Security Guidelines for UICC Profiles

Version 1.0

12 June 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 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
ADM	Administrative Keys
AES	Advanced Encryption Standard
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
CC	Common Criteria
CHV	Card Holder Verification (PIN)
DAP	Data Authentication Pattern
DES	Data Encryption Standard
DF	Dedicated File
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
DRBG	Deterministic Random Number Generator

Term	Description
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)
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
RFM	Remote File Management
RSA	Rivert, Shamir & Adelman
SD	Security Domain
SGSN	Serving GPRS Support Node
SMS	Short Message Service
SPA	Simple Power Analysis
SQN	Sequence Number
SSD	Supplementary Security Domain
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

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.

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

* 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 Customisation

The Milenage and TUAK algorithms can be customised using specific operator key parameters called OP and OPc for Milenage and TOP and TOPc for TUAK.

OP is a 128-bit Operator Variant Algorithm Configuration Field that is a component of the Milenage functions f1, f1*, f2, f3, f4, f5 and f5*.

OPc is a 128-bit value derived from OP and the (e)UICC secret key K and used within the computation of the functions.

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.

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 vendor as it is transparent to the UICC.

The sequence number parameters Δ and L must 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, Annex C, SQN = SEQ || IND, where IND is an index used in the array scheme described in 3GPP TS 33.102, Annex C.1.2 and C.2.2. In the profiles in 3GPP TS 33.102, 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, 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.

3 Theft Protection

The UICC (or profile on an eUICC) can be locked and unlocked using two parameters called Card Holder Verification (CHV) and Personal Unblocking Key (PUK). 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

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

3.2 PUK

- The PUK attempt counter shall be set to 10 (0x0A HEX), by default
- Randomly generated or properly derived values should be used.
- The values must be diversified card by card.

4 Cryptographic Keys

The UICC uses cryptographic keys for network authentication and for remote management and administration purposes. Keys must have different values and should be diversified per type of usage (per ADM, per KeySet) and per UICC.

4.1 Administrative Keys (ADMs)

The administrative keys control the access to, and modification of, the configuration parameters of the UICC.

- Ensure that access rights on file system are mapped on appropriate ADMs codes.
- ADMs must be properly derived or randomly generated.
- ADMs must be at least 64 bits long.

4.2 Keys for Remote Access (KIc, KID)

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 must be properly derived or randomly generated if derivation is not used. Fixed values are totally forbidden.
    - Using derivation will prevent the need to further exchange the final values between vendor and operator, as both sides can perform the same derivation process.
    - Using random value mandate to exchange the value between vendor and operator.
- Values of KIc and KID must not be the same and must be different.
- Keys should be diversified per KeySet. For example, KIC of KeySet1 and KIC of KeySet2 should be different.

4.3 Remote Provisioning Key (KIK)

The Key Identifier for protecting KIc and KID (KIK) is used to protect the KIC and KID keys when provisioned over the air by the network.

- Algorithm and length of KIK (used for Put Key) should be equivalent to, or stronger than, the strongest algorithm and length of KIC and KID.
- KIK must be properly derived or randomly generated if derivation is not used. Fixed values are totally forbidden
- Values of KIc and KID must not be the same and must be different.

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)

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 of each EF ARR within the electrical profile shall be set to ADM code as defined in the Standards (3GPP 51.011, 31.102 & 31.103).
- The electrical profile (access condition of files not in line with access domain of application) will be capable of being updated in the field if needed.

- 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 GlobalPlatform Privileges

The applications running on the UICC (or profile on an eUICC) can be assigned a number of access rights that are standardised by GlobalPlatform and referred as GlobalPlatform privileges.

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

5.3 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.

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

5.4 Access Conditions

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

- For standard files, access conditions must follow the recommendations contained in the ETSI/3GPP standards.
- For applicative files, access conditions must 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 generation of SCP 80 keysets.

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)

6.1.2 Algorithms for HTTPS (SCP81)

The table below details the algorithms that can be used for generation of SCP 81 Keysets

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended
HTTPS TLS 1.0 or HTTPS TLS 1.1 TLS_PSK_WITH_NULL_SHA, as defined in RFC 4785 [PSK NULL] TLS_PSK_WITH_3DES_EDE_CBC_SHA, as defined in RFC 4279 [PSK TLS] TLS_PSK_WITH_AES_128_CBC_SHA, as defined in RFC 4279 [PSK TLS]		**HTTPS TLS 1.2** TLS_PSK_WITH_NULL_SHA256, as defined in RFC 5487 [PSK 256]	**HTTPS TLS 1.2** TLS_PSK_WITH_AES_128_CBC_SHA256, as defined in RFC 5487 [PSK 256]

Note: For recommendations on the use of GlobalPlaform secure channel protocols, refer to http://globalplatform.org

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 security applied to each application during installation. This security level shall be applied in OTA commands sent to an application. In section 6.3.1 each security level is defined

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

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

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended
	0x00: No security		
	0x01: Redundancy Check		
		0x02: Cryptographic Checksum	
	0x04: Ciphering		
	(2)0x05: Ciphering & Redundancy Check		
		0x06: Ciphering & Cryptographic Checksum	
	0x08: Counter available		
	0x09: Redundancy Check & Counter available		

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended
		0x0A: Cryptographic checksum & Counter available	
	0x0C: Ciphering & counter available		
	(2)0x0D: Redundancy Check & Counter available & Ciphering		
		0x0E: Cryptographic Checksum & Counter available & Ciphering	
	0x10: Counter with check if counter value is higher than RE		
	0x11: Redundancy Check & Counter value is higher than RE		
			0x12: (Integrity & No Confidentiality) Cryptographic Checksum (CC) & - anti replay counter
	0x14: Ciphering & anti replay counter with check if counter value is higher than RE		
	0x15: (Integrity & Confidentiality) Redundancy Check (RC) & Anti replay counter with check if counter value is higher than RE & Ciphering		
			0x16: (Integrity & Confidentiality) Cryptographic Checksum (CC) & - anti replay counter with check if counter value is higher than RE & Ciphering
	(1)0x18: Counter value is one higher than RE		
	(1)0x19: Redundancy Check & Counter value is one higher		

Deprecated	Not recommended – vulnerable to known attacks	Acceptable	Recommended
	than RE		
			(2)0x1A: Cryptographic checksum (CC) & anti replay counter with check if counter value is one higher than RE
	(1)0x1C: Ciphering & Counter value is one higher than RE		
	(1), (2) 0x1D: Redundancy Check (RC) & anti replay counter with check if counter value is one higher than RE & ciphering		
			(2)0x1E: 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 since 102.226 and UICC Configuration mandate CC for RAM operations

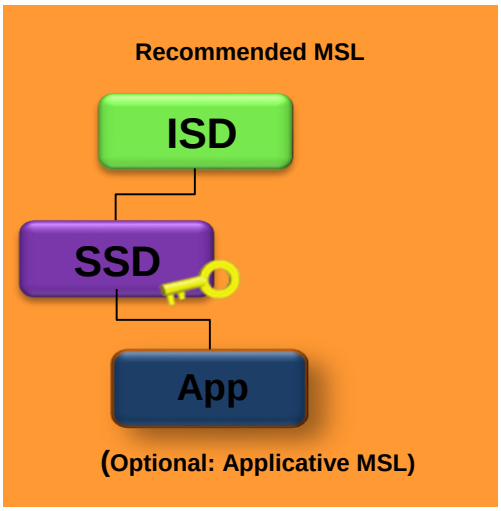
6.3.2 Minimum Security Level (MSL) for Basic Applications

The minimum security level attached to a toolkit application (other than RAM/RFM applications) must 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 server should be consistent to ensure good security behaviour.

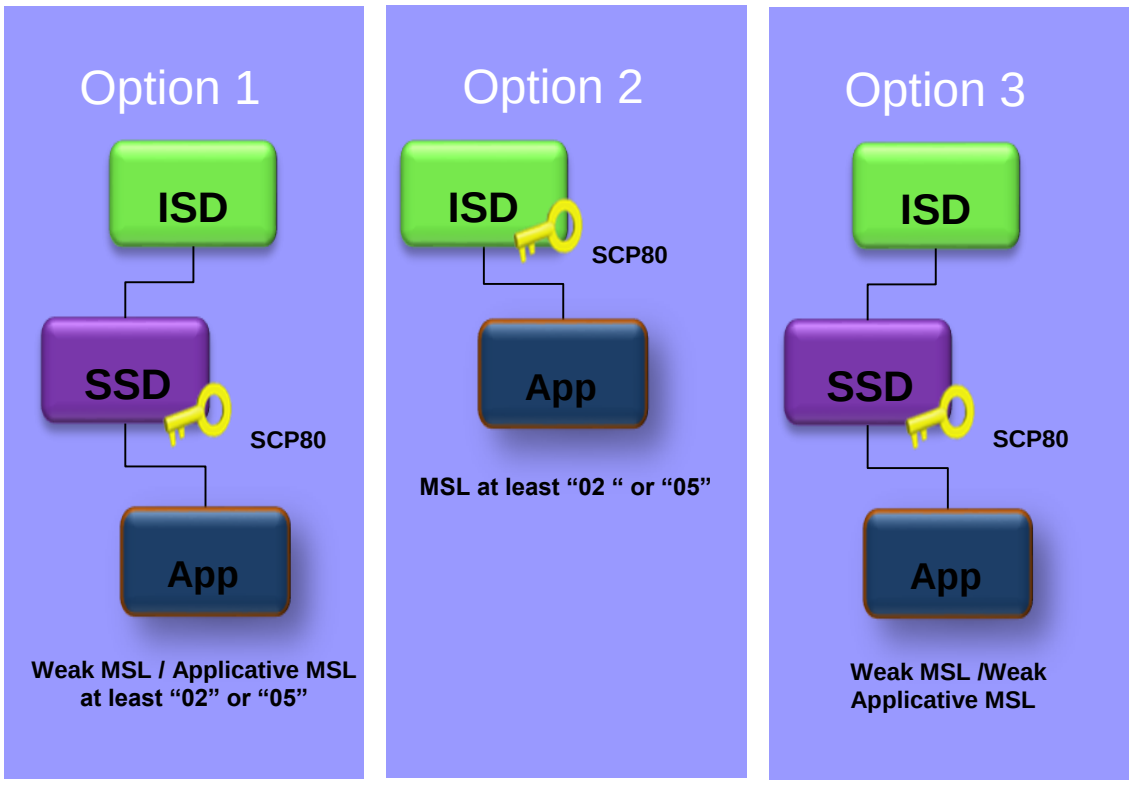
6.3.3 Basic Application Recommendation

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



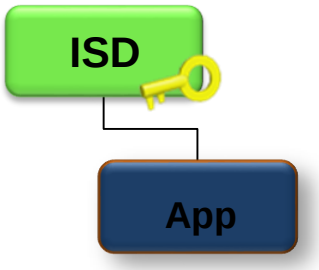
6.3.4 Alternative Options

The following options in table below are acceptable due to possible solution constraints



6.3.5 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 101.220 Annex D) but use a proprietary TAR instead.

7 Application Design

7.1 Applicative Keys

Applicative keys (whether they are used for OTA access or not) must be stored either in a dedicated security domain or in application itself.

Where keys are sent over a secure channel, the key used for channel encryption must be at least as strong as the key being transmitted. In particular, if the key being transmitted is for either 3-key Triple DES or AES, then the key for the secure channel must also be either 3-key Triple DES or AES. It should not be a 2-key Triple DES key.

7.2 Applicative File System

If a file system is needed on the UICC a dedicated file (DF) and its associated Elementary File Access Rule Reference (EF_ARR) are recommended.

Access conditions on the file system must be aligned with the access domain of the applet.

8 Side Channel Attack Recommendations

UICCs must 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 must 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 scenarios, all applets must have a DAP.

9.3 Java applets

Java applets must, at a minimum, follow the “GlobalPlatform Card Composition Model Security Guidelines for Basic Applications”. In particular, Java applets must 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.

Java applet AID must be checked: correct RID, PIX,..

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

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.