GlobalPlatform Card Technology

Security Upgrade for Card Content Management

Card Specification v2.3 – Amendment E

Version 1.1

Public Release

October 2016

Document Reference: GPC_SPE_042

THIS SPECIFICATION OR OTHER WORK PRODUCT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY IMPLEMENTATION OF THIS SPECIFICATION OR OTHER WORK PRODUCT SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE COMPANY, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER DIRECTLY OR INDIRECTLY ARISING FROM THE IMPLEMENTATION OF THIS SPECIFICATION OR OTHER WORK PRODUCT.

Contents

1 Introduction 5
1.1 Audience 5
1.2 IPR Disclaimer 5
1.3 Normative References 5
1.4 Terminology and Definitions 5
1.5 Abbreviations and Notations 6
1.6 Revision History 7

2 Use Cases and Requirements 8

3 Specification Amendments 9
3.1 ECC Algorithms 9
3.1.1 Domain Parameters and Key Length 9
3.1.2 ECC Key Type 9
3.1.3 ECDSA 9
3.1.4 ECKA 9
3.1.5 Key Derivation 9
3.2 RSA Algorithms (Variant 2) 9
3.3 Key Usage Qualifier 9

4 Card Content Management Usage 10
4.1 ECC based DAPs, Tokens, and Receipts 10
4.2 RSA based DAPs, Tokens, and Receipts (Variant 2) 10
4.3 Encrypted Load File with Optional ICV 10
4.4 Load File Data Block Hash 10
4.5 Preloaded ECC Curve Parameters 10
4.6 PUT KEY (ECC Key) 10
4.7 STORE DATA (ECC Key) 10
4.8 Confidential Setup of Secure Channel Keys Using ECKA 10
4.8.1 Confidential Setup of Secure Channel Keys Using Scenario #3 (ECKA) 10
4.8.2 CASD Personalization Data for Scenario #3 (ECKA) 10
4.9 Long Parameter and Command and Response Data Fields 11
4.9.1 Command Chaining 11
4.9.2 Response Chaining 11
4.9.3 Token Calculation for Chained Command Data Fields 11
4.9.4 Long Parameter Fields 11
4.10 Key Information Template ('E0') for ECC Keys 11

5 Confidential Setup of Secure Channel Keys Using ECKA-EG 12

6 Indication of Card and CASD Capabilities 13
6.1 Card Capability Information 13
6.2 CASD Capability Information 13

Tables

Table 1-1: Normative References..5
Table 1-2: Abbreviations...6
Table 1-3: Revision History 7

1 Introduction

The security mechanisms described in the GlobalPlatform Card Specification [GPCS] and its amendments are based on several cryptographic primitives (e.g. TDEA, RSA, AES). The purpose of this amendment was to expand those specifications to include new cryptographic schemes based on Elliptic Curve Cryptography (ECC) and upgraded cryptographic schemes for RSA, but the technical contents of this amendment have now been re-integrated into [GPCS] and [Amd A]. This version of Amendment E is provided for convenience and aims at describing where in these documents the prior contents of this amendment can now be found.

1.1 Audience

This amendment is intended primarily for card manufacturers and application developers developing GlobalPlatform card implementations.

It is assumed that the reader is familiar with smart cards and smart card production, and in particular familiar with the GlobalPlatform Card Specification [GPCS].

1.2 IPR Disclaimer

Attention is drawn to the possibility that some of the elements of this GlobalPlatform specification or other work product may be the subject of intellectual property rights (IPR) held by GlobalPlatform members or others. For additional information regarding any such IPR that have been brought to the attention of GlobalPlatform, please visit https://www.globalplatform.org/specificationsipdisclaimers.asp. GlobalPlatform shall not be held responsible for identifying any or all such IPR, and takes no position concerning the possible existence or the evidence, validity, or scope of any such IPR.

1.3 Normative References

Table 1-1: Normative References

Standard / Specification	Description	Ref
GlobalPlatform Card Specification	GlobalPlatform Card Specification v2.3	[GPCS]
GPCS Amendment A	GlobalPlatform Card, Confidential Card Content Management, Card Specification v2.3 – Amendment A, v1.1	[Amd A]
NIST SP 800-57 Part 1 Revision 3	Recommendation for Key Management – Part 1: General (Revision 3), July 2012	[NIST 800-57]
BSI TR-02102	BSI Technische Richtlinie TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 1.0	[TR 02102]

1.4 Terminology and Definitions

Technical terms used in this amendment are defined in [GPCS].

1.5 Abbreviations and Notations

Table 1-2: Abbreviations

Abbreviation	Meaning
AES	Advanced Encryption Standard
AP	Application Provider
BSI	Bundesamt für Sicherheit in der Informationstechnik
CASD	Controlling Authority Security Domain
DAP	Data Authentication Pattern
DGI	Data Grouping Identifier
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECKA	Elliptic Curve Key Agreement Algorithm
ECKA-EG	ElGamal ECKA
ICV	Initial Chaining Vector
NIST	National Institute of Standards and Technology
PKCS	Public Key Cryptography Standards
RSA	Rivest / Shamir / Adleman asymmetric algorithm
SCP	Secure Channel Protocol
SD	Security Domain
SHA-1	Secure Hash Algorithm 1 (digest size 160 bits)
TDEA	Triple DEA (Data Encryption Algorithm)

1.6 Revision History

Table 1-3: Revision History

Date	Version	Description
November 2011	1.0	Initial release.
July 2014	1.0.1	• Added section 3.3 “Key Usage Qualifier” describing a new qualifier value for Key Agreement. • In section 4.5, clarified the purpose of global and local key parameter references for preloaded ECC curve parameters. Only the ISD may store global key parameter references. • In section 4.6, clarified the format used to load ECC keys using the PUT KEY command. • In section 4.8, added many clarifications for “scenario #3” regarding: o the format of DGI '00A6' which triggers key set generation; o how to generate key sets having keys of different types and lengths; o CASD personalization data (including CASD certificate format); • In section 4.9, added clarifications on how to apply security on chained commands and chained responses. • Added section 4.10 “Key Information Template ('E0') for ECC Keys” • In section 6.1, clarified conditions for the presence of sub-tags within Card Capability Information. In section 6.2, removed the ability to retrieve CASD Capability Information as an individual data with the GET DATA command. CASD Capability Information can still be retrieved as part of tag '66' (CASD Management Data).
October 2016	1.1	The various contents of this amendment have been moved to [GPCS] and [Amd A]. This new version is provided for convenience in order to explain where in these two documents the prior contents of this amendment can now be found.

2 Use Cases and Requirements

Asymmetric Cryptography in [GPCS] is based on RSA with SHA-1 for hashing and the padding scheme from PKCS #1 v1.5. Neither SHA-1 nor the padding scheme is recommended any longer by security organizations like NIST or BSI (see [NIST 800-57] or [TR 02102]).

The purpose of this document is to provide alternative asymmetric security options in line with current recommendations.

To enable compact data structures, ECC is specified for public key cryptography.

Enhanced security mechanisms are provided for:

- Tokens and receipts, which are used in Delegated Management;
- DAPs, which are used for the protection of load files;
- Confidential Setup of Secure Channel Keys.

3 Specification Amendments

3.1 ECC Algorithms

A new section B.4 has been created in [GPCS] to describe the ECC algorithms used in GlobalPlatform Card Specifications.

3.1.1 Domain Parameters and Key Length

The content of this section has been moved to [GPCS] section B.4.1.

3.1.2 ECC Key Type

[GPCS] Table 11-16 has been extended to include ECC key components.

3.1.3 ECDSA

The content of this section has been moved to [GPCS] section B.4.3.

3.1.4 ECKA

The content of this section has been moved to [GPCS] section B.4.4.

3.1.5 Key Derivation

The content of this section has been moved to [GPCS] section B.4.5.

3.2 RSA Algorithms (Variant 2)

The content of this section has been moved to [GPCS] section B.3.2.

3.3 Key Usage Qualifier

The definition of Key Usage Qualifier in [GPCS] section 11.1.9 has been extended to include a value for Key Agreement.

4 Card Content Management Usage

This section defines the provisions if ECC schemes or RSA Variant 2 schemes are used for card content management activities.

4.1 ECC based DAPs, Tokens, and Receipts

The content of this section has been moved to [GPCS] sections C.3 and C.4.

4.2 RSA based DAPs, Tokens, and Receipts (Variant 2)

The content of this section has been moved to [GPCS] sections C.3 and C.4.

4.3 Encrypted Load File with Optional ICV

The content of this section has been moved to [GPCS] section 11.6.2.3.

4.4 Load File Data Block Hash

The content of this section has been moved to [GPCS] section C.2.

4.5 Preloaded ECC Curve Parameters

The content of this section has been moved to [GPCS] section B.4.2.

4.6 PUT KEY (ECC Key)

The content of this section has been moved to [GPCS] section 11.8.2.3.

4.7 STORE DATA (ECC Key)

The content of this section has been moved to [GPCS] section 11.11.4.2.2.

4.8 Confidential Setup of Secure Channel Keys Using ECKA

To enable new EC-based scenario #3, a Controlling Authority Security Domain (CASD) shall be installed and personalized. The personalization of the CASD is described in [Amd A] section 3.3.

4.8.1 Confidential Setup of Secure Channel Keys Using Scenario #3 (ECKA)

The content of this section has been moved to [Amd A] sections 3.2.3, 3.5.1, and 3.5.4.

4.8.2 CASD Personalization Data for Scenario #3 (ECKA)

The content of this section has been moved to [Amd A] sections 3.3.

4.9 Long Parameter and Command and Response Data Fields

Because certificates, digital signatures and some data fields can be long, command and response chaining may be required.

4.9.1 Command Chaining

The content of this section has been moved to [GPCS] section 11.1.5.1.

4.9.2 Response Chaining

The content of this section has been moved to [GPCS] section 11.1.5.2.

4.9.3 Token Calculation for Chained Command Data Fields

The content of this section has been moved to [GPCS] section C.4.

4.9.4 Long Parameter Fields

The content of this section has been moved to [GPCS] section 11.1.5.

4.10 Key Information Template ('E0') for ECC Keys

The content of this section has been moved to [GPCS] section 11.3.3.1.1.

5 Confidential Setup of Secure Channel Keys Using ECKA-EG

The content of this section has been moved to [Amd A] sections 3.2.3.

6 Indication of Card and CASD Capabilities

6.1 Card Capability Information

The content of this section has been moved to [GPCS] sections 7.4.1.4 and H.4. Additional information about “Supported cipher suites for SCP81” has been added in [GPCS] section H.4.

6.2 CASD Capability Information

The content of this section has been moved to [Amd A] sections 3.3.1.