GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

GlobalPlatform Technology
Cryptographic Algorithm Recommendations
Version 1.0

Public Release

February 2019

Document Reference: GP_TEN_053

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

Tables

1 Introduction

Cryptography is an important pillar of a digital service's security and impacts the application, the Secure Component, and the related management systems. In order to help the market to anticipate required migration, GlobalPlatform has decided to provide regular recommendations about cryptographic algorithms and key lengths.

The recommendations define the GlobalPlatform technology usage of the cryptographic strengths for the management of a Secure Component and associated content but also share the targeted security strengths for future GlobalPlatform specifications.

1.1 Audience

This technical note is intended to provide guidance to GlobalPlatform specification developers and to the developers of applications based on GlobalPlatform specifications.

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://globalplatform.org/specifications/ip-disclaimers/. 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 References

Table 1-1: Normative References

Standard / Specification	Description	Ref
ISO/IEC 10118-3:2018	Information technology – Security techniques – Hash functions – Part 3: Dedicated hash functions Translation available at GM/T 0004-2012.	[ISO 10118-3]
ISO/IEC 14888-3:2018	Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms Translation available at: • GM/T 0003.1-2012: Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves Part 1: General • GM/T 0003.2-2012: Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves Part 2: Digital Signature Algorithm	[ISO 14888-3]
ISO/IEC 18033-3:2010	Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers Amendment 2 (under development) Translation available at GM/T 0002-2012.	[ISO 18033-3]
IETF RFC 7748	Elliptic Curves for Security	[RFC 7748]

Table 1-2: Informative References

Standard / Specification	Description	Ref
BSI-CC-PP-0084	Common Criteria Protection Profile Security IC Platform Protection Profile with Augmentation Packages	[PP-0084]

1.4 Terminology and Definitions

Table 1-3: Terminology and Definitions

Term	Definition
Rich Execution Environment (REE)	An execution environment comprising at least one device OS or Rich OS and all other components of the device (SoCs, other discrete components, firmware, and software) which execute, host, and support the Rich OS (excluding any TEEs and SEs included in the device).
Secure Component	Either a Secure Element or a Trusted Execution Environment.
Secure Element	A tamper-resistant secure hardware component which is used in a device to provide the security, confidentiality, and multiple application environment required to support various business models. May exist in any form factor, such as embedded or integrated SE, SIM/UICC, smart card, smart microSD, etc.
Tamper-resistant secure hardware	Hardware designed to isolate and protect embedded software and data by implementing appropriate security measures. The hardware and embedded software meet the requirements of the latest Security IC Platform Protection Profile ([PP-0084]) including resistance to physical tampering scenarios described in that Protection Profile.
Trusted Execution Environment	An execution environment that runs alongside but isolated from an REE. A TEE has security capabilities and meets certain security-related requirements: It protects TEE assets from general software attacks, defines rigid safeguards as to data and functions that a program can access, and resists a set of defined threats. There are multiple technologies that can be used to implement a TEE, and the level of security achieved varies accordingly. Contrast *Rich Execution Environment (REE)*.

1.5 Abbreviations and Notations

Table 1-4: Abbreviations and Notations

Abbreviation / Notation	Meaning
AAD	Additional Authenticated Data
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CCM	Cipher Block Chaining – Message Authentication Code

Abbreviation / Notation	Meaning
CMAC	Cipher-based Message Authentication Code
CTR	Counter mode
CTS	Ciphertext Stealing
DES	Data Encryption Standard
ECDH	Elliptic Curve Diffie-Hellman
ECB	Electronic CodeBook
eGCM	extended GCM
GCM	Galois/Counter Mode
MAC	Message Authentication Code
OAEP	Optimal Asymmetric Encryption Padding
PQC	Post Quantum Cryptography
PSS	Probabilistic Signature Scheme
RSA	Rivest / Shamir / Adleman asymmetric algorithm
RSAES	RSA Encryption Scheme
RSASSA	RSA Signature Scheme with Appendix
XEX	Xor-Encrypt-Xor
XTS	XEX-based tweaked-codebook mode with ciphertext stealing

1.6 Revision History

GlobalPlatform technical documents numbered *n*.0 are major releases. Those numbered *n*.1, *n*.2, etc., are minor releases where changes typically introduce supplementary items that do not impact backward compatibility or interoperability of the specifications. Those numbered *n.n*.1, *n.n*.2, etc., are maintenance releases that incorporate errata and precisions; all non-trivial changes are indicated, often with revision marks.

Table 1-5: Revision History

Date	Version	Description
February 2019	1.0	Public Release

2 Cryptographic Algorithm Recommendations

Table 2-2 provides GlobalPlatform's current recommendations on cryptographic algorithms, categorized by the recommendation levels defined in Table 2-1.

Table 2-1: Recommendation Levels

Recommendation Level	Meaning	Security Strength
Deprecated (Dep)	Should not be used. Specific care is needed for products already in the market.	80 bits of security
Legacy use until 2023 (Leg)	Should not be used for any new products/specifications. Products may already be in the market.	112 bits of security
Recommended (Rec)	Should be used for future (near/long-term) products / specifications.	128 bits of security
Recommended PQC (Rec PQC)	Algorithms recommended for post quantum use.	TBD

Current research does not support mature recommendations for PQC; Table 2-2 makes tentative proposals (or no proposal), to be confirmed or adjusted in subsequent versions of this document.

Table 2-2: Cryptographic Algorithm Recommendations

Cryptographic Primitives	Supported Algorithms	Recommendation Level (see Table 2-1)			
		Dep	Leg	Rec	Rec PQC
Block ciphers					
	DES	x			
	3DES (with 2 keys)	x			
	3DES (with 3 keys)		x		
	AES-128			x	?
	AES-192			x	?
	AES-256			x	x
	SM4 (128-bit block, 128-bit key) *See [ISO 18033-3].*			x	?
Modes of operation					
	ECB	x			
	CBC			x	x
	CTR			x	x
	CTS		x		
	XTS			x (AES-based)	x
Authenticated encryption					
	AES-CCM with support for Additional Authenticated Data (AAD)			x	x
	AES-GCM with support for Additional Authenticated Data (AAD)			x	x
	AES-eGCM			x	x

Cryptographic Primitives	Supported Algorithms	Recommendation Level (see Table 2-1)			
		Dep	Leg	Rec	Rec PQC
Hash functions					
	MD5	x			
	SHA-1 (for signature)	x			
	SHA-1 (in other cases)		x		
	SHA-224		x		
	SHA-256			x	?
	SHA-384			x	x
	SHA-512			x	x
	SHA3-256			x	?
	SHA3-384			x	x
	SHA3-512			x	x
	SM3 (digest size 256 bits) *See [ISO 10118-3].*			x	?
MAC functions					
MAC based on block ciphers	Full 3DES MAC		x		
	Retail MAC	x			
	AES MAC		x		
	AES-CMAC			x	x
MAC based on hash	HMAC with one of the supported digests (SHA-1, SHA-256 and over)		SHA-1	others	≥ 256?
	KMAC			x	x

Cryptographic Primitives	Supported Algorithms	Recommendation Level (see Table 2-1)			
		Dep	Leg	Rec	Rec PQC
Asymmetric algorithms					
Key agreement	ECKA-EG with key size in bits ≥ 256			x	NONE
	ECDH with key size in bits >= 256			x	
Signature/Encryption	RSA	512.1024	≥ 2048	≥ 3k	
Signature	DSA, ECDSA with key size in bits ≥ 256			x	
	SM2 (here we focus on the digital signature algorithm based on elliptic curve) *See [ISO 14888-3].*			x	
Padding	PKCS#1 v2.1 (PSS, OAEP)			x	
	PKCS#1 v1.5 (RSAES, RSASSA)		x		
Standardized elliptic curves	NIST curves: P-256 P-384 P-521			x	
	Curve25519 *See [RFC 7748]*			x	
	Brainpool curves: brainpoolP256r1 brainpoolP256t1 brainpoolP384r1 brainpoolP384t1 brainpoolP512r1 brainpoolP512t1			x	

Cryptographic Primitives	Supported Algorithms	Recommendation Level (see Table 2-1)			
		Dep	Leg	Rec	Rec PQC
TLS version / Cipher suite					
TLS 1.0 & TLS 1.1	TLS_PSK_WITH_3DES_EDE_CBC_SHA, RFC 4279		x		
	TLS_PSK_WITH_AES_128_CBC_SHA, RFC 4279			x	?
	TLS_PSK_WITH_NULL_SHA, RFC 4785	x			
TLS 1.2	TLS_PSK_WITH_AES_128_CBC_SHA256			x	?
	TLS_PSK_WITH_NULL_SHA256			x	?