
019			a| MARS	
020			a| 0470844027 (alk. paper)	
035			a| (OCoLC)51242225	
040			a| DLC c| DLC d| C#P d| UtOrBLW	
041	1		a| eng h| ger	
042			a| pcc	
049			a| UPMM	
050	0	0	a| TS160 b| .F5513 2003	
082	0	0	a| 658.7/87 2| 21	
100	1		a| Finkenzeller, Klaus.	
240	1	0	a| RFID Handbuch. l| English	
245	1	0	a| RFID handbook : b| fundamentals and applications in contactless smart cards and identification / c| Klaus Finkenzeller ; translated by Rachel Waddington.	
250			a| 2nd ed.	
264		1	a| Chichester, England ; a| New York : b| Wiley, c| [2003]	
264		4	c| ©2003	
300			a| xviii, 427 pages : b| illustrations ; c| 26 cm	
336			a| text b| txt 2| rdacontent	
337			a| unmediated b| n 2| rdamedia	
338			a| volume b| nc 2| rdacarrier	
504			a| Includes bibliographical references and index.	
650		0	a| Inventory control x| Automation.	
650		0	a| Radio frequency identification systems.	
650		0	a| Smart cards.	
541			3| Engineering copy: c| Purchased with funds from the a| William L. and Josephine Berry Weiss Special Initiative Fund; d| 20023. 5| PSt.	
949			a| TS160.F5513 2003 w| LC c| 1 i| 000057203508 d| 1/12/2017 e| 9/26/2016 l| STACKS-BD m| BEHREND n| 4 r| Y s| Y t| BOOKFLOAT u| 12/5/2005	
949			a| TS160.F5513 2003 w| LC c| 1 i| 000050767380 d| 12/15/2011 e| 12/2/2011 l| CATO-2 m| UP-ANNEX n| 46 r| Y s| Y t| BOOK u| 6/6/2003 z| 8136	
949			a| TS160.F5513 2003 w| LC c| 1 i| 000051607531 l| STACKS-AB m| ABINGTON r| Y s| Y t| BOOKFLOAT u| 12/5/2007	

screenshot-catalog.libraries.psu.edu-2022.04.22-11_34_51
https://catalog.libraries.psu.edu/catalog/2447992/marc_view
22.04.2022



RFID handbook : fundamentals and applications in contactless smart cards and identification / Klaus Finkenzeller ; translated by Rachel Waddington

Author:	Finkenzeller, Klaus
Uniform Title:	RFID Handbuch. English
Published:	Chichester, England ; New York : Wiley, [2003]
Copyright Date:	©2003
Edition:	2nd ed.
Physical Description:	xviii, 427 pages : illustrations ; 26 cm

Availability

Penn State Abington (1 item)

Call number	Material	Location
TS160.F5513 2003	Book	Being transferred between libraries

Penn State Behrend (1 item)

Call number	Material	Location
TS160.F5513 2003	Book	Stacks - General Collection

Library Storage (1 item)

Call number	Material	Location
TS160.F5513 2003	Book	Annexed Material

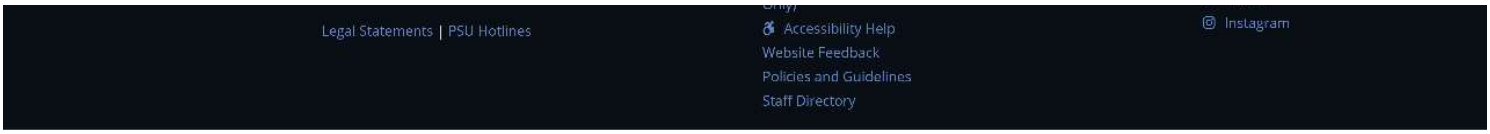
Subject(s):
Inventory control—Automation
Radio frequency identification systems
Smart cards

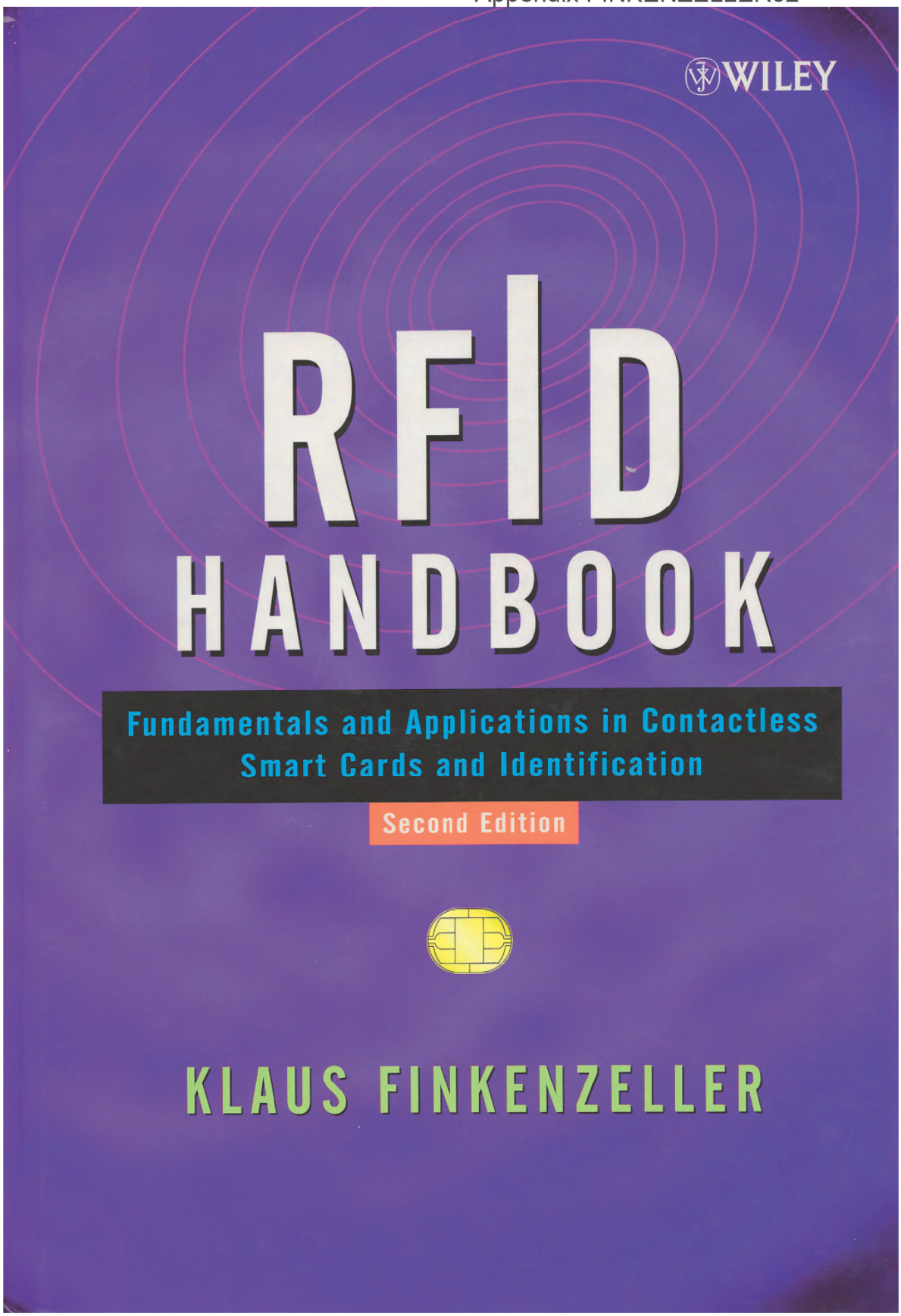
ISBN:
0470844027 (alk. paper)

Bibliography Note:
Includes bibliographical references and index.

Source of Acquisition:
Engineering copy: Purchased with funds from the William L. and Josephine Berry Weiss Special Initiative Fund; 20023.

Appendix FINKENZELLER01




WILEY
RFID
HANDBOOK
Fundamentals and Applications in Contactless Smart Cards and Identification
Second Edition
KLAUS FINKENZELLER

RFID HANDBOOK

Fundamentals and Applications in Contactless Smart Cards and Identification

Second Edition

KLAUS FINKENZELLER

Giesecke & Devrient GmbH, Munich, Germany

Translated by Rachel Waddington, *Swadlincote, UK*

Developments in RFID (Radio-Frequency Identification) are yielding larger memory capacities, wider reading ranges and quicker processing, making it one of the fastest growing sectors of the radio technology industry.

RFID has become indispensable in a wide range of automated data capture and identification applications, from ticketing and access control to industrial automation. The second edition of Finkenzeller's comprehensive handbook brings together the disparate information on this versatile technology. Features include:

- Essential new information on the industry standards and regulations, including ISO 14443 (contactless ticketing), ISO 15693 (smartlabel) and ISO 14223 (animal identification).
- Complete coverage of the physical principles behind RFID technologies such as inductive coupling, surface acoustic waves and the emerging UHF and microwave backscatter systems.
- A detailed description of common algorithms for anticollision.
- An exhaustive appendix providing listings of RFID associations, journals and standards.
- A sample test card layout in accordance with ISO 14443.
- Numerous sample applications including e-ticketing in public transport systems and animal identification.

End users of RFID products, electrical engineering students and newcomers to the field will value this introduction to the functionality of RFID technology and the physical principles involved. Experienced ADC professionals will benefit from the breadth of applications examples combined within this single resource.

WILEY
wiley.com

ISBN 0-470-84402-7
9 780470 844021

RFID Handbook

Second Edition

RFID Handbook

Fundamentals and Applications in Contactless Smart Cards and Identification

Second Edition

Klaus Finkenzeller
Giesecke & Devrient GmbH, Munich, Germany

Translated by
Rachel Waddington
Member of the Institute of Translation and Interpreting

WILEY

First published under the title *RFID-Handbuch, 2 Auflage* by Carl Hanser Verlag

Authorized translation from the 2nd edition in the original German language
published by Carl Hanser Verlag, Munich/FRG

Copyright © 2003 John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester,
West Sussex PO19 8SQ, England

Telephone (+44) 1243 779777

Email (for orders and customer service enquiries): cs-books@wiley.co.uk
Visit our Home Page on www.wileyeurope.com or www.wiley.com

Other Wiley Editorial Offices

John Wiley & Sons Inc., 111 River Street, Hoboken, NJ 07030, USA

Jossey-Bass, 989 Market Street, San Francisco, CA 94103-1741, USA

Wiley-VCH Verlag GmbH, Boschstr. 12, D-69469 Weinheim, Germany

John Wiley & Sons Australia Ltd, 33 Park Road, Milton, Queensland 4064, Australia

John Wiley & Sons (Asia) Pte Ltd, 2 Clementi Loop #02-01, Jin Xing Distripark, Singapore 129809

John Wiley & Sons Canada Ltd, 22 Worcester Road, Etobicoke, Ontario, Canada M9W 1L1

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Library of Congress Cataloging-in-Publication Data

Finkenzeller, Klaus.
[RFID Handbuch. English]
RFID handbook : fundamentals and applications in contactless smart cards and identifcation/Klaus Finkenzeller; translated by Rachel Waddington. — 2nd ed.
p. cm.
Includes bibliographical references and index.
ISBN 0-470-84402-7 (alk. paper)
1. Inventory control — Automation. 2. Radio frequency identification systems. 3. Smart. cards. I. Title.

TS160.F5513 2003
658.7′87 — dc21

2002192439

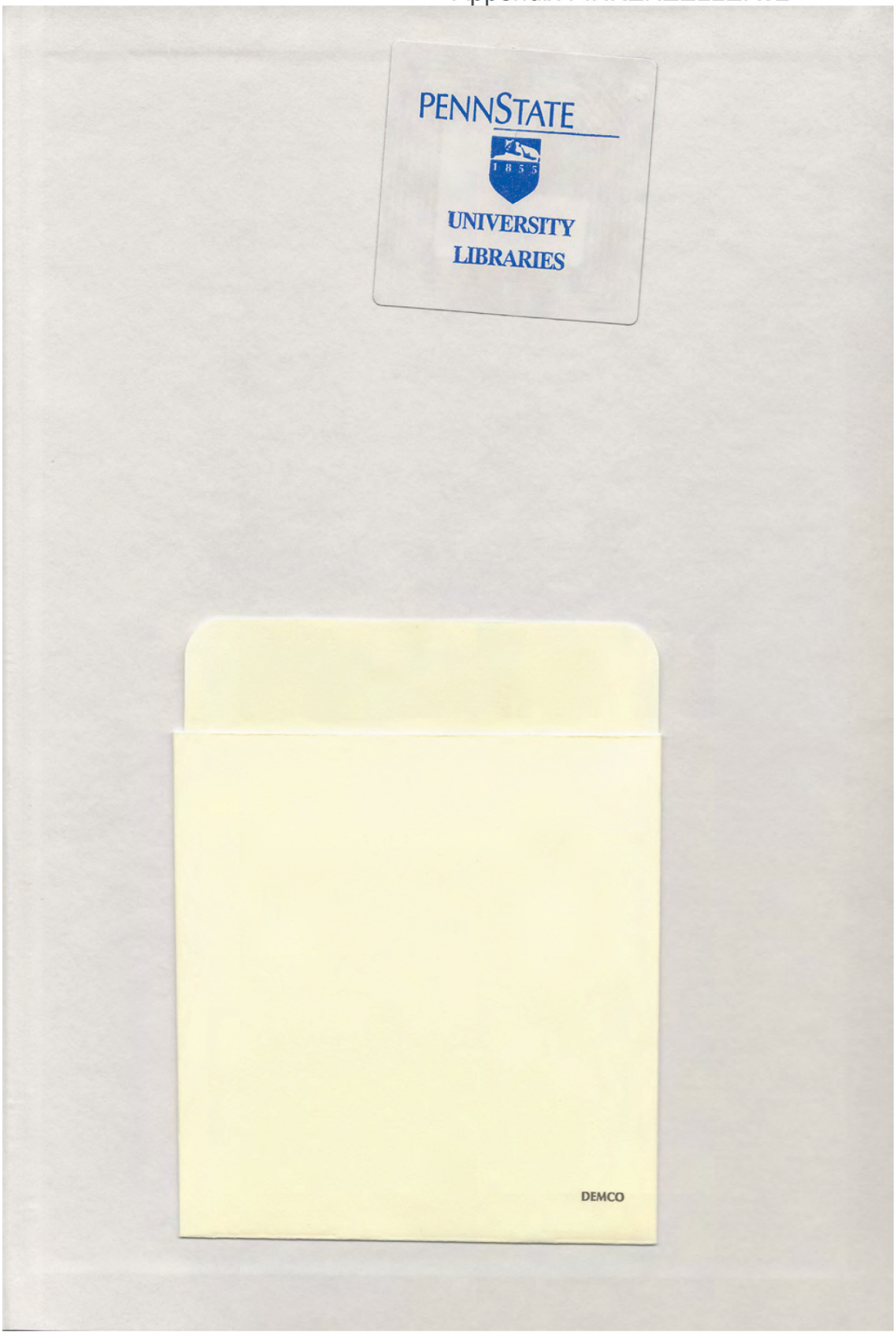
British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN 0-470-84402-7

Typeset in 10/12pt Times by Laserwords Private Limited, Chennai, India
Printed and bound in Great Britain by Antony Rowe Ltd, Chippenham, Wiltshire
This book is printed on acid-free paper responsibly manufactured from sustainable forestry in which at least two trees are planted for each one used for paper production.

Contents


PENNSTATE
1855
UNIVERSITY
LIBRARIES
DEMCO