Security Guidelines for UICC Profiles

Version 2.0

30 January 2024

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSM Association (“Association”) makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Compliance Notice

The information contain herein is in full compliance with the GSM Association’s antitrust compliance policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out in GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1 Scope

This document provides security guidelines for the proper configuration of UICC profiles.

The guidance contained in this document also applies to telecom profiles embedded into an eUICC.

The document contains a number of important recommendations and the key points are highlighted with the colour conventions described below:

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended - if supported

1.1 Definitions

Term	Description
Embedded UICC	A removable or non-removable UICC which enables the remote and/or local management of Profiles in a secure way
Randomly generated	The secret shall be generated from a True Random Number Generator (TRNG) or from a Deterministic Random Bit Generator (DRBG), the seed of which is generated by a TRNG
Properly derived	The secret shall be generated from a master key using a secure key derivation algorithm. Some secure key derivation algorithms are standardised, as the ones recommended by NIST in SP 800-108

1.2 Abbreviations

Term	Description
3GPP	Third Generation Partnership Project
5G	5th Generation
ADF	Application Dedicated File
ADM	Administrative Keys
AES	Advanced Encryption Standard
AID	Application Identifier
AKA	Authentication and Key Agreement
ANSSI	Agence nationale de la sécurité des systèmes d'information
ARR	Access Rule Reference
AuC	Authentication Centre
BSI	Bundesamt für Sicherheit in der Informationstechnik
CBC	Cipher Block Chaining
CC	Common Criteria
CHV	Card Holder Verification (also named PIN)
DAP	Data Authentication Pattern
DEK	Data Encryption Key
DES	Data Encryption Standard

Term	Description
DF	Dedicated File
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
DRBG	Deterministic Random Number Generator
DS	Digital Signature
ECB	Electronic Code Book
EF	Elementary File
EMA	Electromagnetic Analysis
ETSI	European Telecommunications Standards Institute
eUICC	Embedded Universal Integrated Circuit Card
HSS	Home Subscriber Server
HTTPS	Hypertext Transfer Protocol Secure
IMSI	International Mobile Subscriber Identity
ISD	Issuer Security Domain
KIc	Key and algorithm Identifier for ciphering
KID	Key and algorithm Identifier for RC/CC/DS
KIK	Key Identifier for protecting KIc and KID
LTE	Long Term Evolution (4G)
ME	Mobile Equipment
MME	Mobility Management Entity
MNO	Mobile Network Operator
MSL	Minimum Security Level
NIST	National Institute of Standards and Technology (USA)
OP/OPc	Operator key
OTA	Over The Air
PIN	Personal Identification Number
PoR	Proof of Receipt
PUK	Personal Unblocking Key
RAM	Random Access Memory
RAM	Remote Application Management
RFM	Remote File Management
RSA	Rivest, Shamir & Adelman
SCP	Secure Channel Protocol
SD	Security Domain
SGSN	Serving GPRS Support Node
SMS	Short Message Service
SPA	Simple Power Analysis
SPI	Security Parameters Indication

Term	Description
SQN	Sequence Number
SSD	Supplementary Security Domain
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TA	Toolkit Application
TAR	Toolkit Application Reference
TLS	Transport Layer Security
TRNG	True Random Number Generator
UE	User Equipment
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module

1.3 References

Ref	Document Number	Title
[1]	GSMA FS.28	Security Guidelines for Exchange of UICC Credentials
[2]	ETSI TS 102 221	UICC-Terminal interface; Physical and logical characteristics
[3]	3GPP TS 31.102	Characteristics of the Universal Subscriber Identity Module (USIM) application
[4]	GP Card specification	GlobalPlatform Card Specification
[5]	ETSI TS 102 226	Remote APDU structure for UICC based applications
[6]	GP Amendt B	GlobalPlatform Amendment B: RAM over HTTP
[7]	ETSI TS 102 225	Secured packet structure for UICC based applications
[8]	ETSI TS 101 220	ETSI numbering system for telecommunication application providers
[9]	GSMA FS.35	Security Algorithm Implementation Roadmap
[10]	3GPP TS 33.102	3G Security - Security architecture
[11]	GP GPC_GUI_050	Composition Model Security Guidelines for Basic Applications
[12]	3GPP TS 35.205	Specification of the MILENAGE Algorithm Set
[13]	3GPP TS 35.231	Specification of the Tuak algorithm set
[14]	IETF RFC 4279	Pre-Shared Key Ciphersuites for TLS
[15]	GSMA SGP.02	SGP.02 Remote Provisioning Architecture for Embedded - UICC Technical Specification
[16]	GP Sec Note 1	Security Informative Note - SCP02 Usage Recommendation (April 2018)
[17]	GP Amendt D	GlobalPlatform Amendment D: Secure Channel Protocol '03'
[18]	GP Amendt F	GlobalPlatform Amendment F: Secure Channel Protocol '11'
[19]	GP Amendt L	GlobalPlatform Amendment L: Secure Channel Protocol '10'
[20]	TCA S@T Sec Guide	Security Guidelines for S@T Push
[21]	3GPP TS 33.501	Security architecture and procedures for 5G system
[22]	3GPP TS 23.003	Numbering, addressing and identification
[23]	IETF RFC 7748	Elliptic Curves for Security

Ref	Document Number	Title
[24]	GP Crypto Recom.	Cryptographic Algorithm Recommendations
[25]	SECG SEC2	Standards for Efficient Cryptography Group - Recommended Elliptic Curve Domain Parameters
[26]	SOG-IS ACM	Senior Officials Group Information Systems Security - Agreed Cryptographic Mechanisms
[27]	NIST FIPS 186-4	Digital Signature Standard (DSS) / ECC P-256 specification
[28]	ANSSI RGS B2	Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques (French only)
[29]	SECG SEC1	Standards for Efficient Cryptography Group - Recommended Elliptic Curve Cryptography
[30]	IETF RFC 5480	Elliptic Curve Cryptography Subject Public Key Information
[31]	IETF RFC 4785	Pre-Shared Key (PSK) Ciphersuites with NULL Encryption for TLS
[32]	IETF RFC 5487	Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode
[33]	IETF RFC 8439	ChaCha20 and Poly1305 for IETF Protocols
[34]	IETF RFC 8846	The Transport Layer Security (TLS) Protocol Version 1.3
[35]	NIST SP 800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
[36]	3GPP TR 33.834	Study on Long Term Key Update Procedures (LTKUP)
[37]	GSMA SGP.22	RSP Technical Specification for consumer devices
[38]	GSMA SGP.26	RSP Test Certificate Description
[39]	SmartTrust WIB 1.3	Implementation Specification SmartTrust Wib™ version 1.3
[40]	GP UICC Configuration (GPC_GUI_010)	UICC Configuration 2.0
[41]	TCA Interoperable Profile Package	TCA Profile Package: Interoperable Format Technical Specification from TCA Technology Library
[42]	NIST FIPS 800-67 Rev.2	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher

2 Authentication and Key Agreement (AKA) Algorithms

This section provides recommendations on the algorithms that are used by the home operator to authenticate the (e)UICC and to produce the keys used to protect the radio network interface. These algorithms are called Challenge Response on GSM and are referred to as A3/A8. In the case of UMTS, LTE and 5GNR they are called Authentication and Key Agreement, commonly referred to as AKA.

2.1 Algorithm Recommendations

The table below contains a summary of the recommendations contained in GSMA's FS.35 – Security Algorithm Implementation Roadmap [9].

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended
COMP128-1	COMP128-2	COMP128-3	GSM Milenage (COMP128-4) Milenage TUAK

Custom or proprietary algorithms are an alternative to Milenage or TUAK because there is no inter-operability requirement or dependency outside the UICC issuing operator's backend and UICCs. Custom or proprietary algorithm security relies on the MNO and/or its suppliers having sufficient cryptographic expertise. As good practice, it is recommended to have custom/proprietary algorithms formally reviewed by cryptography experts. This can be done by commissioning experts, e.g. from renowned academic institutions, to conduct a review and also by publishing the algorithm and making it available for public review and analysis.

2.2 Algorithm Parameter Customisation

The Milenage algorithm specified in 3GPP TS 35.205 [12] and TUAK algorithm specified in 3GPP TS 35.231 [13] can be customised using specific operator key parameters called OP for Milenage and TOP for TUAK. Further customization of the Milenage algorithm is possible by changing the parameters r1….r5 and/or c1…c5 (see 3GPP TS 35.205 [12] for details). Also the TUAK algorithm set can be further customized by changing the number of permutations of the Keccak algorithm or changing the length of input parameters (see 3GPP TS 35.231 [13] for details as well as the recommendations and limitation described in this document).

OP is a 128-bit Operator variant algorithm configuration field.

OPc is a 128-bit value derived from OP and the authentication secret key K (symmetrically available in USIM and network authentication functions HLR/AuC, HSS or UDM/ARPF for 5G) and used within the computation of the functions f1, f1*, f2, f3, f4, f5 and f5*.

TOP is a 256-bit Operator variant algorithm configuration field. TOPc is a 256-bit value derived from TOP and the authentication secret key K (symmetrically available in USIM and network authentication functions HLR/AuC, HSS or UDM/ARPF for 5G) and used within the computation of the functions f1, f1*, f2, f3, f4, f5 and f5*.

Operators are recommended;

- To randomly generate OP using a True Random Number Generator, configure it in the HSS, provide its value or the value of the derived credentials in a secure way to the UICC manufacturer and store it in a secure way.
- To use different OPs (e.g. for consumer vs M2M markets, for production vs test purposes, etc.)
- To store OPc in the card and not OP.

The same recommendations apply for the TUAK parameters TOP and TOPc.

TUAK facilitates configuration of the length of the elements listed below and the configurations shall be configured properly in USIM and network functions (HLR/AuC, HSS or UDM/ARPF):

- K (128 or 256 bits) internally used in computation functions
- MAC-A (64, 128 or 256 bits) function f1 output
- MAC-S (64, 128 or 256 bits) function f1* output
- RES (32, 64, 128 or 256 bits) function f2 output
- CK (128 or 256 bits) function f3 output
- IK (128 or 256 bits) function f4 output

Where compatibility is required with existing 3GPP specifications, the operator shall set the length of the RES to between 32 and 128 bits, the length of the MAC-A/MAC-S to 64 bits, the length of CK to 128 bits, and the length of IK to 128 bits. Security is increased when selecting longer key lengths. TUAK supports both 128 and 256 bits key K. Operators are encouraged to switch to 256 bits for their subscriber authentication key when deploying TUAK.

TUAK facilitates configuring the number of iterations on call of π Keccak permutation function (see clause 7.2 from 3GPP TS 35.231 [13]). The default number of iterations is one but can be increased for higher security and this configuration shall be configured properly in USIM and network functions (HLR/AuC, HSS or UDM/ARPF).

2.3 Sequence Number Management

The AKA scheme is based on a sequence number to allow the (e)UICC to authenticate the network. AKA uses either a time based or non-time based scheme for sequence-number management. Both schemes have their advantages. The choice of which to deploy is not a UICC profile consideration and it should be agreed between the operator and the HLR/HSS UDM/ARPF vendor as it is transparent to the UICC.

The sequence number parameters Δ and L shall be provided to the UICC manufacturer to configure the cards. Those parameters provide bounds to the 48 bits sequence number, called SQN, which is received by the UICC during the AKA process.

According to 3GPP TS 33.102 [10]**Error! Reference source not found.**, Annex C, SQN = S EQ || IND, where IND is an index used in the array scheme described in 3GPP TS 33.102 [10], Annex C.1.2 and C.2.2. In the profiles in 3GPP TS 33.102 [10], Annex C.3, (which are informative like the rest of Annex C), IND has a length of 5 bits.

GSMA recommends implementing the array scheme in the USIM and also recommends that the IND be set to a length of 5 bits.

SQNMS = SEQMS || INDMS denotes the highest sequence number in the array stored in the USIM.

The parameter Δ provides a maximum increment for a new sequence number. This parameter protects the UICC against excessively large increments by the HSS. We recommend a maximum value of 2^{25} for Δ. This value provides a maximum of 262,144 authentications in a worst case scenario (2^{43} divided by 2^{25}).

Note: The chosen number of authentications should be large enough for the entire lifetime of the UICC to protect from a denial of service (DoS) attack that could try to reduce the lifetime of a UICC by launching authentication requests to the UICC in large numbers.

For all sequence-number generation schemes, the UICC shall also be able to put a limit L on the difference between SEQMS and a received sequence number component SEQ. The use of such a limit L is optional. The choice of value for the parameter L only affects the UICC. It has no impact on the choice of other parameters and it is entirely up to the operator, depending on its security policy. Therefore, no particular value is suggested in the profiles of 3GPP TS 33.102 [10], Annex C.3. Example values for L are suggested here though because choosing a low value for L may lead to frequent re-synchronisations.

To illustrate the purpose of L, we consider a case where a UE starts in 3G and an SGSN downloads a batch of 5 authentication vectors. After one authentication performed with the SGSN, the UE moves to LTE where it performs many authentications with the MME, potentially over a long time. Then the UE returns to 3G. The parameter L ensures that the 4 authentication vectors left in 3G can only be used when they have not been sitting in the SGSN for too long (where ‘too long’ may be expressed in number of authentications performed by the USIM in the meantime, or in time elapsed since the generation of the most recently generated authentication vector accepted by the USIM).

GSMA recommends to limit this value to less than 65,536 (2^{16}) for L and it recommends to choose L to ensure the authentication vectors are valid for less than two weeks. For example, if the HSS increments SEQ every 0.1 second, a value of 2^{23} for L ensures that an authentication vector is valid for almost 10 days.

It is recognised that an operator may have reasons to set L to a larger value for time-based schemes, e.g. if an IoT-device is authenticated very rarely in order to save battery time and the SGSN downloads more than one authentication vector at a time, or to not use L at all. Consequently, the choice of L needs to be carefully considered, especially for time-based schemes.

The authentication succeeds only if SEQ verifies: $SEQ_{MS} + \Delta \geq SEQ > SEQ_{MS} - L$

If L is not used the second part of the equation does not apply. If one of the equations does not verify the UICC a re-synchronisation procedure shall be initiated.

2.4 Authentication key (K)

For authentication secret key K, random generation or proper derivation shall be used. Using random generation mandates to exchange the value between vendor and operator, the value shall be protected during the exchange following recommendations from GSMA FS.28 Security Guidelines for Exchange of UICC Credentials [1]**Error! Reference source not found.**.

3 Theft Protection

The UICC functions are protected by personal user holder codes. The Card Holder Verification (CHV) is protected by an attempt counter that decreases for each false CHV verification. When the counter reaches zero the CHV is blocked and UICC functions are locked.

When blocked, the CHV can be unblocked using another code, the Personal Unblocking Key (PUK), is also protected with an attempt counter.

The CHV parameter, commonly known as Personal Identification Number (PIN), can be usually changed by the mobile user whereas the PUK is non-modifiable. The following settings are recommended for CHV and PUK configuration.

3.1 CHV

It is recommended:

- To set by default the attempt counter for CHV (enabled) to 3 (0x03 HEX),
- To ensure that access rights on file systems are mapped on appropriate PIN codes

3.2 PUK

It is recommended:

- To set by default the PUK attempt counter to 10 (0x0A HEX),
- To use random generation[1] or proper derivation for values.
- To diversify the PUK value card by card.

3.3 Administrative Keys (ADMs)

The administrative keys control access to, and modification of, the configuration parameters of the UICC.
It is recommended:

- To ensure that access rights on file systems are mapped on appropriate ADM codes.
- To use random generation[2] or proper derivation for ADM values.
- To have ADMs of at least 64 bits long.

4 Cryptographic Keys

The UICC uses cryptographic keys for network authentication and for remote management and administration purposes. Keys shall have different values and should be diversified per type of usage (e.g. RAM/RFM/DAP/Token verification) and per UICC.

[1] Using random generation requires the values to be exchanged between the vendor and the operator. The values shall be protected during the exchange following recommendations from GSMA FS.28 [1].

[2] Using random generation requires the values to be exchanged between the vendor and the operator. The values shall be protected during the exchange following recommendations from GSMA FS.28 [1].

4.1 Keys for Remote Access (KIc, KID) – SCP80

The remote access keys are used to encrypt and verify the integrity of the commands exchanged over the air between the UICC and the network using, respectively, the Key and algorithm Identifier for ciphering (KIc) and the Key and algorithm Identifier for RC/CC/DS (KID).

- Keys for remote access shall be properly derived or randomly generated if derivation is not used. Fixed values are forbidden.
  - Using derivation will prevent the need to further exchange the final values between the vendor and the operator as both sides can perform the same derivation process.
  - Using random values requires the exchange of values between the vendor and the operator. The values shall be protected during the exchange following recommendations from GSMA FS.28 [1].**Error! Reference source not found.**
- Values of KIc and KID shall be different.
- Keys should be diversified per KeySet. For example, KIC of KeySet1 and KIC of KeySet2 should be different.

4.2 Data Encryption Key (KIK/DEK) – SCP80

The Data Encryption Key (KIK/DEK) is used to protect the KIC and KID keys when creating or updating over the air any Key Version as defined in ETSI TS 102.226 [5].

- Algorithm and length of KIK/DEK (used for Put Key) should be equivalent to, or stronger than, the strongest algorithm and length of KIC and KID transported by PUT KEY command.
- KIK/DEK shall be properly derived or randomly generated if derivation is not used. Fixed values are forbidden.
- Using random values requires the values to be exchanged between the vendor and the operator. The values shall be protected during the exchange following recommendations from GSMA FS.28 [1]**Error! Reference source not found.**.
- KIK/DEK values shall be different to the KIc and KID values.

4.3 HTTPs / TLS – SCP81

4.3.1 PSK Identity Format

PSK Identity is defined for each SCP81 administration agent, as specified in GP – Amendment B [6] and is used to identify the (e)UICC administration agent during the TLS handshake procedure.

PSK Identity format specified in GSMA SGP.02 [15] could be used.

4.3.2 PSK TLS

It is recommended to use PSK Identity to associate the corresponding PSK TLS key to use.

Identification of the PSK-ID format defined with ‘02’ value for ‘random PSK’ can be used.

Using random values requires the values to be exchanged between the UICC provider/SCP81 OTA server provider and the operator. The values shall be protected during the exchange following recommendations from GSMA FS.28 [1].**Error! Reference source not found.**

Other PSK-ID formats, based on an PSK TLS derivation scheme, can be agreed between the UICC provider and the SCP81 OTA server provider prior to a review and agreement from the operator.

4.3.3 PSK DEK

It is recommended to use AES keys for PSK DEK keys. The AES key length shall be at 128 bits minimum. Triple DES is deprecated from GP – Amendment B [6] since version 1.2.

4.4 Other Keys

For other keys, fixed values should be avoided unless these are part of the key type definition. Examples where profiles may contain fixed keys are:

- Mandated DAP (keyset version 0x73, Key index 01) with asymmetric key (RSA)
- ETSI DAP key (keyset version 0x11, Key index 02)
- RSA Key's Public exponent (RSA Public exponent is almost always 010001)

4.5 Other Secure Channel

Other Secure Channel Protocol (SCP) can be defined on any Security Domain in the (e)UICC. The following clauses provide security recommendations on symmetric and asymmetric protocols.

4.5.1 Secure Channel Protocol with Symmetric Keys

SCP02 is not recommended by GP (see SCP02 Usage Recommendation [16] for details) and is deprecated from GP Card Specification [4] since version 2.3.1.

SCP03, specified in GP Amendment D [17], is recommended with any AES key length (AES-128, AES-192 or AES-256). Security is increased when selecting a longer key length.

4.5.2 Secure Channel Protocol with Key Establishment Using Asymmetric Keys

SCP10 provides mutual authentication based on PKI and secure messaging based on AES keys, see GP Amendment L [19] for details.

SCP10 is deprecated by GP - Card Specification [4] since version 2.3.2 and is not recommended.

SCP11 provides mutual authentication based on ECC and secure messaging based on AES keys, see GP Amendment F [18],**Error! Reference source not found.** for details:

- SCP11a and SCP11c provide mutual authentication between Off-Card Entity (OCE) and card
- SCP11c is adapted for scripting mode
- SCP11b provides only authentication of the card to the OCE

5 File System Control

5.1 EF_ARR (Access Rule Reference) File

The Elementary File Access Rule Reference (EF_ARR) contains access rules for the different files stored in the UICC.

- The UPDATE Access Condition of each EF ARR within the electrical profile shall be set to ADM code as defined in ETSI TS 102.221 [2]**Error! Reference source not found.**.
- The electrical profile will be capable of being updated in the field if needed (e.g. access condition of files not in line with access domain of the application).
- If any access condition is set to NEVER, the recommendation is to set the UPDATE Access Condition of the EF ARR to NEVER so there is no way to supersede the original value set to NEVER.

Note: When the EF $_{ARR}$ UPDATE Access Condition is set to NEVER, the EF ARR will not be modifiable OTA when the UICC is in the field, meaning access conditions of all EFs related to this EF ARR are not modifiable.

5.2 Access Domain

The access domain is used to specify the UICC files that may be accessed by an application and the operations allowed on these files and is standardised in ETSI TS 102.226 [5]**Error! Reference source not found.**.

- The “least privilege” principle should be applied i.e. privileges shall be limited to operations needed on the file system.

5.3 Access Conditions

The access conditions specify the level of access required (by any application or on the mobile interface) to access a given file on the UICC. The following rules shall apply for access conditions:

- For standard files, access conditions shall follow the recommendations contained in the ETSI/3GPP standards.
- For applicative/proprietary files, access conditions shall be limited to the necessary rights that need to be granted.

6 Over The Air (OTA) Management

This section describes the different recommendations related to the remote management of the UICC by the network operator.

6.1 Cryptographic Algorithm Recommendations

This section provides recommendations on the algorithms used to generate keys to protect the commands exchanged between the UICC and the network.

6.1.1 Algorithms for SMS/CAT-TP (SCP80)

The table below details the algorithms that can be used for confidentiality and integrity protection of the SCP80 channel.

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended
Single DES (8 Bytes) 3DES (16 bytes) with twice the same 8 bytes value 3DES (24 bytes) with thrice the same 8 bytes value	3DES (16 bytes) 3DES (24 bytes)		AES (16 bytes) AES (24 bytes) AES (32 bytes)

AES security is increased when selecting a longer key length.

3DES (see NIST SP 800-67 Rev. 2 [42]) is being deprecated by NIST and has been withdrawn from 1st January 2024.

6.1.2 Algorithms for HTTPS (SCP81)

The table below details the algorithms that can be used for confidentiality and integrity protection of the SCP81 channel.

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended
HTTPS TLS 1.0[(1)] **or HTTPS TLS 1.1**[(1)] TLS_PSK_WITH_NULL_SHA, as defined in IETF RFC 4785 [31].**Error! Reference source not found.** TLS_PSK_WITH_3DES_EDE_CBC_SHA, as defined in IETF RFC 4279 [14] TLS_PSK_WITH_AES_128_CBC_SHA, as defined in IETF RFC 4279 [14]		**HTTPS TLS 1.2** TLS_PSK_WITH_NULL_SHA256, as defined in IETF RFC 5487 [32][(2)]	**HTTPS TLS 1.2** TLS_PSK_WITH_AES_128_CBC_SHA256, as defined in IETF RFC 5487 [32].**Error! Reference source not found.** **HTTPS TLS 1.3** TLS_AES_128_GCM_SHA256 as defined in NIST SP 800-38D **Error! Reference source not found.**[35] TLS_AES_256_GCM_SHA384 as defined in NIST SP 800-38D [35] TLS_CHACHA20_POLY1305_SHA256 as defined in IETF RFC 8439 [33]

			TLS_AES_128_CCM_SHA256 as defined in IETF RFC 8846 [34] TLS_AES_128_CCM_8_SHA256 as defined in IETF RFC 8846 [34]

(1) TLS 1.0 and 1.1 are deprecated from GP – Amendment B [6] since version 1.2

(2) TLS_PSK_WITH_NULL_SHA256 is without confidentiality. Data is transported from server to card in the clear.

6.2 Issuer Security Domain (ISD) and Supplementary Security Domain (SSD)

If the security domain supports both SCP81 and SCP80, to achieve a consistent level of security, keys and algorithms should have an equivalent level of security for both channels.

6.2.1 Security Domain for RAM / RFM and Applications

The table below describes the different Security Domain recommendations for RAM/RFM and Applications

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended
	Unique SD for RFM, RAM and OTA-able applets(s) with one or several keysets	One ISD (or SD) for RFM/RAM One SD for OTA-able applets(s) of the same service provider	One SD for RFM One SD for RAM One SD for OTA-able applets(s) of the same service provider

6.2.2 Additional Security Domain Rules for Applications

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended
	A unique SD for all applications (different families) and administered by different entities with the same or different keyset		Each application family in a dedicated SD and administrated by one entity

Note: An application family is a set of applets that have the same level of sensitivity

6.3 Minimum Security Level (MSL) over SMS/CAT-TP (SCP80)

The Minimum Security Level (MSL) is the OTA security configuration for each application defined during applet installation as specified in ETSI TS 102 226 [5]**Error! Reference source not found.**. This security level will be checked by the UICC before the OTA commands are forwarded to the targeted application in the UICC. If the security level is below the MSL (based on the comparison done on SPI first byte bits in the incoming message as defined in ETSI TS 102 226 [5]) the application will never receive the commands.

MSL coding follows SPI first byte coding specified in ETSI TS 102 225 [7].

6.3.1 MSL for Remote Applet Management (RAM) and Remote File Management (RFM) and System Applications

Remote Applet Management and Remote File Management are defined in ETSI TS 102 226 [5] and have to be considered carefully because they allow modification of the UICC content (Files, Applets and Keys) remotely.

Any configuration without counter check (b5=0 of MSL) does not prevent replay attacks.

The table below describes each MSL value setting and its recommendation.

Digital Signature settings are recommended but the settings are not included in the table to improve readability and because this channel integrity protection is not used in practice.

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended
0x00 No security **0x01** Redundancy Check **0x04** Ciphering **0x08** Counter available **0x09** Redundancy Check & Counter available **0x10** Counter with check if counter value is higher than RE **0x11** Redundancy Check & Counter value is higher than RE **0x14** Ciphering & anti replay counter with check if counter value is higher than RE **0x0C** Ciphering & counter available	**0x05**(2)(3) Ciphering & Redundancy Check **0x0D**(2) Redundancy Check & Counter available & Ciphering **0x15**(2) (Integrity & Confidentiality) Redundancy Check (RC) & Anti-replay counter with check if counter value is higher than RE & Ciphering	**0x02**(3) Cryptographic Checksum **0x06**(3) Ciphering & Cryptographic Checksum **0x0A**(3) Cryptographic checksum & Counter available **0x0E**(3) Cryptographic Checksum & Counter available & Ciphering	**0x12** (Authenticity & Anti-Replay but without Confidentiality Cryptographic Checksum (CC) & Anti replay counter with check if counter value is higher than RE **0x16** (Authenticity & Anti-replay & Confidentiality) Cryptographic Checksum (CC) & Anti replay counter with check if counter value is higher than RE & Ciphering
0x18(1) Counter value is one higher than RE **0x19**(1) Redundancy Check & Counter value is one higher than RE **0x1C**(1) Ciphering & Counter value is one higher than RE	**0x1D**(1)(2) Redundancy Check (RC) & Anti replay counter with check if counter value is one higher than RE & Ciphering		**0x1A**(1) Cryptographic Checksum (CC) & Anti replay counter with check if counter value is one higher than RE **0x1E**(1) Cryptographic checksum & Anti replay counter with check if counter value is one higher than RE & Ciphering

Note: (1) This is not related to security but to serviceability: NEVER use the "Counter value is one higher than RE" except if strongly requested.

(2) Use of this MSL is restricted: Such MSL is not a valid option for RAM, ETSI TS 102.226 [5] and UICC Configuration [40] mandate CC for RAM operations.

(3) This MSL is forbidden if an AES key is used. Since ETSI TS 102.225 [7] release 8.0.1, it is mandatory to have the counter checked in this configuration (b5=1 of MSL).

6.3.2 Minimum Security Level (MSL) for Basic Applications

6.3.2.1 S@T application

Following TCA Security guidelines for S@T Push [20], it is recommended to set on the S@T browser, in push mode application, the following MSL:

- 0x06: Ciphering & Cryptographic Checksum (CC)
- 0x16: Cryptographic Checksum (CC) & anti replay counter with a check if the counter value is higher than RE & Ciphering

6.3.2.2 WIB application

L0 security level shall not be used as recommended in Implementation Specification SmartTrust Wib™ version 1.3 [39]. L0 security level can be used only for test purposes.

6.3.2.3 Other Applications

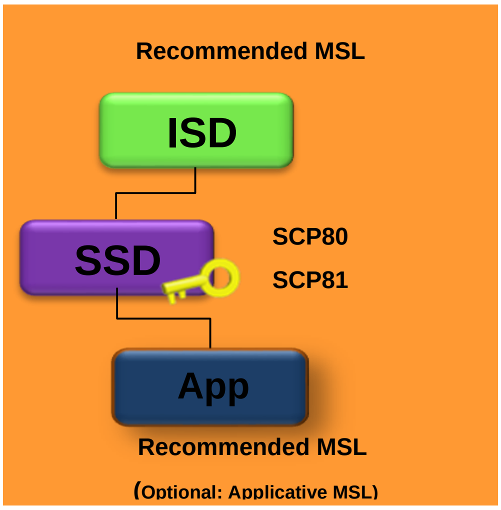
The minimum security level attached to a toolkit application (other than RAM/RFM applications) shall be configured according to the security aspects of application functions and to its associated access domain.

- If toolkit applications require the sending of proof of receipt (PoR), it is strongly recommended that minimum security levels enforce at least a cryptographic checksum (CC).
- The minimum security levels of the application and the security applied by the server should be consistent to ensure good security behaviour.

6.3.3 Application Architectures Depending on MSL Setting

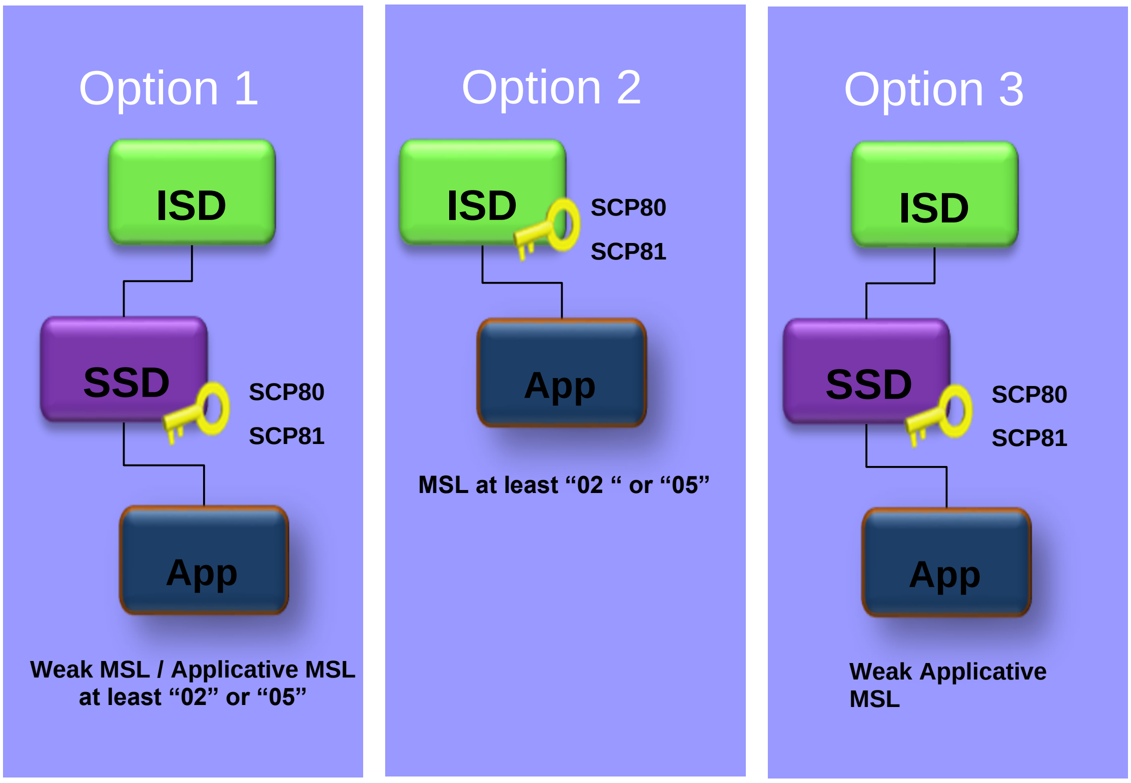
6.3.3.1 Basic Application with Recommended MSL

For basic applications, the recommended structure is as defined in section 6.2.1 and is illustrated below.



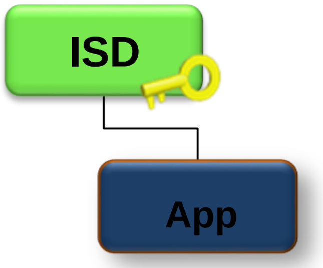
6.3.3.2 Basic Application Alternative Options

The following options are acceptable due to possible solution constraints.



6.3.4 Non Recommended Option

The option detailed below in maintaining an application under the issuer security domain with a weak minimum security level, as illustrated in section 6.3.1, is not recommended.



Weak MSL

6.4 Toolkit Application Reference (TAR)

Do not use the default toolkit application reference (TAR) value, as defined in the standard (e.g.: ETSI TS 101.220 Annex D [8]) but use a proprietary TAR instead.

7 Application Design

7.1 Applicative Keys

Applicative keys (whether they are used for OTA access or not) shall be stored either in a dedicated security domain, in the application itself or in an Elementary File (EF).

If applicative keys are stored in an EF:

- the EF READ Access Condition access shall be limited to legitimate application(s) (i.e. Access Condition consistent with Access Domain restricted to legitimate application(s) only)
- no access right shall be allowed on the device interface (i.e. I/O channel)
- the EF content should be ciphered with a key stored in the application

Where keys are sent over a secure channel, the key used for channel encryption shall be at least as strong as the key being transmitted.

3DES (see NIST SP 800-67 Rev. 2 [42]) is being deprecated by NIST and has been withdrawn from 1st January 2024. AES is the recommended algorithm to be used for encryption.

7.2 Applicative File System

If applicative files are needed on the UICC a dedicated file (DF) storing the applicative files and their associated Elementary Files, Access Rule Reference (EF_ARR) are recommended.

Applicative files shall not be defined directly under MF.

Access conditions on each applicative file shall be consistent with the access domain of the applet(s) accessing those files.

7.3 GlobalPlatform Privileges

The applications running on the UICC (or in the profile on an eUICC) can be assigned a number of privileges (e.g. lock the UICC, delete application, DAP verification, etc..) that are standardised by GlobalPlatform [4] and referred to as GlobalPlatform privileges.

The “least privilege” principle should be applied i.e. privileges must be limited to operations needed.

8 Side Channel Attack Recommendations

UICCs shall be protected against side channel attacks that acquire, process and analyse signals. The side channel attack techniques can vary and definitions can be found in a variety of sources, including publications by the JIL Hardware Attack Subgroup (JHAS). Some examples, provided here for illustration purposes only and not intended to be an exhaustive list, can include the following;

- Simple power analysis (SPA) and differential power analysis (DPA) – which seek to exploit the information leaked through characteristic variations in the power consumption of electronic components. The power consumption can be measured and there is a range of methods from direct interpretation of the retrieved signal to a complex analysis of the signal with statistical methods to do so. SPA attacks can be applied to the implementation of any cryptographic algorithm to try to extract the secret subscriber key (Ki) from the UICC.
- Differential Fault Analysis (DFA) – which seeks to obtain the secret Ki by comparing a calculation without an error and calculations that do have an error. DFA can break cryptographic key systems, allowing the retrieval of secret keys, by running the devices under unusual physical circumstances and by injecting an error at the right time and location.
- Electromagnetic Analysis (EMA) – measures the electromagnetic emissions from a UICC during its operation and inferences to the data processed. It uses similar analysis techniques to those used in power analysis and attacks typically aim to recover the secret subscriber key but may also be applied to recover other secret data such as the IMSI, PIN, etc. EMA could be used for identification of activity that may assist in synchronisation of other attacks. For example, it may be possible to detect actions within a cryptographic algorithm or PIN check that enable the precise synchronisation of a perturbation.
- Timing Analysis (TA) - requires a means to measure the duration of a command and this can be done by monitoring to detect the first falling edge and the last rising edge and the result corresponding to the command duration.

9 Certified UICCs

9.1 OTA / Key Set and RFM Application Positions

Over the air key sets and remote file management application positions are very important and the following guidance is recommended.

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended
	Secured keys and non-secured keys in a single SD		One SD for Secured keys One SD for non-secured Keys

A secured key is a key that has been properly derived and the value is protected during personalisation using “secure put key” commands (e.g. banking keys)

A non-secured key is a key that has been properly derived but the value is not protected during personalisation (e.g. OTA key)

- Never put payment/sensitive applets in the ISD or SD if it is already used by another entity such as an MNO OTA platform.
- Sensitive applications with secure keys shall be set up in their own SD.

9.2 Applet Verification

To increase card content management protection, the use of a Mandated domain application provider (DAP) is recommended. In applet verification schemes, all applets shall be provided with a DAP after security verification.

9.3 Java applets

Java applets shall, at a minimum, follow the “GlobalPlatform Card Composition Model Security Guidelines for Basic Applications” [11]. In particular, Java applets shall successfully pass byte code verification using tools from Oracle or from the platform issuer of the target platform. The tools used for byte code verifications shall be the latest versions available.

Export files used for verification shall be in the format version 2.3 or newer and shall correspond to the package version present on the target platform.

AIDs (Load File AID, Executable Module AID, Application AID) shall be checked: correct RID, PIX,..

10 5G Profiles

10.1 SUPI Concealment – Privacy - SUCI Structure

The SUPI (Subscription Permanent Identifier) is the generalised subscription identifier specified by 3GPP since 5G (e.g. IMSI is specified as SUPI Type 0).

The SUCI (Subscription Concealed Identifier) was specified to optionally apply privacy on SUPI.

The SUCI structure, as described in 3GPP TS 23.003 [22], is as below:

10.2 SUPI Concealment – Protection Scheme Id

The SUPI Concealment scheme to apply in SUCI Scheme Output field is based on Protection Scheme Id, specified in 3GPP TS 33.501 [21] Annex C from the following values:

• Null-Scheme:	0x00
• Profile <A>:	0x01
• Profile <B>:	0x02
• Reserved Scheme:	0x03 to 0x0B
• Operator-Specific:	0x0C to 0x0F

NULL-scheme protection scheme is not recommended (EF_{UST} from USIM service n°124 ‘Subscription identifier privacy support’ is not available, see TS 31.102 [3]**Error! Reference source not found.** for details).

NULL-scheme is without privacy, meaning SUPI (generally IMSI) is in clear from Scheme Output.

Standardized Profile <A> and Profile <B> protection schemes are with privacy, meaning SUPI (generally IMSI) is concealed based on ECIES, Elliptic Curve Integrated Encryption Scheme (refer to 3GPP TS 33.501 - Annex C.3.4 [21] for details) in Scheme Output.

- Profile <A> is based on elliptic curve `Curve25519` (see IETF RFC 7748 [23]) which is recommended by GP
- Profile <B> is based on elliptic curve `secp256r1` (also called `ANSI X9.62 prime256v1` or `NIST P-256`) which is recommended by GP [24], SECG [25], SOG-IS [26], NIST [27] and ANSSI [28].

Operator-Specific (values from 0xC to 0xF) protection scheme requires specific implementation in user equipment (ME or USIM) and the network (UDM). Concealment relies on operator expertise. Refer to GSMA FS.35 [9] for GSMA recommendations on appropriate algorithm selection.

10.3 SUCI Calculation

For SUCI calculation by the ME, services in EF_{UST} from the USIM are configured as follows (see TS 31.102 [3] for details):

- service n°124 ‘Subscription identifier privacy support’ is available
- service n°125 ‘SUCI calculation by the USIM’ is not available

$\text{EF}_{\text{SUCI\_Cal\_Info}}$ under DF_{5GS} in ADF_{USIM} contains information needed by the ME to support the subscription identifier privacy as defined in 3GPP TS 33.501 [21].

For SUCI calculation by USIM, services in EF_{UST} from USIM are configured as below (see TS 31.102 [3] for details):

- service n°124 ‘Subscription identifier privacy support’ is available
- service n°125 ‘SUCI calculation by the USIM’ is available

Following TCA interoperable profile package [41] the $EF_{SUCI\_Cal\_Info\_USIM}$ under DF_{SAIP} in ADF_{USIM} contains information needed by the USIM to support the subscription identifier privacy as defined in 3GPP TS 33.501 [21].

Operators can make their own assessment on whether the SUCI calculation is done by USIM or ME.

10.4 Home Network Public Key

10.4.1 Key Format for the Exchange between Operator and UICC provider

Home Network Public Keys are elliptic curve parameters provided by the operator that are used to apply subscription identifier privacy (SUPI concealment) from user equipment (ME or USIM) as described in 3GPP TS 33.501 [21]. Each Home Network Public Key is associated to an Home Network Public Key Identifier, which is shared on the network during the subscription identifier privacy procedure.

Standardised Home Network Public Keys are elliptic curve parameters provided by the operator.

The Home Network Public Key can be provided to the UICC provider as a:

- public key only as a byte array or in PEM format
- X.509 certificate generally issued from a PKI (Public Key Infrastructure) from operator

Coding of Home Network Public Key values for Profile <A> (Curve25519 curve) is specified in IETF RFC 5480 [30].**Error! Reference source not found.** and for Profile <B> (secp256r1 curve) is specified in IETF RFC 7748 [23]. Both formats are different:

- For Profile <A> this is a 32 bytes (256 bits) value
- For Profile <B> this can have two different formats (see SECG SEC1 [29] §2.3.3 for details):
  - 65 bytes, starting with 0x04, this is uncompressed format
    Next bytes are X, Y coordinates on the curve both concatenated and each on 256 bits (32 bytes)
  - 33 bytes, starting with 0x02 or 0x03, this is compressed format
    Y is deducted from first byte, next bytes is X coordinate on the curve on 256 bits (32 bytes)

Note: Key format during the exchange and the key format for the storage can be different, the storage format is specified in 3GPP TS 31.102 [3].

10.4.2 Key Exchange between Operator and UICC Provider

If the Home Network Public Key is provided as a X.509 certificate, it should be provided with the full certification path (e.g. as .p7b file format) to verify the integrity of certificate in recipient side (the UICC provider).

If the Home Network Public Key is provided as the public key value only, the integrity of the key (hash of the public value) shall be verified through another channel. Refer to GSMA FS.28 [1] for guidance.

If SUCI calculation is performed by the ME, it is not necessary to exchange Home Network Public Keys in confidentially (configuration stored in $EF_{SUCI\_Calc\_Info}$ protected in read mode only with PIN).

If SUCI calculation is performed by the USIM, it is recommended to exchange Home Network Public Keys in confidentiality (i.e. encrypted).

11 eUICC

All recommendations introduced in the following sub-sections are dedicated to the eUICC, specified by GSMA (GSMA SGP.02 [15] / GSMA SGP.22 [37]).

11.1 Certificate Issuer (CI) Management

11.1.1 TEST CIs

TEST CIs should be used only for test use cases and never deployed in final products.

11.1.1.1 GSMA TEST CI

The ‘GSMA TEST CI’ is defined in GSMA SGP.26 [38] clause 3 ‘Test Certificates and keys – Valid test cases’, published on GSMA public web site.

Note: GMSA TEST CI is for consumer products only but is available in two implementations: one on NIST P-256 curve the other on BrainpoolP256r1 curve.

Any eUICC containing LIVE data (e.g. ISD-R LIVE data or any operational profile) shall not be configured with GSMA TEST CI (GSMA SGP.26 [38] clause 3).

11.1.1.2 Other TEST CIs

Other TEST CI is any CI defined on demand for test purpose:

- following generation step described from GSMA SGP.26 [38] clause 2
  or
- from any private parameters disclosed for test purpose

Any eUICC containing LIVE data (e.g. ISD-R LIVE data or any operational profile) shall not be configured with other TEST CI.

11.1.2 LIVE CIs

TEST CIs shall not be mixed with LIVE CIs.

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended
	Multi-CIs, with at least one CI with TEST CI or one CI with the GSMA TEST CI and	Multi-CIs, all LIVE CIs and a CI with one GSMA LIVE CI	Mono-CI with only one GSMA LIVE CI

	with one CI with GSMA LIVE CI		

11.2 ISD-R SCP81

11.2.1 Cipher Suites

PSK-TLS Cipher Suites shall follow the GSMA SGP.02 specification §2.4, see [15] for details and at least one of below values:

- TLS_PSK_WITH_AES_128_GCM_SHA256
- TLS_PSK_WITH_AES_128_CBC_SHA256

11.2.2 PSK-ID format

PSK-ID format shall follow the GSMA SGP.02 specification §2.4.4.1.2, see [15] for details.

11.2.3 PSK-TLS key

PSK-TLS key shall follow the GSMA SGP.02 specification §2.4.3 with 128 bits key lengths at least, see [15] for details.

PSK-TLS key shall follow the SGP.02 specification §2.4.4.1.2 with random generation, see [15] for details.

PSK-TLS key shall follow the SGP.02 specification §5.1.1.2.5, Table 103 and be available encrypted in EIS file, see [15] for details.

‘This data SHALL be encrypted with a transport key agreed between the provider and the requester’.

The encryption mode shall follow the SGP.02 specification §2.8, see [15] for details, and encryption key length shall be equal or greater to the PSK-TLS key length.

11.3 Activation Code / eVoucher

Activation Code is defined in GSMA SGP.22 [37]**Error! Reference source not found.**.

Voucher is QR Code version of Activation Code.

eVoucher is the digital version of voucher, generally in PDF format.

If present in any file exchanged between operator and profile provider, Activation Code shall be encrypted in file and file shall be protected following recommendations from GSMA FS.28 [1].

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	12/06/20	Final version of new PRD (FS.27) agreed by FSAG approved	TG	James Moran, GSMA
2.0	30/01/24	• A references section has been added • TLS 1.3 has been included in the SCP81 recommendations • Clarification has been added on RFM/RAM applications • Recommendations on MSL have been updated • A note has been added to the MSL table to add recommendations on counter to include in case of AES key being used • Recommendations on S@T and WIB application MSL values have been added • Recommendations have been added on applicative keys management • Recommendations have been added on applet verification to use the last version of the export file when using bytecode verifier • A new section to cover recommendations on 5G profiles has been added • A new section has been added to cover eUICC recommendations • Recommendations on the use of 3DES have been updated in light of NIST's decision to deprecate the block cipher	ISAG	James Moran. GSMA

A.2 Other Information

Type	Description
Document Owner	GSMA Fraud and Security Group
Editor / Company	James Moran, GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.