Security Guidelines for Exchange of UICC Credentials

Version 1.0

10 November 2020

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and 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.

Antitrust Notice

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

Table of Contents

1. Scope

This document provides security guidelines for the protection of UICC credentials exchanged between the MNO and the UICC vendor.

The guidelines do not address the security of the UICC profile itself as these are defined in FS.27 – Security Guidelines for UICC Profiles.

The document contains a number of 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 Abbreviations

Term	Description
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
DES	Data Encryption Standard
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
HSM	Hardware Security Module
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
MNO	Mobile Network MNO
NIST	National Institute of Standards and Technology
OTA	Over The Air
PGP	Pretty Good Privacy
RSA	Rivest Shamir Adleman
SFTP	SSH File Transfer Protocol
SSH	Secure Shell
SSL	Socket Secure Layer
TLS	Transport Layer Security
UICC	Universal Integrated Circuit Card
ZMK	Zone Master Key

1.2 References

Ref	DocNumber	Title
[1]	GSMA SAS	Accredited UICC Production Sites https://www.gsma.com/security/sas-accredited-sites/
[2]	NIST SP 800-90A Rev1	Recommendation for Random Number Generation Using Deterministic Random Bits Generators

Ref	DocNumber	Title
[3]	NIST SP 800-88	NIST Guidelines for Media Sanitization https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization
[4]	ENISA Handbook	Handbook on Security of Personal Data Processing https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing/at_download/fullReport
[5]	ITU-T X.509	Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks
[6]	Symantec	PGP Command Line from Symantec https://www.symantec.com/content/en/us/enterprise/white_papers/b-pgp-command-line-from-symantec-wp-21347937-en.pdf
[7]	AIS 31	A proposal for: Functionality classes for random number generators V2
[8]	GSMA FS.27	Security Guidelines for UICC Profiles https://infocentre2.gsma.com/gp/wg/FSG/OfficialDocuments/FS.27%20Security%20Guidelines%20for%20UICC%20Profiles%20v1.0%20(Current)/FS.27%20v1.0.docx

1.3 Conventions

The key words “must”, “must not”, “required”, “shall”, “shall not”, “should”, “should not”, recommended”, “may”, and “optional” in this document are to be interpreted as described in RFC2119.”

2. Accredited Vendor

The GSMA runs a voluntarily accreditation scheme called the Security Accreditation Scheme (SAS) for UICC production (SAS-UP) that subjects the production sites and processes of UICC vendors to a comprehensive security audit. Successful sites are awarded SAS-UP accreditation for a period of up to two years. The scheme has accredited, and enjoys the participation of, some of the industry’s largest UICC suppliers [1].

MNOs are advised to require their UICC vendors to be SAS accredited as part of their supplier selection process.

Note: The requirement for SAS accreditation is mandatory for eUICC.

3. Secure Data Exchange and Key Management

To ensure high levls of security, integrity and trust, it is essential that MNOs and UICC vendors exchange data used to provision the UICC and the network with the security credentials, (including cryptographic keys), in a secure manner. This section provides recommendations on the generation of security credentials (see Section 3.1), the protection of the exchange of credentials between MNOs and UICC vendors (see Section 3.2), the establishment of a secure channel between both parties (see Section 3.3) and the refresh and deletion of credentials (see Section 3.4).

3.1 Security Credential Generation

Cryptographic keys and other security credentials must be randomly generated or diversified. Diversification is the process of deriving security credentials from a:

- Master key
- Unique input exchanged between the MNO and the vendor, the diversification input data/salt.
- Derivation method

Key diversification can be implemented in a dedicated hardware component, called the Hardware Security Module (HSM), but still requires the master keys to be randomly generated.

Cryptographic keys can be randomly generated either by using

I. a dedicated hardware module that provides a true random source based on a physical phenomenon which is highly unpredictable; or
II. dedicated software, called pseudo-random number generator.

A pseudo-random number generator uses a special algorithm to generate a sequence of numbers, called pseudo-random numbers, from an initial set of input values, called the seed.

The seed should be generated using a hardware random number generator and changed periodically to avoid the sequence of pseudo-random numbers repeating itself and to protect it against cryptanalytic attacks.

We distinguish between two categories of security credentials that need to be generated:

- Credentials that are unique to each UICC (e.g. subscriber keys, OTA keys, service provider keys, subscriber specific parameters), called **UICC unique credentials** (see Section 3.1.1)
- Credentials that are common to one or several batches of UICCs (e.g. seeds, master keys, MNO specific parameters), called **UICC common credentials** (see Section 3.1.2).

3.1.1 Generation of UICC Unique Credentials

In case of the diversification the UICC unique credential is to be derived by the operation and the UICC vendor using:

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended - if supported
	Software Solution		Hardware Security Module (HSM)

The master key to be generated and stored using:

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended - if supported
	Software Solution		Hardware Security Module (HSM)

Advice and recommendations on the use of algorithms to derive a UICC unique credential are:

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended - if supported
Single DES[1] 3DES – 2 keys, with same value for both[2] 3DES – 3 keys, with same value for the three[2] 3DES – 3 keys, but first and second keys equal, or second and third keys equal[2]	3DES – 2 keys[3] 3DES – 3 keys	AES 128, 192	AES 256

[1] Single DES is deprecated by ETSI standard TS 102 225 since release 8.

[2] Equivalent to Single DES.

[3] 2-key 3DES is the same as 3-key 3DES where the first and third keys are identical.

The generation of the master key is recommended to be based on a random number generator conforming to the following recommendations. In addition, the same recommendations apply if other unique credentials are generated with a random number generator:

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended - if supported
	Software Random Generation		Hardware Random Generation compliant with recommendation [2] [7]

3.1.2 Generation of UICC Common Credentials

Two main families of UICC common credentials can be handled:

- Public UICC common credentials

- Public part in asymmetric cryptographic scheme (e.g. RSA/ECC public keys)

- Private and/or Shared UICC Common credentials
  - Private part in asymmetric cryptographic scheme (e.g. RSA/ ECC private keys)
  - Shared elements in symmetric cryptographic scheme (e.g. OP/TOP keys)

The Public and/or Shared UICC common credentials are recommended to be generated by the MNO and stored by the MNO and the UICC vendor using;

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended - if supported
	Software Solution		Hardware Security Module (HSM)

The Private UICC common credentials are recommended to be generated and stored only by the MNO using:

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended - if supported
	Software Solution		Hardware Security Module (HSM)

The random number generator involved in the generation is recommendation to be bsed on:

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended - if supported
	Software Solution		Hardware Random Generation compliant NIST recommendation [2]

The generation of Private and/or Shared UICC common credentials should be based on split knowledge among more than one MNO custodians to prevent any one person from knowing the complete value of the UICC common credentials.

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended - if supported
	One custodian performs generation		>= 2 Custodians perform generation

Note: For Shared UICC common credentials, such as the Milenage OP value or the TUAK TOP value, it is not currently realistic to avoid one person ever knowing the full value. In particular, Authentication Centres that need to be programmed with the OP or TOP value have it programmed all at once, not in parts or shares. An ambition for the future is for Authentication Centre programming interfaces to evolve to allow split entry of OP or TOP.

3.2 Secure Data Exchange

The exchange of security credentials, primarily unique credentials, between UICC vendors and MNOs is protected on three levels:

- 1st level: each credential is individually encrypted, referred to as **record protection** (see Section 3.2.1)
- 2nd level: encrypted credentials are combined in a file that is encrypted and integrity protected, referred to as **file protection** (see Section 3.2.2)
- 3rd level: protected files are exchanged using a secure protocol, referred to as **transport protection** (see Section 3.2.3)

Note: The combination of encryption algorithms must be at least as cryptographically strong as any of the cryptographic algorithm that uses these credentials as keys. Preferably, the encryption algorithm used for record protection must be at least as cryptographically strong as any of the cryptographic algorithm that uses these credentials as keys.

Note: Encryption at record level ensures the longest secure channel compared with file and transport protection. In addition to encryption at record level, encryption at file and transport level ensures the confidentiality of the nature of the exchanged data.

3.2.1 Record Protection

The individual encryption of credentials at the record level ensures these credentials remain protected in case a credentials file is compromised.

Each credential is to be encrypted using a transport key generated by the mobile MNO, which in turn needs to be encrypted and exchanged with the UICC vendor.

The credential record protection should follow the following recommendations:

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended - if supported
Secret in clear	All credential encrypted with same transport key	One transport key per credential data type (e.g. Ki, OTA keys) and per UICC vendor	

Advice and recommendations on the use of algorithms are:

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended - if supported
Single DES[1] 3DES – 2 keys, with same value for both[2] 3DES – 3 keys, with same value for the three[2] 3DES – 3 keys, but first and second keys equal, or second and third keys equal[2]	3DES – 2 keys[3] 3DES – 3 keys Each key shall have a different value	AES 128, 192	AES 256

[1] Single DES is deprecated by ETSI standard TS 102 225 since release 8.

[2] Equivalent to Single DES.

[3] 2-key 3DES is the same as 3-key 3DES where the first and third keys are identical.

3.2.2 File Protection

File level protection provides encryption and integrity protection to the security credentials in addition to their associated identifiers and parameters included in the same file.

Symmetric or asymmetric algorithms can be used.

X.509 provides an international standard for exchanging public keys although PGP has become the defacto standard within the mobile industry [5], [6].

Advice and recommendations on the use of algorithms are:

	Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended - if supported
Symmetric	ZIP + Password No logical encryption	3DES – 2 keys 3DES – 3 keys Each key shall have a different value	AES 128,192	AES 256
Asymmetric		PGP RSA < 2048b	PGP RSA 2048b	PGP RSA >= 4096b PGP ECC, order of subgroup >= 256

3.2.3 Transport protection

Transport level protection prevents a malicious party to intercept the protected files while in transit between the mobile MNO and the UICC vendor or to maliciously inject files.

Different protocols can be used with different security levels and the recommendations are as follows:

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended - if supported
eMail	HTTP, FTP, Courrier Transport		HTTPS FTPS SFTP CFT over TLS S/MIME

Recommendations on TLS versions to be used are:

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended - if supported
	SSL V2, V3 TLS 1.0, 1.1		TLS 1.2 or more recent versions

The recommend algorithms with suitable key size for all protocols are as follows:

Authentication:

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended - if supported
	RSA, DSA <= 1024 ECDSA <= 223		RSA >= 2048 ECDSA >= 224

Encryption:

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended - if supported
	3DES		AES >= 128

Integrity:

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended - if supported
	SHA1		SHA2 or SHA3

3.3 Establishment of Initial Secure Channel between Parties

To establish an initial secure channel in cryptographic symmetric mode, for efficient and secure exchange of further cryptographic keys and security parameters, both parties have to establish a common secret: the Zone Master Key (ZMK). When established, the ZMK is used to encrypt further keys which can be transmitted as cryptograms between parties and used to protect data transfers at any of the levels identified in Section 3.2, or to protect master keys for UICC credentials generation. The algorithm associated with the ZMK should be at least as strong as any of the keys it protects.

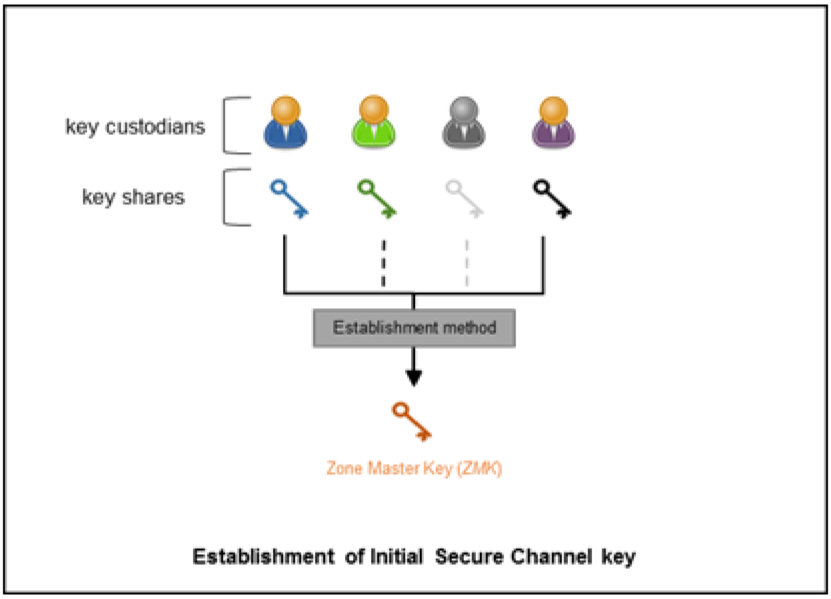

Figure 1. The ZMK is established from key shares, each key share known only by one key custodian

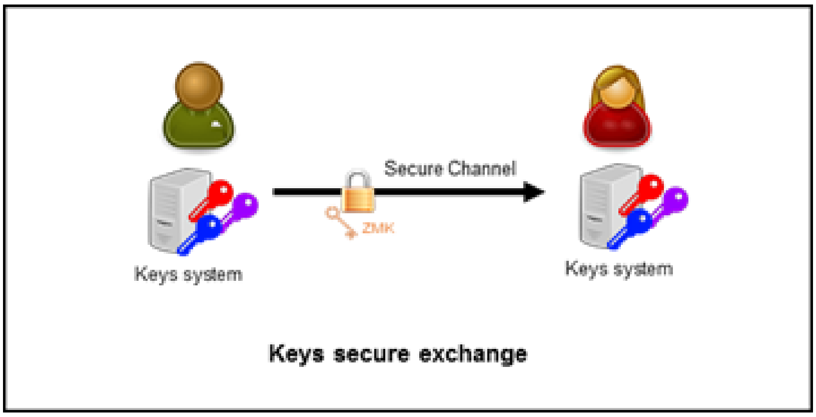

Figure 2. The ZMK protects the transmission of other keys which can be used in the derivation of unique credentials (Master Keys) or during their transport (Transport Keys).

For this key agreement two different methods are suggested:

- **Physical** transmission (see Section 3.3.1)
- **Digital** transmission (see Section 3.3.2)

3.3.1 Physical Transmission of the Zone Master Key Shares

If the ZMK is to be established through physical transmission, then it is recommended to split the key securely into two or more “key shares”, each as long as the ZMK. Two methods are proposed for this, although others are possible:

Method 1 – Key share hashing: Each key custodian at the UICC vendor or MNO generates one key share, each following the master key generation guidelines in Section 3.1 above. Each key share is transmitted by independent means to the counterpart key custodian in the other party (more details are provided later in this section). Both parties establish the ZMK by concatenating all of the key shares in an agreed order and format to produce one longer string, using that string as input to a secure hash function such as SHA-256, and taking as many bits as required of the hash function output as the ZMK. Concatenation and hashing must be done using a system not allowing access to independent key shares in clear (e.g. Hardware Security Module). Only the KCV (Key Check Value) of the established ZMK is output to confirm integrity from both parties.

Method 2 – Key share XORing: Each key custodian at the UICC vendor or MNO generates one key share following the master key generation guidelines in Section 3.1 above. Each key share is transmitted by independent means to the counterpart key custodian in the other party (more details are provided later in this section). The ZMK is established by computing the bitwise XOR of the N key shares. XOR-ing must be done using a system not allowing access to independent key shares in clear (e.g. Hardware Security Module). Only the KCV (Key Check Value) of the established ZMK is output to confirm integrity from both parties.

Key shares may be sent either printed on paper or on digital storage media. Each key share is then sent to the counterpart key custodian of the receiving party sealed in a tamper evident bag. After each receiving party key custodian acknowledges receipt of the key part unbroken the next part will be sent, preferably via another transport medium. If the key has been split into more than two parts additional parts should be sent following the same steps.

After the ZMK has been computed by the receiving party, the integrity of the ZMK consolidated version can be confirmed using KCV (Key Check Value) verification with the sending party.
The key shares should then be securely destroyed and destruction should be confirmed to the other party.

3.3.2 Digital Transmission of the Zone Master Key Shares

Key shares generation principle presented in previous section applies, digital transmission of each key share (replacing sealed tamper evident bag in Section 3.3.1) is described below.

Key custodians at both the UICC vendor and the MNO generate a public/private key pair following the guidelines set out in Section 3.1.1 as far as possible (note that encryption tools such as PGP have their own mechanisms for key pair generation that the user cannot change).

The public keys can then be exchanged in digital format (e.g. via email). After public key exchange, both parties should check the key fingerprints via a separate channel (e.g. via phone).

Once key integrity is confirmed by both sides, one party can generate the actual Zone Master Key share, and after encrypting it with the other party's public key it can be sent to the counterparty.

Each custodian shall verify that only their own RSA key pair was used to encrypt the Zone Master Key share received from their counterpart to ensure no other party has access to the Zone Master Key share.

The public/private RSA key pair can be securely erased after the Zone Master Key share has been decrypted.

3.4 Data Retention Related Security Credentials

The protection of the files exchanged between the UICC vendor and the MNO as mentioned in Section 3.2.2 is not limited to exchange in a secure way.

Once the file has been exchanged and processed a period of data retention is recommended to be defined. Except for specific MNO requirements, it is recommended that data and files not be stored for more than seven months at the UICC vendor site after receipt of the input file, transmission of the output file and despatch of the UICC shipment.

At the end of data retention period files, and related backups, shall be securely erased using secure methods such as those recommended in NIST's SP 800-88 Guidelines for Media Sanitisation [3] and ENISA's Handbook on Security of Personal Data Processing [4].

3.5 Key Management

A number of keys are involved in the protection of security credentials. Consequently, a robust key management process is recommended to be applied to these keys during the entire lifecycle, from generation to end of life.

As a basic principle, MNOs shall only use keysets for one UICC vendor and UICC vendors shall not reuse or share keys across various customers.

A key should have a finite life span. A renewal process should be in place that ensures keys are changed at least every 3 years.

It is essential to monitor key usage and verify the efficacy and security of algorithms and protocols in use to ensure they remain fit for purpose.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	27-Oct-20	New PRD	TG	Eric Gauthier, Orange

A.2 Other Information

Type	Description
Document Owner	Fraud and Security Group
Editor / Company	Eric Gauthier, Orange

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.