GLOBALPLATFORM

ADVANCING STANDARDS FOR SMART CARD GROWTH

GlobalPlatform

Card Specification

Version 2.1.1

March 2003

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights or other intellectual property rights of which they may be aware which might be infringed by the implementation of the specification set forth in this document, and to provide supporting

DOCKET ALARM

Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

Table of Contents

1. INTRODUCTION 16

1.1 Audience 16

1.2 Normative References 17

1.3 Terminology and Definitions 17

1.4 Abbreviations and Notations 20

1.5 Revisions History 21
1.5.1 Open Platform Card Specification v2.0 to Open Platform Card Specification v2.0.1 21
1.5.2 Major Adjustments in GlobalPlatform Card Specification V2.1 22
1.5.3 Revisions in GlobalPlatform Card Specification V2.1.1 24

2. SYSTEM ARCHITECTURE 27

3. CARD ARCHITECTURE 28

3.1 Runtime Environment 29

3.2 Card Manager 29
3.2.1 GlobalPlatform Environment (OPEN) 29
3.2.2 Issuer Security Domain 30
3.2.3 Cardholder Verification Management 30

3.3 Security Domains 30

3.4 GlobalPlatform API 30

3.5 Card Content 31

4. SECURITY ARCHITECTURE 32

4.1 Goals 32

4.2 Security Responsibilities 33
4.2.1 Card Issuer's Security Responsibilities 33
4.2.2 Application Provider's Security Responsibilities 33
4.2.3 Controlling Authority's Security Responsibilities 33
4.2.4 On-Card Components' Security Requirements 34
4.2.5 Back-End System Security Requirements 35

Copyright © 2003 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

4.3 Cryptographic support 36
4.3.1 Integrity and Authentication for Card Content Management 36
4.3.2 Secure Communication 37

5. LIFE CYCLE MODELS 39

5.1 Card Life Cycle 39
5.1.1 Card Life Cycle States 39
5.1.2 Card Life Cycle Transitions 42

5.2 Executable Load File/ Executable Module Life Cycle 43
5.2.1 Executable Load File Life Cycle 43
5.2.2 Executable Module Life Cycle 43

5.3 Application and Security Domain Life Cycle 43
5.3.1 Application Life Cycle States 44
5.3.2 Security Domain Life Cycle States 47

5.4 Sample Life Cycle Illustration 49

6. CARD MANAGER 51

6.1 Card Manager Overview 51
6.1.1 OPEN 51
6.1.2 Issuer Security Domain 53
6.1.3 CVM Handler 53

6.2 Card Manager Services 53
6.2.1 Application Access to OPEN Services 53
6.2.2 Application Access to CVM Services 54
6.2.3 Application Access to Issuer Security Domain Services 54
6.2.4 Issuer Security Domain Access to Applications 55

6.3 Command Dispatch 55
6.3.1 Basic Logical Channel 56
6.3.2 Supplementary Logical Channel 59

6.4 Card Content Management 62
6.4.1 Card Content Loading and Installation 62
6.4.2 Content Removal 67
6.4.3 Content Extradition 70

6.5 Delegated Management 71

6.6 GlobalPlatform Registry 72
6.6.1 Issuer Security Domain Data Elements Description 72
6.6.2 Application/Executable Load File/Executable Module Data Elements 73

Copyright © 2003 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

6.7 Security Management 76
6.7.1 Application Locking 76
6.7.2 Card Locking 77
6.7.3 Card Termination 78
6.7.4 Operational Velocity Checking 79
6.7.5 Tracing and Event Logging 80
6.7.6 Securing Content Loading and Installation 80

6.8 Issuer Security Domain 81
6.8.1 Issuer Identification Number 82
6.8.2 Card Image Number 82
6.8.3 Card Recognition Data 82
6.8.4 On-Card Key Information 83

6.9 CVM Management 84
6.9.1 CVM States 84
6.9.2 CVM Format 85

7. SECURITY DOMAINS 86

7.1 Overview 86

7.2 Security Domain Services 87
7.2.1 Application Access to Security Domain Services 87
7.2.2 Security Domain Access to Applications 88

7.3 Personalization Support 88

7.4 Runtime Messaging Support 90

7.5 DAP Verification 91

7.6 Delegated Management 91
7.6.1 Delegated Loading 92
7.6.2 Delegated Installation 92
7.6.3 Delegated Extradition 95
7.6.4 Delegated Deletion 95

7.7 Delegated Management Tokens and Receipts and DAP Verification 96
7.7.1 Load Token 97
7.7.2 Load Receipt 97
7.7.3 Install and Extradition Tokens 98
7.7.4 Install Receipt 98
7.7.5 Extradition Receipt 99
7.7.6 Delete Receipt 99
7.7.7 Load File Data Block Hash 99
7.7.8 Load File Data Block Signature (DAP Verification) 100

Copyright © 2003 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.