

EMV Card Personalization Specification

Version 1.0
June 2003

© 2003 EMVCo, LLC ("EMVCo"). All rights reserved. Any and all uses of the EMV Card Personalization Specification ("Materials") shall be permitted only pursuant to the terms and conditions of the license agreement between the user and EMVCo found at <http://www.emvco.com/specifications.cfm>.

The specifications, standards and methods set forth in these Materials have not been finalized or adopted by EMVCo and should be viewed as "work-in-process" subject to change at anytime without notice. EMVCo makes no assurances that any future version of these Materials or any version of the EMV Card Personalization Specification will be compatible with these Materials. No party should detrimentally rely on this draft document or the contents thereof, nor shall EMVCo be liable for any such reliance. These Materials are being provided for the sole purpose of evaluation and comment by the person or entity which downloads the Materials from the EMVCo web site ("User"). The Materials may not be copied or disseminated to any third parties, [except that permission is granted to internally disseminate copies within the organization of the User]. Any copy of any part of the Materials must bear this legend in full. These Materials and all of the content contained herein are provided "AS IS" "WHERE IS" and "WITH ALL FAULTS" and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in these materials. MATERIALS AND INFORMATION PROVIDED BY EMVCO ARE NOT FINAL AND MAY BE AMENDED AT EMVCO'S SOLE OPTION. EMVCO MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO THE MATERIALS AND INFORMATION CONTAINED HEREIN. EMVCO SPECIFICALLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, AND FITNESS FOR A PARTICULAR PURPOSE. EMVCo makes no representation or warranty with respect to intellectual property rights of any third parties in or in relation to the Materials. EMVCo undertakes no responsibility of any kind to determine whether any particular physical implementation of any part of these Materials may violate, infringe, or otherwise use the patents, copyrights, trademarks, trade secrets, know-how, and/or other intellectual property rights of third parties, and thus any person who implements any part of these Materials should consult an intellectual property attorney before any such implementation. WITHOUT LIMITATION, EMVCO SPECIFICALLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES WITH RESPECT TO INTELLECTUAL PROPERTY SUBSISTING IN OR RELATING TO THESE MATERIALS OR ANY PART THEREOF, INCLUDING BUT NOT LIMITED TO ANY AND ALL IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT OR SUITABILITY FOR ANY PURPOSE (WHETHER OR NOT EMVCO HAS BEEN ADVISED, HAS REASON TO KNOW, OR IS OTHERWISE IN FACT AWARE OF ANY INFORMATION). Without limitation to the foregoing, the Materials provide for the use of public key encryption technology, which is the subject matter of patents in several countries. Any party seeking to implement these Materials is solely responsible for determining whether their activities require a license to any technology including, but not limited to, patents on public key encryption technology. EMVCo shall not be liable under any theory for any party's infringement of any intellectual property rights.

THIS PAGE LEFT INTENTIONALLY BLANK

Table of Contents

1.	Purpose	v
2.	Scope	vi
3.	Audience	vii
4.	Normative References	viii
5.	Definitions	ix
6.	Abbreviations and Notations	x
1	Card Personalization Data Processing	1
1.1	Overview of the Process	1
1.2	The Infrastructure of Card Personalization	2
1.3	Secure Messaging	3
1.4	The STORE DATA Command	3
1.5	The Common Personalization Record Format	4
2	Data Preparation	7
2.1	Creating Personalization Data	7
2.1.1	Issuer Master Keys and Data	7
2.1.2	EMV Application Keys and Certificates	8
2.1.3	Application Data	8
2.2	Creation of Data Groupings	9
2.3	Completion of Personalization	10
2.3.1	Multiple Transport Key Capability	11
2.4	Processing Steps and Personalization Device Instructions	11
2.4.1	Order that Data must be sent to the IC Card	12
2.4.2	Support for Migration to New Versions	13
2.4.3	Encrypted Data Groupings	14
2.4.4	PIN Block Format and Random Numbers	14
2.4.5	Grouping of DGIs	15
2.5	Creation of Personalization Log Data	16
2.6	Data Preparation-Personalization Device Interface Format	16
3	Personalization Device-ICC Interface	25
3.1	Key Management	26
3.2	Processing Flow	26
3.2.2	SELECT Command	27
3.2.3	INITIALIZE UPDATE Command	28
3.2.4	EXTERNAL AUTHENTICATE Command	30
3.2.5	STORE DATA Command	32
3.2.6	Last STORE DATA Command	36
3.3	Command Responses	36
3.4	Personalization Log Creation	36
4	IC Card Personalization Processing	39
4.1	Preparation for Personalization (Pre-Personalization)	39
4.2	Personalization Requirements	40
4.2.1	IC Card Requirements	40
4.2.2	Command Support	40
4.2.3	Secure Messaging	41
5	Cryptography for Personalization	43
5.1	Key Zones	43

5.2	Session Keys	43
5.3	MACs	44
5.3.1	MACs for Personalization Cryptograms	45
5.3.2	C-MAC for Secure Messaging	45
5.3.3	MAC for integrity of the personalization data file	47
5.4	Encryption	49
5.4.1	Encryption Using ECB mode	49
5.4.2	Encryption Using CBC Mode	49
5.5	Decryption	49
5.5.1	Decryption Using ECB Mode	50
5.5.2	Decryption Using CBC Mode	50
5.6	Triple DES Calculations	50
6	Personalization Data Elements	51
6.1	ACT (Action to be Performed)	51
6.2	AID (Application Identifier)	51
6.3	ALGSCP (Algorithm for Secure Channel Protocol)	51
6.4	C-MAC	51
6.5	CMODE (Chaining Mode)	51
6.6	CSN (Chip Serial Number)	52
6.7	DTHR (Date and Time)	52
6.8	ENC (Encryption Personalization Instructions)	52
6.9	IDTK (Identifier of the Transport Key)	52
6.10	IDOWNER (Identifier of the Application Specification Owner)	52
6.11	IDTERM (Identifier of the Personalization Device)	52
6.12	K _{ENC} (DES Key for Creating Personalization Session Key for Confidentiality and Authentication Cryptogram)	52
6.13	K _{DEK} (DES Key for Creating Personalization Session Key for Key and PIN Encryption)	53
6.14	K _{MAC} (DES Key for Creating Personalization Session Key for MACs)	53
6.15	Key Check Value	53
6.16	KEYDATA (Derivation Data for Initial Update Keys)	53
6.17	KMC (DES Master Key for Personalization Session Keys)	53
6.18	KMC _{ID} (Identifier of the Master Key for Personalization)	54
6.19	L (Length of Data)	54
6.20	LCCA (Length of IC Card Application Data)	54
6.21	LOGDATA (Data Logging Personalization Instructions)	54
6.22	MAC _{INP} (MAC of All Data for an Application)	54
6.23	MACkey (MAC Key)	55
6.24	MIC (Module Identifier Code)	55
6.25	ORDER (Data Grouping Order Personalization Instructions)	55
6.26	POINTER (Additional Pointer to Personalization Data or Instructions)	55
6.27	R _{CARD} (Random Number from the IC Card)	55
6.28	R _{TERM} (Random Number from the Personalization Device)	55
6.29	RANDOM (Random Number)	55
6.30	REQ (Required or Optional Action)	56
6.31	SEQNO (Sequence Number)	56
6.32	SKU _{ENC} (Personalization Session Key for confidentiality and authentication cryptogram)	56
6.33	SKU _{DEK} (Personalization Session Key for Key and PIN Encryption)	56

6.34	SKU _{MAC} (Personalization Session Key for MACing)	56
6.35	TAG (Identifier of Data for a Processing Step)	57
6.36	TK (Transport Key)	57
6.37	TYPE _{TK} (Indicator of Use(s) of Transport Key)	57
6.38	VERCNTL (Version Control Personalization Instructions)	58
6.39	VNL (Version Number of Layout)	58
Annex A.	Common EMV Data Groupings	59
A.1	Introduction	59
A.2	Common DGIs for EMV Payment Applications	59
A.3	Common DGIs for EMV PSE	63
Annex B.	Overview of EMV Card Personalization	65

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.