



Guide to Common Personalization

*Version 1.0
March 2003*

Table of Contents

1. Document Overview	1
1.1 Scope	1
1.2 Intended Audience	1
1.3 Document Structure	1
1.4 Normative References	2
1.5 Abbreviations and Notations	2
2. Overview of the Common Personalization Process	6
2.1 The Infrastructure of Common Personalization	6
2.2 Secure Messaging	7
2.3 The STORE DATA Command and Data Groupings	7
2.4 The Data Container Format	8
2.5 Common Personalization and CAMS	10
2.5.1 Data Preparation	11
2.5.2 Personalization Device Processing	12
2.5.3 IC Card Application Processing	12
2.6 Process Overview	13
3. Data Preparation	16
3.1 Creating Personalization Data	16
3.1.1 Application Provider Master Keys and Data	16
3.1.2 Application Keys and Certificates	16
3.1.3 Application Data	17
3.2 Creation of Data Groupings	17
3.3 DGIs Defined by Common Personalization	18
3.3.1 Completion of Personalization	18
3.3.2 Restricting the STORE DATA Command after Personalization	18
3.3.3 Replacing the initial Security Domain key(s) after Personalization	18
3.4 Multiple Transport Key Capability	20
3.5 Processing Step	21
3.6 Creation of Personalization Device Instructions (Processing Step '0F')	21
3.6.1 Order that Data must be sent to the Smart Card	22
3.6.2 Support for Migration to New Versions	22
3.6.3 Encrypted Data Groupings	23
3.6.4 PIN Block Format	24
3.6.5 Random Number for Processing	24
3.6.6 Group of DGIs in one STORE DATA command	24
3.6.7 The PDI Field	25
3.6.8 ICC Data populated with DGIs	26
3.7 Pre-computed APDU Commands (Processing Step '0B')	27
3.7.1 Types of pre-computed APDU Commands	27
3.7.2 Coding of APDU Commands	27
3.7.3 ICC Data populated with pre-computed APDUs	28
3.8 Creation of Personalization Log Data	29
4. Personalization Device Processing	30
4.1 Processing Step with code action '0F'	30
4.1.1 Key Management	30
4.1.2 Processing Flow	31
4.1.3 Return Data From Smart Card application	39
4.2 Processing Step with code action '0B'	40

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 information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

4.2.1	Syntax Checking	40
4.2.2	Types of data elements in ICC Return data field	41
4.2.3	Coding of ICC Return Data Field	41
4.2.4	Abstraction from transport layer	42
4.3	Personalization Log Creation	43
5.	IC Card Processing	44
5.1	Preparation for Personalization	44
5.2	Personalization	44
5.2.1	Smart Card Requirements	44
5.2.2	Command Support	44
5.2.3	Secure Messaging	44
6.	Cryptography for Personalization	45
6.1	Key Zones	45
6.2	Session Keys	46
6.3	MACs	46
6.4	Encryption	46
6.5	Decryption	46
6.6	DES Calculations	47
7.	Data Dictionary	48
7.1	List of data elements	48
7.1.1	ACT (Action to be Performed)	48
7.1.2	AID (Application Identifier)	48
7.1.3	CMK (Final Master Key)	48
7.1.4	CMODE (Chaining Mode)	48
7.1.5	DTHR (Date and Time)	48
7.1.6	ENC (Encryption Personalization Instructions)	48
7.1.7	GROUP (Group of Data Grouping as part of Personalization Instructions)	49
7.1.8	ID _{TK} (Identifier of the Transport Key)	49
7.1.9	ID _{OWNER} (Identifier of the Application Specification Owner)	49
7.1.10	ID _{TERM} (Identifier of the Personalization Device)	49
7.1.11	ISSUERID (Issuer Identifier Data for Personalization)	49
7.1.12	K _{ENC} (DES Key for Creating Personalization Session Key for Secret Data Encryption)	49
7.1.13	K _{KEK} (DES Key for Creating Personalization Session Key for DES Key Encryption)	49
7.1.14	K _{MAC} (DES Key for Creating Personalization Session Key for MACs)	50
7.1.15	KEYDATA (Derivation Data for Initial Update Keys)	50
7.1.16	KMC (DES Master Key for Personalization Session Keys)	50
7.1.17	L (Length of Data)	50
7.1.18	LOGDATA (Data Logging Personalization Instructions)	50
7.1.19	MAC _{INP} (MAC of All Data for an Application)	50
7.1.20	MACkey (MAC Key)	50
7.1.21	MIC (Module Identifier Code)	50
7.1.22	ORDER (Data Grouping Order Personalization Instructions)	51
7.1.23	R _{CARD} (Random Number from the Smart Card)	51
7.1.24	R _{TERM} (Random Number from the Personalization Device)	51
7.1.25	RANDOM (Random Number)	51
7.1.26	REQ (Required or Optional Action)	51
7.1.27	SEQNO (Sequence Number)	51
7.1.28	SKU _{ENC} (Personalization Session Key for Encryption)	51
7.1.29	SKU _{DEK} (Personalization Session Key for Secret Data Exchange)	51
7.1.30	SKU _{MAC} (Personalization Session Key for MACing)	52
7.1.31	TAG (Identifier of Data for a Processing Step)	52
7.1.32	TK (Transport Key)	52

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 information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

7.1.33	<i>TYPE_{TK} (Indicator of Use(s) of Transport Key)</i>	52
7.1.34	<i>VERCNTL (Version Control Personalization Instructions)</i>	53
8.	<i>Examples of document</i>	54
8.1	Examples of Data Groupings	54
8.1.1	<i>CPS Demonstrator</i>	54
8.2	Examples of Personalization Device Instructions	56
8.2.1	<i>CPS Demonstrator</i>	56
8.3	Completion of Personalization	57
8.3.1	<i>CPS Demonstrator</i>	57
9.	<i>Examples of APDU mapping to T=0 TPDU</i>	58

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 information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Table of Figures

Figure 2-1 – Personalization Data by MIC.....	8
Figure 2-2 – Overview of Smart Card Personalization Data Format.....	9
Figure 2-3 – Overview of Personalization Data for a Single Smart Card Application.....	9
Figure 2-4 – CAMS Architecture Diagram.....	11
Figure 2-5 – Example Personalization Data Layout for one application.....	12
Figure 2-6 – Example of Personalization Data for one Application for one Card.....	13
Figure 2-7 – Personalization Input File for One Card.....	13
Figure 2-8 – Interface between the SCMS and the Loader.....	14
Figure 2-9 – Interface between the SCMS and the Personalization device.....	15
Figure 3-1 – Layout of ICC Data Portion of Record.....	26
Figure 3-2 – Formatting of Personalization Data within ICC Data Portion of Record.....	26
Figure 3-3 – Pre-computed APDU Command placed in BER–TLV structure.....	27
Figure 3-4 – Layout of ICC Data Portion of Record.....	28
Figure 3-5 – Formatting of Personalization Data within ICC Data Portion of Record.....	29
Figure 4-1 – Personalization Command Flow with Explicit Initiation SCP.....	32
Figure 4-2 – Personalization Command Flow with Implicit Initiation SCP.....	33
Figure 6-1 – Common Personalization Key Zones.....	45
Figure 6-2 – Common Personalization Key Zone in pre-computed APDU commands.....	45

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 information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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.