3GPP TR 33.834 V16.1.0 (2019-03)

Technical Report

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Security aspects;

Study on Long Term Key Update Procedures (LTKUP)

 (Release 16)

 

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.
The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.
This Report is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.
Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

LTKUP,security, key

***3GPP***

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis

Valbonne - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

***Copyright Notification***

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 2019, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners

GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword 6

1 Scope 7

2 References 7

3 Definitions and abbreviations 8

3.1 Definitions 8

3.2 Abbreviations 9

4 Background 9

5 Identification of long term keys 10

5.1 Introduction 10

5.2 K / Ki 10

5.3 OP / Opc / TOP / TOPc 11

5.4 OTA Keys 11

6 USIM related key stores and key transport processes 12

6.1 Introduction 12

6.2 Potential Key Stores 12

6.2.1 Personalisation centre 12

6.2.2 eSIM provisioning elements 12

6.2.3 Network operator provisioning system 12

6.2.4 HSS / AuC 13

6.2.5 USIM / SIM 13

6.3 Example key transport interfaces 13

7 Key issues 13

7.1 Key Issue 1: individual subscription - K exposed 13

7.1.1 Issue description 13

7.1.2 Threat Description 13

7.1.3 Potential Security requirements 14

7.2 Key Issue 2: batch of subscriptions - K exposed 14

7.2.1 Issue description 14

7.2.2 Threat Description 14

7.2.3 Security requirements 15

7.3 Key Issue 3: LTK Derivation vs. LTK Transport 15

7.3.1 Issue description 15

7.3.2 Threat Description 15

7.3.3 Security requirements 15

8 Evaluation Criteria 17

8.1 Overview 17

8.2 Key Issues Addressed 17

8.3 Impact on USIM and ISIM, types and releases 17

8.4 Impact on USIM hardware and software 17

8.5 Key exchange protocols and their transportation 18

8.6 3GPP technologies supported 18

8.7 Assessment of additional risks 18

8.8 Lawful Interception impacts 18

8.9 Impact on core and RAN networks 18

8.10 Ease of implementation 18

9 Solutions 18

9.1 Solution #1: 'Replace the affected Profile on eUICC' 18

9.1.1 Introduction 18

9.1.2 Solution Description 18

9.1.3 Solution Evaluation 19

9.1.3.1 General evaluation 19

9.1.3.2 Key Issues 19

9.1.3.3 USIM and ISIM types applicable 19

9.1.3.4 Potential hardware and software impacts 19

9.1.3.5 Key exchange protocols and transportation 19

9.1.3.6 3GPP technologies supported 19

9.1.3.7 Assessment of additional risks 19

9.1.3.8 Conclusion 19

9.2 Solution #2: Pre-installed multiple key pairs 20

9.2.1 Introduction 20

9.2.2 Solution Description 20

9.2.3 Solution Evaluation 20

9.2.3.1 Key Issues 20

9.2.3.2 USIM and ISIM types applicable 21

9.2.3.3 Potential hardware and software impacts 21

9.2.3.4 Key exchange protocols and transportation 21

9.2.3.5 3GPP technologies supported 21

9.2.3.6 Assessment of additional risks 21

9.2.3.7 Conclusion 21

9.3 Solution #3: Certificate based negotiation 22

9.3.1 Introduction 22

9.3.2 Solution Description 22

9.3.3 Solution Evaluation 23

9.3.3.1 Key Issues 23

9.3.3.2 USIM and ISIM types applicable 23

9.3.3.3 Potential hardware and software impacts 23

9.3.3.4 Key exchange protocols and transportation 23

9.3.3.5 3GPP technologies supported 23

9.3.3.6 Assessment of additional risks 23

9.3.3.7 Conclusion 23

9.4 Solution #4: Diffe-Hellman based Key agreement 23

9.4.1 Introduction 23

9.4.2 Solution Description 24

9.4.2.1 Solution overview 24

9.4.2.2 Notes on statefulness at the HSS 25

9.4.2.3 Proposed message flow 26

9.4.2.4 Transport over new Signalling protocol (Solution 4a) 26

9.4.2.5 Transport over USIM OTA protocol (Solution 4b) 26

9.4.2.6 Transport over USSD protocol (Solution 4c) 27

9.4.2.7 Transport over BEST protocol (Solution 4d) 27

9.4.2.8 Transport over AUTHENTICATION protocol (Solution 4e) 27

9.4.3 Solution Evaluation 28

9.4.3.1 Key Issues 28

9.4.3.2 USIM and ISIM types applicable 28

9.4.3.3 Potential hardware and software impacts 28

9.4.3.4 Key exchange protocols and transportation 28

9.4.3.5 3GPP technologies supported 29

9.4.3.6 Assessment of additional risks 29

9.4.3.7 Conclusion 29

9.5 Solution #5: Multiple sets of parameters 29

9.5.1 Introduction 29

9.5.2 Solution Description 29

9.5.3 Solution Evaluation 31

9.5.3.1 Key Issues 31

9.5.3.2 UICC applications types applicable 31

9.5.3.3 Potential hardware and software impacts 31

9.5.3.4 Key exchange protocols and transportation 31

9.5.3.5 3GPP technologies supported 31

9.5.3.6 Assessment of additional risks 31

9.5.3.7 Lawful interception impacts 31

9.5.3.8 Core and RAN networks impacts 31

9.5.3.9 Ease of implementation 32

9.6 Solution #6: LTK generation 32

9.6.1 Introduction 32

9.6.2 Solution Description 32

9.6.3 Solution Evaluation 33

9.6.3.1 Key Issues 33

9.6.3.2 USIM and ISIM types applicable 33

9.6.3.3 Potential hardware and software impacts 33

9.6.3.4 Key exchange protocols and transportation 33

9.6.3.5 3GPP technologies supported 33

9.6.3.6 Assessment of additional risks 33

9.6.3.7 Conclusion 33

10 Conclusions 34

Annex A: Change history 35

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

# 1 Scope

The present document is a study on the remote update of 3GPP long term secret keys held in a SIM / USIM.

It:

- Identifies which Long Term Keys should be updatable within this proposed feature.

- Identifies the 3GPP/non 3GPP elements that would be affected by the update of these keys.

- Identifies the Key Issues relating to the updating of long term keys.

- Identifies potential requirements for the updating of long term keys.

- Identifies the applicability of Long Term Key Updating to GSM, UMTS, LTE and 5G and how the requirements may change across these technologies.

- Identifies solutions for the updating of long term keys.

- Evaluates solutions for the updating of long term keys.

- Concludes on the best solutions(s) for the updating of long term keys.

- Makes recommendations for further work.

This study will consider existing and new solutions that can be used for the update of 3GPP Long Term Keys.

The management of subscriptions is out of scope for the present document.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] GPC\_SPE\_093: "GlobalPlatform Card Specification v.2.2 Amendment F: Secure Channel Protocol '11'".

[3] 3GPP TS 33.102: "3G Security; Security architecture".

[4] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[5] 3GPP TS 31.115: "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications".

[6] ETSI TS 102 225: "Smart Cards; Secured packet structure for UICC based applications".

[7] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application".

[8] 3GPP TS 35.205: "3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1\*, f2, f3, f4, f5 and f5\*;Document 1: General".

[9] 3GPP TS 35.231: "Specification of the Tuak algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1\*, f2, f3, f4, f5 and f5\*; Document 1: Algorithm specification".

[10] GSMA SGP.22: "RSP Technical Specification".

[11] GSMA SGP.02: " Remote Provisioning Architecture for Embedded UICC Technical Specification".

[12] ETSI TS 102 226: "Smart Cards; Remote APDU structure for UICC based applications".

[13] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[14] 3GPP TS 31.116: "Remote APDU Structure for (U)SIM Toolkit applications".

[15] 3GPP TS 31.111: "Universal Subscriber Identity Module (USIM)
Application Toolkit (USAT)".

[16] 3GPP TS 33.163: "Battery Efficient Security for very low Throughput Machine Type Communication (MTC) devices (BEST)".

[17] GSMA SGP.01: "Embedded SIM Remote Provisioning Architecture".

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**DEK:** Key used to update USIM OTA keys detailed in ETSI TS 102 226 [12]

**eSIM:** A USIM provisioning mechanism specified in GSMA SGP.22 [10] and GSMA SGP.02 [11]

**KIC:** OTA ciphering key specified in ETSI TS 102 225 [6]

**KID:** OTA digital signing key specified in ETSI TS 102 225 [6]

**MILENAGE:** authentication and key generation algorithm as specified in 3GPP TS 35.205 [8]

**OP:** 128-bit value chosen by the home network operator which is stored in the AuC/HSS that is used with MILENAGE

**OPc:** is defined as 128-bit value that is derived from OP and K

**OTA:** protocol specified in ETSI TS 102 225 [6]

**PoR:** Proof of Receipt as specified in ETSI TS 102 225 [6]

**TOP:** 128-bit value chosen by the home network operator which is stored in the AuC/HSS that is used with TUAK

**TOPc:** is defined as 128-bit value that is derived from TOP and K

**TUAK:** authentication and key generation algorithm as specified in 3GPP TS 35.231 [9]

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

KDF Key Derivation Function

LTK Long term Key

M2M Machine to Machine

MNO Mobile Network Operator

PKI Public Key Infrastructure

# 4 Background

The current mobile security architectures – GSM / GPRS, UMTS and LTE – rely almost entirely on the secrecy of the long term secret key (called Ki in GSM / GPRS, or K in UMTS/LTE –called K in this clause) that is stored in a USIM / SIM. Knowledge of the USIM OTA update keys may allow an attacker to modify/ read aspects of the USIM remotely.

The fundamental security assumption is that the attacker does not know K or the USIM OTA keys. But if this security assumption fails, the loss of security is catastrophic.

Long Term Keys might massively or individually leak to an attacker or attackers for a number of reasons, e.g.:

a) a security compromise at the factory (SIM vendor or subscription manager) where K is generated.

b) a security compromise of the communication channel over which Ki is transported from SIM vendor or subscription manager to network operator.

c) a compromise of the mobile operators' equipment or software.

d) an insider attack on the key store at a network operator or SIM vendor.

e) a local attack (e.g. side channel) on the SIM card in the supply chain.

f) a local attack (e.g. side channel) on the SIM card while temporarily "borrowed" from the customer.

g) by accident due to misconfiguration in the mobile operator network.

Operators and vendors should of course try to prevent any of (a) – (g) from happening. But the risks could be significantly reduced by the definition of a mechanism to recover from a compromise of the long term keys, or to replace long term keys potentially exposed to many of the threats listed above by new keys exposed to fewer of those threats.

Currently, there is no standardized mechanism within 3GPP that enables the secure and expedited update of the 3GPP specified long term keys in both the USIM and HLR/HSS either in bulk or for an individual subscriber.

This means that currently, if long term keys are exposed (through accidental exposure or other compromise), the only existing method of recovering from the compromise and re-establishing the same level of security is replacement/re-issuance of the USIM/UICC(s) (or USIM profile in eUICC(s)) and updating the HLR/HSS key(s) and/or OTA keys. The same is true even when there is no concrete evidence that the keys have been exposed, reducing the likelihood that they have been.

# 5 Identification of long term keys

## 5.1 Introduction

Long term keys are keys, used for security, that typically do not change in the device that they are stored and are used for repeated security transactions. 3GPP uses long term keys as a basis for authentication, authorisation and secure management.

The long term keys used for authentication between the 3GPP network and the UE and authorisation of services, are stored in the USIM and the HLR/AuC (GSM and 3G) or the HSS (LTE). In addition to the authentication keys, optionally the network operator may specify long term OTA keys for the management of the USIM.

For GSM and 3G, the long term keys for authentication are specified in 3GPP TS 33.102 [3].

For LTE, the long term keys for authentication are specified in 3GPP TS 33.401 [4].

OTA keys are specified in 3GPP TS 31.115 [5] and ETSI TS 102 225 [6].

## 5.2 K / Ki

The K (sometimes referred to as the Ki) is the permanent key securely stored on the USIM on a UICC and in the Authentication Centre AuC / HSS. Currently, this key may be either 128 bits or 256 bits long. K is defined as "USIM Individual key" in 3GPP TS 31.102 [7] which implies that it changes on a per USIM basis, however the uniqueness and the rules by which K is generated are not standardised in 3GPP. It is assumed in 3GPP standards that there is only one K per USIM.

This key is specified as a permanent key in 3GPP TS 33.401 [4] and as a "Long-term secret key shared between the USIM and the AuC" in 3GPP TS 33.102 [3]. 3GPP TS 31.102 [7] defines that the K is stored in the USIM but does not define a specific USIM file or storage mechanism for this. There are currently no standardised processes that change the K for a specific subscription, after issue of a USIM.

K is used, together with other parameters, by the authentication functions (f1 to f5) specified in 3GPP TS 33.102 [2] but it is never directly exposed outside of the AuC/HSS or the USIM.

It is typically, generated randomly for each USIM by the USIM supplier in a secure environment and transported securely to the home network operator to be placed in the AuC / HSS. As USIMs are typically produced in batches, the K's are typically transported to the home operator in batches. 3GPP does not standardise this communication.

K may be used for any authentication algorithm specified by the home network operator. It is used by MILENAGE as detailed in 3GPP TS 35.205 [8] and in TUAK as detailed in 3GPP TS 35.231 [9].

3GPP TS 31.115 [5] specifies mechanisms that allow files and parameters on a USIM to be updated remotely when the USIM is connected to a network, but as the storage of K is not standardised, this would be different for each type of USIM and it is likely that the current USIM would not support the remote changing of K through these mechanisms.

The GSMA eSIM specifications, GSMA SGP.22 [10] and GSMA SGP.02 [11] describe remote profile provisioning processes that provision K "over the air" together with the rest of the USIM parameters. This may be used to change a whole USIM remotely after issue, but not to change a specific parameter within a USIM such as K.

## 5.3 OP / Opc / TOP / TOPc

OP, OPc, TOP and TOPc are used to provide separation between the functionality of the algorithms when the same algorithm (e.g. MILENAGE or TUAK) is used by different operators.

OP and OPc are defined in 3GPP TS 35.205 [8] for use with MILENAGE based authentication and are related to each other.

OP is defined as 128-bit value chosen by the home network operator which is stored in the AuC/HSS. There are no standardised rules for the generation and use of OP, but it is industry practice that OP is the same value across large batches of subscriptions and in some cases across all network subscriptions for a specific network operator. Typically, OP and / or TOP are generated by the home network operator and communicated to a UICC manufacturer by non-electronic means.

OPc is defined as 128-bit value that is derived from OP and K which is stored in the USIM. As the K is expected to change for each USIM, this means that OPc is likely to be different for each USIM. 3GPP TS 35.205 [8] defines that the OPc is stored in the USIM but 3GPP TS 31.102 [7] does not define a specific USIM file or storage mechanism for this. There are currently no standardised processes that change the OPc for a specific subscription, after issue of a USIM.

TOP and TOPc are defined in 3GPP TS 35.231 [9] for use with TUAK based authentication and are related to each other.

TOP is defined as 256-bit value chosen by the home network operator which is stored in the AuC/HSS. There are no standardised rules for the generation and use of TOP, but it is industry practice that TOP is the same value across large batches of subscriptions and in some cases across all network subscriptions for a specific network operator.

TOPc is defined as 128-bit value that is derived from TOP and K which is stored in the USIM. As the K is expected to change for each USIM, this means that TOPc is likely to be different for each USIM. 3GPP TS 35.231 [9] defines that the TOPc is stored in the USIM but 3GPP TS 31.102 [7] does not define a specific USIM file or storage mechanism for this. There are currently no standardised processes that change the TOPc for a specific subscription, after issue of a USIM.

3GPP TS 31.115 [5] specifies mechanisms that allow files and parameters on a USIM to be updated remotely when the USIM is connected to a network, but as the storage of OPc or TOPc is not standardised, this would be different for each type of USIM and it is likely that the current USIM would not support the remote changing of OPc or TOPc through these mechanisms.

The GSMA eSIM specifications, GSMA SGP.22 [10] and GSMA SGP.02 [11] describe remote profile provisioning processes that provision OPc or TOPc "over the air" together with the rest of the USIM parameters. This may be used to change a whole USIM remotely after issue, but not to change a specific parameter within a USIM such as OPc or TOPc.

## 5.4 OTA Keys

ETSI TS 102 225 [6] and ETSI TS 102 226 [12] define a secure mechanism for "over the air" update of USIM files and applications. Up to 15 optional secret keys for cyphering (KIC) and15 optional secret keys for digital signing (KID) or cryptographic checksum are defined for the over the air protocol. These are stored securely in the USIM and in a one or more "OTA severs".

OTA servers are used to update USIM files and applications, the OTA server(s) are typically part of the home network operator's domain. However, as the ability for each OTA keyset to manage files and applications on the USIM can be very finely set and as the OTA mechanisms can also be used to update non standardised files, it is not uncommon for an OTA server to exist outside of a network operators domain that can manage specific USIM files for specific USIMs in a specific way.

The key lengths for KIC and KID depend on the algorithm being used and are defined as being:

- 128 bits for two key 3DES,

- 192 bits for three key 3DES,

- 128 bits, 192 bits or 256 bits for AES,

- no standardised length for proprietary algorithms.

KIC, KID and DEK values are usually generated by the USIM supplier and are typically different for each USIM. These values are then distributed to the relevant OTA servers by the UICC manufacturers as agreed by the home network operator. In some cases, some keys need to be sent to 3rd parties in a way that the home network operator cannot determine the key values.

KIC and KID keys are typically associated to form a keyset. ETSI TS 102 226 [12] defines a secure mechanism for updating the KIC and KID keys as a keyset (PUT KEY) that uses an additional static Key, DEK, for each of the 16 keysets. There is no 3GPP or ETSI mechanism for updating the DEK.

USIM applet updates are typically managed using the ETSI TS 102 225 [6] protocol using specific KID and KIC keys without the need for any additional keys. This is detailed in ETSI TS 102 226 [12].

The GSMA eSIM specifications, GSMA SGP.22 [10] and GSMA SGP.02 [11] describe remote profile provisioning processes that provision KIC, KID and DEK values "over the air" together with the rest of the USIM parameters. This may be used to change a whole USIM remotely after issue, but not to change a specific parameter within a USIM such as KIC, KID and DEK.

# 6 USIM related key stores and key transport processes

## 6.1 Introduction

During the lifecycle of a USIM secret keys may be generated and transported between many elements.

## 6.2 Potential Key Stores

### 6.2.1 Personalisation centre

Typically, the personalisation centre is a UICC manufacturer factory that generates USIM profiles and their keys and stores these keys for an agreed amount of time. There is no specific definition of a personalisation centre in 3GPP, ETSI or GSMA.

### 6.2.2 eSIM provisioning elements

GSMA SGP.02 [10] and GSMA SGP.22 [11] define specific provisioning elements that contain the secret key information.

### 6.2.3 Network operator provisioning system

It is normal for a network operator to have a system that manages and distributes subscription information between the home network operator elements. This service is not standardised in 3GPP, ETSI or GSMA.

### 6.2.4 HSS / AuC

The AuC and HSS are secure 3GPP elements that are standardised by 3GPP. The AuC (for GSM and UTRAN) is defined in 3GPP TS 33.102 [3] and the HSS (for LTE) is defined in 3GPP TS 33.401 [4].

The AuC and HSS securely store information used for authentication and create authentication vectors used for 3GPP authentication. These elements store K for each USIM and OP and TOP as specified by the home network operator.

### 6.2.5 USIM / SIM

The USIM (and SIM for legacy use) stores and uses the K/Ki for the subscription and the OPc and or TOPc as required. The UICC stores and uses the OTA keys KIC, KID and DEK as specified by the home network operator.

## 6.3 Example key transport interfaces

Typically, the following transport interfaces are used to transfer long term keys together with other information:

- Personalisation centre to network operator provisioning system

- Network operator provisioning system to HLR / HSS / AuC

- eSIM provisioning systems to Network operator provisioning systems

- Network Operator provisioning systems to OTA server(s)

- Personalisation centre to OTA server(s)

These interfaces are not standardised by 3GPP and it is up to the home network operator to make sure that these are suitably secure. Some of these systems are batch systems with typically 10 - 100K subscriptions per batch others are on a per subscription basis.

# 7 Key issues

## 7.1 Key Issue 1: individual subscription - K exposed

### 7.1.1 Issue description

This Key issue is where an individual subscription key K is exposed by some means. This may happen due to:

- a security compromise at the factory (UICC vendor or subscription manager) where K is generated.

- a compromise of the mobile operators' equipment or software.

- an insider attack on the key store at a network operator or UICC vendor.

- a local attack (e.g. side channel) on the UICC in the supply chain.

- a local attack (e.g. side channel) on the UICC while temporarily "borrowed" from the customer.

- by accident due to misconfiguration in the mobile operator network.

For this key issue, only one subscription is compromised and no information is exposed that could reduce the security of any other subscription.

### 7.1.2 Threat Description

An attacker who knows the K for a specific subscriber may be able to:

- decrypt encrypted communications that are taking place or were pre-recorded.

- clone a USIM subscription and use services that the cloned subscriber may be billed for.

However for these attacks to succeed, the attacker would also need to know (or be able to guess) other parameters such as OP/OPc, TOP/TOPc, and (for some attacks) the sequence number system being used.

The home network operator has many ways of detecting cloning attacks such as frequent re-synching of sequence numbers, wrong re-synch procedures used, same subscription active at two distant locations, USIM not OTA updatable. It will typically be much harder, however, to detect passive eavesdropping attacks.

For a customer, the consequences are that their service may become more unreliable, their calls and data may be eavesdropped and they may be billed incorrectly.

The consequence for the operator is that as there is only one customer affected, a replacement of the UICC is far less costly (than a mass replacement of UICCs). For an IoT UICC this may still be very costly due to the location of the UICC and the access required to change it. Moreover, an operator is likely only to replace a UICC if its key is known to be compromised; if the attacker is able to keep the compromise secret (e.g. only carrying out passive eavesdropping attacks) then the operator is likely to remain unaware and therefore takes no action.

If this attack is due to a systematic failure, the network operator may suffer loss of reputation and / or punishment from a regulatory body.

### 7.1.3 Potential Security requirements

The home network operator shall have a means to change the K/OPc or K/TOPc combination being used for 3GPP authentication on a specific USIM. It is expected that this change will be infrequent.

Where used, the communication used to transport a new K/OPc or K/TOPc shall be both tamper resistant and confidentiality protected by a suitably strong means.

Where communication is used to indicate the K/OPc or K/TOPc to use, it shall be initiated by the home operator and shall be tamper resistant, replay protected and optionally confidentiality protected by a suitably strong means.

## 7.2 Key Issue 2: batch of subscriptions - K exposed

### 7.2.1 Issue description

This Key issue is similar to Key issue 1 except a batch of subscriptions are compromised at the same time.

### 7.2.2 Threat Description

An attacker who knows the K for a specific subscriber may be able to:

- decrypt encrypted communications that are taking place or were pre-recorded.

- clone a USIM subscription and use services that the cloned subscriber may be billed for

However for these attacks to succeed, the attacker would also need to know (or be able to guess) other parameters such as OP/OPc, TOP/TOPc, and (for some attacks) the sequence number system being used.

The home network operator has many ways of detecting cloning attacks such as frequent re-synching of sequence numbers, wrong re-synch procedures used, same subscription active at two distant locations, USIM not OTA updatable. It will typically be much harder, however, to detect passive eavesdropping attacks.

For a customer, the consequences are that their service may become more unreliable, their calls and data may be eavesdropped and they may be billed incorrectly.

The consequence for the operator is that as a whole batch is affected, a replacement of the UICCs is potentially very costly. For IoT UICCs this may be even more costly due to the location of the UICCs and the access required to change them. Moreover, an operator is likely only to replace UICCs if the keys are known to be compromised; if the attacker is able to keep the compromise secret (e.g. only carrying out passive eavesdropping attacks) then the operator is likely to be unaware and therefore takes no action.

If this attack is due to a systematic failure, the network operator may suffer loss of reputation and / or punishment from a regulatory body.

### 7.2.3 Void

## 7.3 Key Issue 3: LTK Derivation vs. LTK Transport

### 7.3.1 Issue description

A compromise of LTK (K, a.k.a permanent key or USIM Individual key) may happen while it is being transported between stakeholders' domains or while being stored.

a) a security compromise of the communication channel over which Ki is transported from SIM vendor or subscription manager to network operator.

b) a compromise of the mobile operators' equipment or software.

c) an insider attack on the key store at a network operator or SIM vendor.

Such a leak may have dire consequences for the security of the entire system.

At the onset, there are risks inherent to the fact that LTK is being transported across various stakeholders' domains (i.e., changing hands) during provisioning, namely:

- between SIM vendor and MNO sites during conventional UICC personalization process;

- between MNO, SM-DP and eUICC during eUICC remote provisioning procedures.

A conventional recovery scenario for the MNO may be realized through a replacement of the UICC for the affected subscriber. However, this approach can be impractical and very costly when dealing with a very large number of compromised subscriptions. Such an approach may be costly even for a single M2M device, primarily for reasons given here:

a) in the case of a single M2M device physically located in a hard-to-reach place; and

b) certain devices' hardware layouts may make the UICC access and replacement extremely difficult. In addition, physical replacement of UICCs may create high customer impact in forms of service friction and disruption to service.

### 7.3.2 Threat Description

Unauthorized usage of MNO services that are still billed to the affected subscriber(s) (e.g., via a cloned USIM).

Unauthorized decryption of the communications (live or pre-recorded) of the affected subscriber(s).

Unreliability of the service due to unauthorized use of the same subscription from multiple locations (e.g., causing frequent re-synching of messages' sequence numbers).

Possible denial-of-service to legitimate subscribers.

### 7.3.3 Security requirements

In order to mitigate the above threats, it should be possible to generate the long term keys rather than distribute or transport them over communication channels.

Note: It is FFS which long term keys have to be updated.

7.4 Key Issue 4: Loss of Synchronisation of long term keys

7.4.1 Issue description

When updating the Long Term keys in the USIM and the network, if there is:

- an error in the process

- loss of network coverage

- an attack that prevents the re-synchronisation process from completing correctly

it may be possible for the Long Term Key stored in the USIM to be different to the Long Term Key stored in the Network.

This lack of synchronisation between the Long Term Keys will prevent the user from using all telecoms service (except emergency calls) and will also potentially prevent the re- synchronisation of the Long Term Keys making the USIM unusable.

7.4.2 Threat Description

Due to either:

- An error in the implementation of the LTKUP procedures.

- Loss of network coverage.

- The LTKUP procedures being re-run before the previous LTKUP procedure completes.

- An attack on the LTKUP procedure that corrupts the LTKUP process.

The USIM and the Network version of the same Long Term Key may be different.

If this occurs, then the user is unlikely to get any network service (other than emergency calls) and may have no way to remedy the situation without replacing the USIM.

7.4.3 Potential Security requirements

The LTKUP procedure shall mitigate against loss of telecoms service due to corruption of the LTKUP process.

The LTKUP process shall mitigate against loss of telecoms service due to the LTKUP procedures being run several times in parallel.

The LTKUP process shall be tolerant to losses of network service during the LTKUP process.

The LTKUP process shall have mechanisms to recover to a known good state if the LTKUP process fails.

7.5 Key Issue 5: undetected leakage of K

7.5.1 Issue description

This key issue addresses the use of LTKUP procedures to mitigate an undetected attack.

7.5.2 Threat Description

It is possible for an attacker to steal the long term keys without the Home Network operator knowing this has occurred.

An attacker who knows the K for a specific subscriber may be able to decrypt encrypted communications that are taking place or were pre-recorded, in a passive and generally undetectable way. However, for these attacks to succeed, the attacker would also need to know (or be able to guess) other parameters such as OP/OPc or TOP/TOPc.

For a customer, the consequences are that their calls and data may be eavesdropped over an extended period. If large scale leakage of K has occurred, then large scale eavesdropping may be possible.

There are occasions when the operator cannot detect that leakage has occurred, and thus has no reason to update or replace any particular UICC.

Using the LTKUP procedures pre-emptively may mitigate this type of attack.

7.5.3 Potential Security requirements

The network operator shall be able to trigger the LTKUP procedure without detecting a security compromise.

The LTKUP method shall reduce the risk of compromise from one or more of the following mechanisms:

a) a security compromise at the factory (SIM vendor or subscription manager) where K is generated.

b) a security compromise of the communication channel over which K is transported from SIM vendor or subscription manager to network operator.

c) a compromise of the mobile operators' equipment or software.

d) an insider attack on the key store at a network operator or SIM vendor.

e) a local attack (e.g. side channel) on the SIM card in the supply chain.

f) a local attack (e.g. side channel) on the SIM card while temporarily "borrowed" from the customer.

g) by accident due to misconfiguration in the mobile operator network.

# 8 Evaluation Criteria

## 8.1 Overview

In addition to the key issues described in the present document, the potential solutions also need to be evaluated against operational criteria when assessing their suitability. This clause details the evaluation criteria for the solutions.

## 8.2 Key Issues Addressed

Each solution clearly identifies the key issue(s) that it is addressing.

The evaluation l assesses whether this key issue is met and any limitations on the way it is met (e.g. if the solution is only applicable to aspects of the key issue).

The evaluation may assess the solution against all of the key issues.

## 8.3 Impact on USIM and ISIM, types and releases

The solution indicates whether it is possible to be used on USIM and or ISIMs and from which release (or all releases). Where a specific setup for the USIM is required (such as eSIM or any preloaded functionality), this should be stated.

The evaluation should clearly identify the types of USIM/ISIM that the solution works with and whether modification of existing USIMs / ISIMs is required.

## 8.4 Impact on USIM hardware and software

The solution details any likely impacts on the USIM hardware (e.g. additional processing power may be required if public keys are generated in the USIM or a specific hardware component may need adding to the USIM as part of the solution).

## 8.5 Key exchange protocols and their transportation

The solution details all key exchange and transport protocols (if any) used in the solution. These protocols are identified as new or existing (where existing means that this protocol exists in standards for this purpose already). The solution notes if any development of the protocols is required and provide a summary of the protocol changes.

## 8.6 3GPP technologies supported

The solution evaluation identifies the 3GPP technologies that the solution will work with and whether these technologies require any modification for this solution.

## 8.7 Assessment of additional risks

The solution evaluation identifies all additional risks that are due to the solution (e.g. if a new transport protocol is used there may be an additional risk due to the implementation of this new protocol).

## 8.8 Lawful Interception impacts

The solution evaluation identifies any Lawful intercept impacts it may have.

## 8.9 Impact on core and RAN networks

The solution identifies any changes required in the core network and or RAN.

## 8.10 Ease of implementation

The solution evaluation identifies what specifications need to change or whether new specifications are needed to implement it.

# 9 Solutions

## 9.1 Solution #1: 'Replace the affected Profile on eUICC'

### 9.1.1 Introduction

This solution discusses one potential way to update long term keys on the eUICC by using remote Profile provisioning processes defined in GSMA SGP.22 [11], specifically, by downloading a new Profile with new long term keys and deleting the Profile on the eUICC whose long term keys are exposed.

Profile is defined as combination of data and applications to be provisioned on an eUICC for the purpose of providing services. A Profile includes one MNO-SD and NAAs, where the MNO-SD contains the Operator's Over-The-Air (OTA) keys and provides a secure OTA channel, and NAAs include K/Ki for authentication between the 3GPP network and the UE. A Profile is identified by ICCID as defined in GSMA SGP.22 [10].

### 9.1.2 Solution Description

When the long term keys of the Profile on the eUICC are exposed, the end user can download a new Profile following the Profile download and installation procedure as defined in section 3.1.3 of GSMA SGP.22 v2.1 [10], and then the end user should delete the Profile whose long term keys are exposed following Profile deletion procedure as defined in section 3.2.3 of GSMA SGP.22 v2.1 [10].

### 9.1.3 Solution Evaluation

#### 9.1.3.1 General evaluation

This solution takes advantage of standardized GSMA eUICC Profile provisioning procedures to solve the issue of long term keys exposure, by downloading a new Profile to replace the affected Profile whose long term keys are exposed.

This solution requires no change of 3GPP specifications, neither GSMA eUICC specifications.

The usage of the solution is limited to eUICC, and does not apply to traditional UICC/SIM cards.

The solution requires the end user consent for Profile downloading and Profile deletion, which may confuse the end user as it is not expected by the end user, so the end user may reject the procedure.

The solution may also impact the end user data stored in some applets of the affected Profile, e.g. payment applet, when the whole Profile is replaced by a new one.

#### 9.1.3.2 Key Issues

This solution allows the long term keys to be changed as part of a secure profile change process but this requires solution user interaction to download / activate the new profile so it is not purely in the control of the home network operator.

Batch updates (Key issue 2) can only be achieved by multiple single updates and in this case this requires messaging to the end user to enable to change.

#### 9.1.3.3 USIM and ISIM types applicable

This solution is only available for eSIMs.

#### 9.1.3.4 Potential hardware and software impacts

This solution has no impact on eSIMs and eSIM provisioning services.

The user will be impacted as the new USIM downloaded will not include any of the user information contained on the old USIM (address book, SMS's, user preferred networks…).

#### 9.1.3.5 Key exchange protocols and transportation

The key exchange is defined in GSMA SGP.22 [10]. This is a secure protocol that includes replay protection, integrity protection and confidentiality protection. It is available over many types of bearer.

#### 9.1.3.6 3GPP technologies supported

This solution can be used on all 3GPP technologies (where an eSIM can be used).

#### 9.1.3.7 Assessment of additional risks

GSMA SGP.22 [10] is defined for consumer use and so requires user confirmation. This solution is not suitable for M2M use cases.

#### 9.1.3.8 Conclusion

This solution is a viable solution for consumer eSIM based USIMs. However, the update requires user interaction and the user is likely to lose data as the old USIM is replaced completely by a new USIM.

This solution requires all USIMs to be on consumer eSIMs.

This solution is not suitable for M2M use cases.

## 9.2 Solution #2: Pre-installed multiple key pairs

### 9.2.1 Introduction

This solution proposes to have multiple K/Opc or K/TOPc pairs pre-installed on the USIM and for the pair to be used to be indicated by some means.

This solution addresses key issue #1 and #2.

### 9.2.2 Solution Description

The USIM and the HSS may hold multiple K/OPc or K/TOPc pairs for a USIM subscription although the operation of this is not currently standardised.

For this solution, multiple K/OPc and/or K/TOPc combinations are loaded into the USIM at manufacture. The Ks may be either related to each other by the use of some strong algorithm or completely independent of each other. Where a strong algorithm is used to generate other K's, this will be pre-agreed between the network operator and the manufacturer and any keys used by this algorithm will be exchanged both securely and by a different means than the normal provisioning process.

Only one of the K/OP or K/TOPc combinations is sent to the network operator provisioning system by the normal provisioning means. If the K's are independent of each other, the other K's may be securely stored by the manufacturer or transported to the operator separately using a different transport mechanism.

When the operator determines that a change of K is needed (either in response to a compromising event or as part of a planned change to improve security), the operator signals this change to the USIM. This could be achieved using the following existing mechanisms:

- For 3G, LTE and 5G, the K to use could be signalled by the HSS in the authentication message using the proprietary AMF bits detailed in 3GPP TS 33.102 [3]. This has the advantage that the HSS and USIM will be synchronised even if several vectors have been pre-allocated to visited networks. Additionally, the home operator may also send an OTA message to the USIM prior to the sending of the authentication message with proprietary AMF bits. This OTA message activates the replacement mechanism to change K in the USIM.

- For all 3GPP technologies, the switch from one key to another could be made using a USIM OTA message. This message could either update a file that holds which K to use or a specific APDU for the purpose. As the handset will fail authentication while the USIM and HSS are out of sync, care will need to be taken as to when to update the HSS record with the new K. As there may be an authentication as part of the delivery of the SMS OTA, it is advised that the HSS is updated on receipt of a successful OTA PoR. This method could also be used to deactivate keys that are known to be compromised.

This solution does not require any changes to the current 3GPP specifications.

### 9.2.3 Solution Evaluation

#### 9.2.3.1 Key Issues

This solution does not mitigate a security issue due to a compromise at the manufacturer as all of the keys are preinstalled by the manufacturer. It may help to mitigate a compromise of the communication channel over which K is transported from the SIM vendor or subscription manager to the network operator, if different transport mechanisms are used for different keys (although it is left to the vendor and operator to select those different transport mechanisms). It may help to mitigate a compromise of the operator's equipment or software, or an insider attack at the operator, if only one key is initially sent to the operator. It may mitigate side channel attacks on the SIM card, although the details of this will depend on how individual keys are "activated".

This solution may mitigate all of the other potential attacks listed for key issue #1, but the extent of this depends on the details:

- It may help to mitigate a compromise of the communication channel over which K is transported from the SIM vendor or subscription manager to the network operator, if different transport mechanisms are used for different keys (although it is left to the vendor and operator to select those different transport mechanisms).

- It may help to mitigate a compromise of the operator's equipment or software, or an insider attack at the operator, if only one key is initially sent to the operator.

- It may mitigate side channel attacks on the SIM card, although the details of this will depend on how individual keys are "activated".

Where the AMF indication is used to indicate the K/OPc or K/TOPc to use, genuine AMF indications are suitably replay protected and integrity protected by the authentication procedure (see 3GPP TS 33.102 [3]). However, an attacker who has learned one of the stored keys can still spoof authentication vectors using that key, and thus carry out false network attacks.

Where USIM OTA is used to indicate the K/OPc or K/TOPc to use, this communication should be integrity protected, privacy protected and replay protected by the OTA protocol. Note: from the current options, only AES is recommended as a secure enough ciphering algorithm.

This solution mitigates Key issue 2 by updating the key to use on each effected USIM individually.

The solution has the potential to be quite effective at meeting reactive requirements (replacing a key that is known / suspected to be compromised): by proving diversity of keys, and potentially diversity about how those keys are transported, it may be less likely that a second key is compromised in the same way as a first one. The solution is less effective at meeting pre-emptively (making it less likely that a key in use is compromised): the diversity does not make it less likely that any one particular key is compromised.

#### 9.2.3.2 USIM and ISIM types applicable

This solution is suitable for all USIMs and ISIMs. This solution would also work with eSIMs.

#### 9.2.3.3 Potential hardware and software impacts

For this solution the USIM and the HSS software will need to be updated to implement the key change procedure and to implement the key indication procedure.

Optionally, a standardised interface between the OTA server and the HSS could be developed to manage the K/OPc or K/TOPc change and synchronisation of use between the HSS and the USIM.

#### 9.2.3.4 Key exchange protocols and transportation

In this solution, the keys are preinstalled on the USIM so there is no key exchange between the home network operator and the USIM.

The key exchange between the manufacturer and the home operator should be different that the normal provisioning message else this solution will have the same drawbacks as not using this solution.

#### 9.2.3.5 3GPP technologies supported

Where the AMF indication is used to indicate the K/Opc or K/TOPc to use, this solution is suitable for 3G, LTE and 5G.

Where USIM OTA is used to indicate the K/Opc or K/TOPc to use, this solution is suitable for GSM, 3G, LTE and 5G.

#### 9.2.3.6 Assessment of additional risks

There is still a storage and transport risk with solution. As all the keys are generated at production time, all of the keys will need to be stored somewhere and also transported from production to the home operator.

#### 9.2.3.7 Conclusion

This solution is completely in the home network operators control and can be used by all 3GPP technologies.

This solution, however, does not alleviate the transport risks or the risks associated with the key generation, as all of the keys used are pre-programmed into the USIM so both exist at a third party and need to be transported to the home operator.

The solution has the potential to be quite effective at meeting reactive requirements but less effective at pre-emptively changing the key.

Note: this solution overlaps heavily with solution #5.

## 9.3 Solution #3: Certificate based negotiation

### 9.3.1 Introduction

When certificates are introduced to both the tamper resistant hardware component which holds SIM/USIM and the network provisioning server which manages the tamper resistant hardware component remotely, a secure communication channel could be established between the UE and the network server based on mutual authentication via certificates. The solution is proposed to use this secure channel to update long term keys.

This solution uses the concept of profile as a representation of SIM/USIM and other data provisioned on the tamper resistant hardware component for the purpose of providing services.

### 9.3.2 Solution Description



Figure 9.3.2-1: Long term keys update based on certificate exchange and key negotiation

The overall flow is described below:

1. The UE and the Provisioning server perform mutual authentication based on certificates exchange and verification.
2. The UE and the Provisioning server negotiate common cryptographic suite for further communication, using mechanisms e.g. as specified by the GlobalPlatform Card Specification Amendment F [2].
3. The Provisioning system sends a Profile update request to the UE, including new long term keys to be provisioned, identity of the target Profile to be updated.
4. Upon reception of the Profile update request, the UE updates the target Profile using the new long term keys.
5. The UE sends a Profile update result containing the identity of the target profile to the Provisioning server.
6. The Provisioning server updates the long term keys of the target profile in the HSS.
7. The UE detaches from the network and re-attaches the network using the updated long term keys.

Note: It is not clear what entity is expected to operate this provisioning server.

### 9.3.3 Solution Evaluation

### 9.3.3.1 Key Issues

This solution meets the requirements for key issue 1. Although the solution description is vague about the low level transport for this protocol, it is possible to develop a HPLMN initiated session to implement this.

This solution meets key issue 2 by individual updates to each subscriber.

This solution meets the requirements for key issue 3 as the keys are not transported between 3rd parties unprotected.

### 9.3.3.2 USIM and ISIM types applicable

Although this solution can be used by any USIM and ISIM, because of the new certificates and the public key cryptography involved, it only applies to new USIMs that support this feature and could not be easily "retro-fitted" to existing USIMs and ISIMs.

### 9.3.3.3 Potential hardware and software impacts

The solution requires the USIM hardware to be preloaded with a certificate and that it supports certificate verification.

### 9.3.3.4 Key exchange protocols and transportation

SCP11a could be used as the key exchange protocol to establish keys to protect the long term keys, with necessary enhancement if needed.

The solution is not specific as to how this is transported between the USIM and the HPLMN.

Step 3 introduces a new key transport risk.

### 9.3.3.5 3GPP technologies supported

The solution could be used for all 3GPP technologies as long as the USIM hardware supports profile of the corresponding 3GPP technology.

### 9.3.3.6 Assessment of additional risks

It is not addressed in the present document whether this solution introduces a new long term key, i.e. private key of the certificate, which may have its own security risk.

This solution requires a global/regional PKI system. The implications of such global/regional PKI system is significant and is not addressed in the present document. The location of the root of trust is not addressed in the present document.

The solution may introduce new risk of the compromise of the Certificate Authority which issues certificates.

### 9.3.3.7 Conclusion

What risks this solution mitigates, and what risks remain, depend partly on what entity operates the provisioning server - which is not yet clear in the solution description. Subject to this point of uncertainty, this solution potentially meets all of the key issues, but it also introduces significant overheads (the creation of a PKI system to support this solution) and additional technical risks (compromise of the certificates used).

## 9.4 Solution #4: Diffe-Hellman based Key agreement

### 9.4.1 Introduction

This solution addresses key issue #1 and key issue #2.

It will be very difficult to achieve really robust security against an attacker who knows all of the algorithms and long term secret keys that a subscription is using. However, it is possible to make these attacks much harder in practice. A realistic objective is that an attacker, even if she knows the long term secret key and Authentication and Key Agreement algorithm (including any global constants) that a subscription is using, would have to carry out a long-term active man-in-the-middle attack in order to eavesdrop on that subscription.

### 9.4.2 Solution Description

### 9.4.2.1 Solution overview

NOTE 1: In this clause the terms "UICC" and the "HSS" are referred to. These should be understood as shorthand, referring respectively to the "device's UICC / secure element (or wherever the long term key is stored)" and the "HSS (or its Next Generation Systems equivalent)".

NOTE 2: In this clause, the GSM term "Ki" to refers to the long-term shared secret key stored in the UICC and the HSS – assuming that NextGen security remains largely based on such a shared secret key. The UMTS or LTE equivalent would be K. The terminology for NextGen is not yet decided.

Clause 7.1.1 lists a number of ways in which the original shared secret key might leak to an attacker. Many of the possible leakage points arise from the initial provisioning process. This solution involves a key exchange protocol being run between the UICC and the home network HSS, in order to create a newly agreed Ki value to replace the existing one. Elliptic Curve Diffie Hellman would be a suitable key exchange algorithm.

Exposing the HSS to update may in itself introduce new risks, and so should be handled with great care. One might consider running the key exchange protocol with a proxy for the HSS rather than with the HSS directly. However, the benefits of doing this are not entirely clear. Below, it is recommended that the update protocol take place over 3GPP-standardised signalling, rather than over the internet; and it is also recommended that the HSS, rather than the UICC, be the entity to trigger the update protocol. With these two points in mind, it is recommended for simplicity that the update protocol be carried out by the HSS directly, rather than by a proxy.

The key exchange protocol should be authenticated using the pre-existing shared secret, so that an attacker who does not already know the secret cannot act as man-in-the-middle at all. An attacker who does already know the secret may be able to act as man-in-the-middle during the key exchange protocol; however, a good protocol design can ensure that this attacker will have to remain as an active man-in-the-middle, essentially forever, in order to exploit that.

Using a key exchange protocol raises a risk that this protocol itself might be compromised over the lifetime of Next Generation Systems (perhaps using quantum computers), and allow newly-exchanged keys to be recovered by an attacker. One counter-measure is that where parties to the protocol already have a shared secret (e.g. the UICC and HSS already share Ki), then this existing shared secret should be fed into the new key derivation function, together with the output from the key exchange protocol. That way, an attacker would have to know the existing shared secret and compromise the key exchange to learn the newly derived secret. A suitable key derivation algorithm can use HMAC-SHA256, as defined in 3GPP TS 33.220 [13], as follows:

new Ki = KDF (key exchange protocol output, initial Ki)

where "key exchange protocol output" refers to the shared secret resulting from the key exchange protocol, and "initial Ki" refers to the Ki value that was shared between the UICC and the HSS before the protocol was run, and that was used to authenticate the key exchange.

There are two alternative ways to carry the key exchange protocol messages:

1. Over signalling messages. In this case, signalling messages will have to be defined to carry the protocol messages between UICC / secure element (or wherever the long term key is stored) and the home network HSS (or its Next Generation Systems equivalent), across core and (potentially roamed-to) radio network.

2. Over the user plane and the internet.

The recommended option is to carry the key exchange protocol messages over signalling messages. This is the safer option.

There are two alternative entities that could initiate the key exchange protocol:

1. The UICC.

2. The HSS.

To maintain operator control, and mitigate possible DoS risks, the recommended option is to have the HSS trigger the key exchange protocol. Either way, the key exchange protocol should be run, and the long term key replaced, at the earliest feasible opportunity after the subscription is activated. It is not necessary, though, to do this before any user traffic is allowed.

### 9.4.2.2 Notes on statefulness at the HSS

Using something like Elliptic Curve Diffie Hellman for key agreement might suggest that the HSS would need to maintain state during the key agreement session – whereas HSS/AuCs today are generally stateless, not running multi-pass communication sessions.

If this is a concern, then there are a number of ways to mitigate it:

1. It was already noted that it might be better to run the key exchange protocol with a proxy for the HSS, rather than with the HSS directly. In that case the proxy would be new, and there would be less reason to avoid it being stateful.

2. The "statefulness" could be managed by using the database that the HLR maintains with information for each subscription.

3. If the UICC sends the first message in the two-pass ECDH key exchange then it's the UICC, not the HSS, that needs to remember a secret ECDH parameter. (The HSS could still initiate the overall protocol by first sending a trigger message to the UICC.)

4. The HSS need not store its secret ECDH parameter at all, but instead can send it to the UICC – encrypted under an HSS public key, and signed under an HSS private key. The UICC then simply sends this back to the HSS in the return message. Neither the UICC nor any eavesdropper can read the secret parameter (because of the encryption), nor can they modify it without the HSS detecting that (because of the signature).

5. The above mechanism could work in reverse, with the UICC sending its secret ECDH parameter to the HSS encrypted and signed, and the HSS returning it.

### 9.4.2.3 Proposed message flow

Once the communications channel has been opened the following general message flow will allow the K/OPc to be updated securely:

HSS

USIM

1. Initiate LTKUP process (includes ECDH ephemeral public exponent)

2. Initial LTKUP response (includes ECDH ephemeral public exponent)

3. Calculate ECDH shared secret

4. Apply KDF to determine new K

3. Calculate ECDH shared secret

4. Apply KDF to determine new K

5. Run authentication procedure to verify the change of K

Figure 9.4.2.3-1: General DH message Flow

Steps:

1. Initiate LTKUP process - The LTKUP process is initiated by the HSS (transport methods are detailed below). This message includes ECDH ephemeral public exponent. This message, and subsequent messages in the handshake are integrity protected; the protection depends on the transport method applied.

2. Initial LTKUP response - The USIM responds with the ECDH ephemeral public exponent.

3. Both the USIM and HSS independently calculate ECDH shared secret.

4. Apply KDF to determine new K. This KDF should include the last K (and ideally a hash of any previous Ks combined) as an input.

5. Run authentication procedure to verify the change of K.

### 9.4.2.4 Transport over new Signalling protocol (Solution 4a)

In this option a new signalling protocol is designed between the HSS and the UE. This signalling protocol would be specific for this purpose and would follow the proposed message flow above.

As this is a new protocol there would be limited support or none for this signalling in GSM, UTRAN and possibly LTE. As the signalling is new, the home operator would not be able to rely on the visited network supporting this protocol so would not be able to depend on this being available while roaming.

### 9.4.2.5 Transport over USIM OTA protocol (Solution 4b)

In this option, the Diffe-Hellman exchange is transported by USIM OTA (3GPP TS 31.115 [5] and 3GPP TS 31.116 [14]). This solution, whilst it is likely to need new USIMs to implement it, would work over all existing 3GPP technologies and when roaming.

The HSS first communicates with the USIM OTA server to schedule the Initiate LTKUP process message. The HSS provides the ECDH ephemeral public exponent and may format the message as an APDU.

The OTA server schedules and sends the Initiate LTKUP process message as a secure USIM OTA message (see TS 31.115 [5]). This could be achieved either by SMS or BIP as described in TS 31.111 [15]. The USIM OTA security should be suitably strong and currently only AES with a key length equal or longer than the K being determined should be used. Integrity is used. Counters is used. Ciphering is optional. The APDU could be a new standardised APDU or an extension of the AUTHENTICATE APDU.

The USIM Initial LTKUP response is returned either in the USIM OTA PoR message or by a separate USIM OTA message. The USIM OTA security should be suitably strong and currently only AES with a key length equal or longer than the K being determined should be used. Other security requirements are as detailed above for the Initiate LTKUP process message.

Note: The K should not be changed until the response message has been acknowledged as sent, as the sending of the response may itself require authentication.

The next authentication will use the new K values (whether the counter is changed at this point is up to the HPLMN). The SIM may trigger this authentication by taking an authenticatable action such as sending a USSD string.

When using this option care should be taken not to transport the initial K with the OTA keys or to update the OTA keys after issue (there are many standardised ways to do this).

### 9.4.2.6 Transport over USSD protocol (Solution 4c)

It is possible for a new protocol to be designed that is delivered over USSD for this purpose. USSD is setup by the UE, can transport data messages of variable length and can keep a session live over many message exchanges.

As USSD strings originate from the UE, any solution based on USSD will need a means to trigger the USSD exchange.

As USSD messages are not secured, a security protocol will be needed to allow for integrity protection and replay attack resilience.

As the USSD data is not defined, a protocol for the LTKUP messages will need to be developed.

### 9.4.2.7 Transport over BEST protocol (Solution 4d)

The BEST protocol (TS 33.163 [16]) defines a secure protocol between the UE and the HPLMN. This protocol can be used between the HSE in the HPLMN and the USIM by using BIP as defined in TS 31.111 [15].

To initiate an LTKUP session a BEST session between the USIM and the HSE in the HPLMN will need to be setup by the USIM. This USIM could do this as a result of an OTA trigger message or by some other means.

The BEST protocol provides a secure channel with cyphering, integrity protection and replay protection. It is currently limited to 128-bit keys, so is currently not suitable for 256bit TOPc values.

For BEST, a protocol for the LTKUP messages will need to be developed.

### 9.4.2.8 Transport over AUTHENTICATION protocol (Solution 4e)

The LTKUP messages may be transported in special AUTHENTICATE commands.

To achieve this, the data from the HPLMN to the USIM is contained in the RAND and a bit indicating that this is an LTKUP message is in the AMF. For messages from the USIM to the HPLMN the data is sent in an AUTS||MACS as part of a dummy re-synchronisation request. This approach will allow 128 bits to be sent to the UE per authentication and 122 bits to be returned from the UE.

The AUTHENTICATE command provides integrity protection and replay protection, but not cyphering. The protocol for the LTKUP messages will need to be developed. This protocol will need to integrity protect messages from the USIM to the HPLMN.

Authenticate commands are only sent by the VPLMN, so determining when the LTKUP update will happen is difficult and currently the VPLMN may discard quintets so the messages may never be delivered.

### 9.4.3 Solution Evaluation

#### 9.4.3.1 Key Issues

An attacker who does not know the original Ki at the time that the key exchange protocol is run will not be able to carry out a man in the middle attack on it (because it is authenticated with the original Ki).

An attacker who does know the original Ki may be able to carry out an active man in the middle attack on the key exchange protocol. (This is likely to be easier if the protocol runs over the internet, harder if it runs over inter-operator signalling.) By doing this, the attacker can trick the HSS and UICC into thinking that they are sharing a new key, whereas in fact one key is shared between HSS and attacker, and another key between attacker and UICC.

What the attacker cannot do, though, is to trick the HSS and UICC into agreeing a new Ki that the attacker also knows. To exploit the man in the middle attack, therefore, the attacker will have to remain as an active man in the middle on all subsequent exchanges that use, or depend on, the new Ki value. This is a much harder attack in practice than the passive eavesdropping that an attacker who knows Ki can carry out today.

Clause 4 lists seven possible ways (labelled a – g) in which a long term secret key might leak to an attacker. This solution fully addresses points a, b and e, and reduces the exposure to points c, d and g. It does not address point f.

The recommended approach is to carry the key update protocol messages over signalling, rather than over the user plane and the internet. This requires less exposure of the HSS to possible malicious attack. Based on this recommended approach, it is also recommended that the key update protocol be carried out with the HSS directly, rather than in a proxy "in front of" the HSS. While a proxy would in some sense shield the HSS from attacks attempting to exploit the key update mechanism, it also complicates the picture, and the extent to which it would reduce risks in practice is not very clear. Another recommendation made for this solution, which is to have the HSS rather than the UICC trigger the key update protocol, also reduces the exposure of the HSS.

It's interesting to note that this mechanism could also address some concerns with embedded SIM. In the embedded SIM world, operators may have to accept UICC hardware and IMSI/Ki credentials from a much wider set of suppliers than before, with less confidence about their quality. Supplier accreditation schemes can give some reassurance here; and if "profile interoperability" is supported – allowing profiles from any subscription manager to work on any UICC hardware – then operators will be able to work with their favourite subscription managers irrespective of the UICC hardware manufacturer. But the Ki replacement mechanism described above gives another way to reduce risk: the operator can accept initial Ki's from vendors they may not entirely trust, but then replace those Ki's with new ones created directly between the AuC and the UICC, with no involvement from the subscription manager at all.

This solution can be used to update keys when they are known / suspected to have been compromised (key issues 1 and 2). It does not completely remove the ongoing risk from an exposed key, because the attacker could in principle use her knowledge of the old key to carry out a man in the middle attack on the establishment of the new key, but it makes it hard to exploit such an attack in practice, especially for eavesdropping attacks.

The solution can also be used pre-emptively, to reduce the risk of a key leaking. Compared to traditionally installed long term keys, or long term keys installed in an eUICC profile, a long term key established using this solution is exposed to fewer of the leakage vectors mentioned in clause 4.

The solution could apply to any type of USIM/ISIM (including eUICC), but requires new functionality both in the USIM/ISIM and in the HSS.

### 9.4.3.2 USIM and ISIM types applicable

This solution is suitable for all USIMs and ISIMs. This solution would also work with eSIMs.

### 9.4.3.3 Potential hardware and software impacts

This solution requires the USIM to support Diffie-Hellman based key agreement.

### 9.4.3.4 Key exchange protocols and transportation

Keys are agreed as a result of a DiffieHellman based key agreement. This solution proposes 4 possible transport mechanisms:

- Transport over new Signalling protocol (Solution 4a)

- Transport over USIM OTA protocol (Solution 4b)

- Transport over USSD protocol (Solution 4c)

- Transport over BEST protocol (Solution 4d)

### 9.4.3.5 3GPP technologies supported

The solution could be used for all 3GPP technologies as long as the USIM hardware supports profile of the corresponding 3GPP technology.

### 9.4.3.6 Assessment of additional risks

An attacker who does know the original Ki may be able to carry out an active man in the middle attack on the key exchange protocol. (This is likely to be easier if the protocol runs over the internet, harder if it runs over inter-operator signalling.) By doing this, the attacker can trick the HSS and UICC into thinking that they are sharing a new key, whereas in fact one key is shared between HSS and attacker, and another key between attacker and UICC.

What the attacker cannot do, though, is to trick the HSS and UICC into agreeing a new Ki that the attacker also knows. To exploit the man in the middle attack, therefore, the attacker will have to remain as an active man in the middle on all subsequent exchanges that use, or depend on, the new Ki value. This is a much harder attack in practice than the passive eavesdropping that an attacker who knows Ki can carry out today.

### 9.4.3.7 Conclusion

This solution meets the requirements for Key Issues 1, 2 and 3 can be used for all new USIMs from 2G to 5G. This solution can also be implemented on an eSIM.

This solution will impact the HSS both in terms of new interfaces and loading.

This solution does not mitigate a permanent man in the middle attack.

Within solution 4, option 4b has the least impact on current systems.

## 9.5 Solution #5: Multiple sets of parameters

### 9.5.1 Introduction

This solution aims to update the long term key K stored on a USIM application on UICC. The solution relies on the presence of several sets of parameters (K/OPc or K/TOPc) stored in the USIM. Only one set of parameters is active at a time in the USIM.

NOTE: the UICC application mentioned in this solution is the USIM. But the solution also applies to ISIM application and eSIM.

### 9.5.2 Solution Description

This solution consists of 4 phases:

1) In Personalisation Centre:

- For each UICC, several sets of parameters (K/OPc or K/TOPc) are generated and provisioned in a USIM. But, only one set is active at a time in this USIM.

- The output file sent to the network operator contains only one single set of parameters (K and eventually OPc or TOPc). This set of parameters is provisioned in the network operator backend. The other sets of parameters generated are kept in the personalisation centre using secured storage means.

2) In home network operator:

- When the network operator decides to update the long term key K of a given USIM within a UICC, the network operator asks the personalisation centre to deliver new output file containing a new set of parameters for a given USIM/UICC.

- The personalisation centre generates a new output file containing new set of parameters for this USIM. The set of parameters of the output file (containing K and eventually OPc or TOPc) corresponds to a set of parameters initially provisioned in the USIM (confer phase 1).

- After output file reception, the network operator launches an OTA [1] campaign targeting the corresponding USIM/UICC. The OTA campaign does not intend to immediately update the parameters in the USIM; the OTA campaign activates the replacement mechanism for the targeted USIM. The USIM/UICC is ready to proceed the change of parameters set, but waits for an event to do so. The change of key is not yet done.

- Once the UICC has been reached by the OTA campaign, the network operator can provision the received set of parameters in its backend using usual mechanism. Only one single set of parameters (K/OPc or K/TOPc) is active at a time in the HSS of the network operator for a given USIM.

- The network operator issues authentication vectors with the new set of parameters. Since the USIM has not yet replaced the set of parameters, the USIM will detect an authentication failure during the processing of AUTHENTICATE command with these authentication vectors. The authentication failure aims to trigger the replacement mechanism in the USIM/UICC.

3) In USIM/UICC:

- In case that the replacement mechanism has been activated in the targeted USIM by OTA, and that this USIM detects an authentication failure due to wrong key K, the USIM tries to perform the MAC verification of the AUTHENTICATE command with another set of parameters ((K/OPc or K/TOPc) already provisioned in the USIM. If the MAC verification matches, the set of parameters used becomes active and the authentication process can continue with these parameters. The USIM returns the results of the authentication successfully performed.

- After a successful change of set of parameters, the replacement mechanism is deactivated for this given USIM.

4) In home network operator:

- The operator knows the status of the key replacement procedure thanks to the result of the authentication procedure sent by the USIM.

- If the result of the authentication procedure sent by the USIM indicates an authentication failure, then the home operator can select another set of parameters and issue new authentication vectors generated using this new set of parameters, as defined in last step of phase 2). If the home operator selected a new key set, then phase 3 also takes place.

To improve the security of the solution, the use of additional key named "replacement mechanism protection key" is proposed to secure the OTA command sent to activate the replacement mechanism in the USIM.

Secured OTA command:

- The "replacement mechanism protection" key is provisioned in the UICC in the personalisation centre. This key will never exit the Personalisation Centre.

- When the network operators asks for the delivery of new set of parameters ((K and eventually OPc or TOPc), the UICC manufacturer computes the payload of the OTA command to be sent to the USIM/UICC. This OTA command is secured by the "replacement mechanism protection" key of the UICC.

- When receiving the OTA command, the UICC verifies the payload using the "replacement mechanism protection" key provisioned in the UICC. If the verification is not successful, the replacement mechanism remains inactive.

- A "failed payload check counter" may be implemented to increase the security level.

### 9.5.3 Solution Evaluation

#### 9.5.3.1 Key Issues

This solution does not mitigate a security due to the presence of an attacker at the personalisation centre where the set of parameters are generated and stored in the USIM.

For all the other security issues of Key Issues #1 and #2, an attacker having been able to retrieve the long term key K may be no longer present when the new set of parameters is sent or handled to replace the compromised set of parameters.

To mitigate Key Issue #2, the solution applies to each USIM/UICC of the batch of subscriptions.

This solution meets requirements for Key Issue#4. Once the operators has activated the key replacement mechanism in the USIM and triggered the replacement by issuing authentication vectors generated using the new set of parameters, the new set of parameters in the USIM becomes active only when there is successful MAC verification of the AUTHENTICATE command in the USIM. The operator knows the status of the key replacement procedure in the USIM thanks to the result of the authentication procedure it receives.

This solution meets requirements for Key Issue #5 since the operator is the originator of the key replacement mechanism. The home operator can decide when to perform a long term key update procedure. Based on security policy, the home operator can ask for new set of parameters from personalisation centre, then activate and trigger the key replacement in the USIM.

#### 9.5.3.2 UICC applications types applicable

This solution is applicable to all USIMs and ISIMs. This solution is also applicable to eSIMs but may not be the most efficient solution since also solution #1 applies to eSIM.

#### 9.5.3.3 Potential hardware and software impacts

USIM/UICC software will be updated to support the replacement mechanism. The solution does not require any additional hardware.

#### 9.5.3.4 Key exchange protocols and transportation

The longer term key K is not exchanged between the personalisation centre and the network operator.

The channel of communication used to exchange data between the personalisation centre and the home network may be changed.

#### 9.5.3.5 3GPP technologies supported

This solution is applicable to GSM, UMTS, LTE and 5G.

#### 9.5.3.6 Assessment of additional risks

If a HSM-based KMS (Key Management System) compliant to GSMA Security Assurance Scheme (SAS) is used at the personalization centre, then the long term keys and associated parameters, e.g. K/OPc or K/TOPc, are securely generated and stored at personalisation centre. If not, then the long term keys and associated parameters, e.g. K/OPc or K/TOPc may be compromised over time.

#### 9.5.3.7 Void

#### 9.5.3.8 Core and RAN networks impacts

This solution has impacts only on the HSS/AuC of the home network operator.

#### 9.5.3.9 Ease of implementation

This solution does not require significant changes to the current 3GPP specifications. Only additional OTA command is needed to implement the solution.

## 9.6 Solution #6: LTK generation

### 9.6.1 Introduction

This solution provides high-level description of a mechanism for LTK generation. This solution addresses the threat described in Key Issue # 3. This high-level description may be seen as generic framework for LTK generation replacing LTK transport, for example, for a Diffie-Hellman based solution for LTK generation.

### 9.6.2 Solution Description



Figure 9.6.2.1: LTK Generation Process

The high-level steps involved in the LTK generation process are described below:

Step 0: Operator makes a decision based either on the policy or detected LTK compromise to update LTK. Steps 1-8 describe the LTK Re-generation process.

Step 1: On detection of the compromise, or triggering of the LTK re-generation according to policy, the UE / eSIM and the AUSF / ARPF perform a mutual authentication and establish a secure connection.

NOTE 1: Mutual authentication between the UE / eSIM and the AUSF / ARPF may be performed by leveraging existing trust between SM-DP / SM-SR and MNO / AUSF / ARP e.g., using eSIM private key. Details of mutual authentication and key agreement between eSIM/UE and AUSF/ARPF/SM-DP are specified in GSMA SGP.02 [11] and GSMA SGP.01 [17].

Step 2: The UE / eSIM or the AUSF / ARPF notifies one another of the compromise (or of any other policy-based triggering of the LTK re-generation) over the secure connection established in Step 1.

Note 2: It is not detailed in the present document whether it should be possible for a LTK update to be triggered by the UE/eSIM, or whether only the home network should have the ability to do this.

Step 3: The notification from Step 2, triggers the LTK keying material generation on the eSIM associated with the compromised LTK and at the AUSF / ARPF.

Step 4: The UE / eSIM and the AUSF / ARPF exchange the keying material generated at Step 3.

Step 5: The UE / eSIM uses the keying material that it had generated together with the keying material received from the AUSF / ARPF to generate the LTK. Similarly, the AUSF / ARPF uses the keying material that it had generated together with the keying material received from the UE / eSIM to generate the fresh identical LTK.

Step 6: The UE / eSIM and the AUSF / ARPF exchange messages to provide Acknowledgement/proof-of-possession of the fresh LTK to each other.

Step 7: The UE / eSIM activates the fresh LTK for use with the particular MNO.

Step 8: The fresh LTK is activated and associated with the subscriber (USIM) within the ARPF (database) in a secure manner.

### 9.6.3 Solution Evaluation

#### 9.6.3.1 Key Issues

This solution while focussed on key issue 3 meets the requirements of Key Issues 1 and 2.

#### 9.6.3.2 USIM and ISIM types applicable

This solution requires the use of eSIM.

#### 9.6.3.3 Potential hardware and software impacts

The solution requires the USIM hardware to be preloaded with a certificate and that it supports certificate verification.

Note: The solution description does not clearly specify this.

#### 9.6.3.4 Key exchange protocols and transportation

No keys are exchanged in this solution however material used to generate the key is exchanged. Capture of this key material is not adequate for an attacker to generate the keys. This assumes that a suitable key exchange protocol, such as (Elliptic Curve) Diffie Hellman, is used in steps 4-5.

#### 9.6.3.5 3GPP technologies supported

This solution could be used on UMTS, LTE or 5G where a eSIM is used.

#### 9.6.3.6 Assessment of additional risks

The quality of the key material will affect the efficacy of the protocol.

The SIMAlliance specification for eSIM profile package describes an interoperable profile format transmitted to the eSIM to be loaded and installed in compliance with GSMA eSIM remote provisioning procedures.

Current SIMAlliance specification for eSIM defines the MNO profile as the complete collection of parameters (file structure, data and applications: USIM, etc.). The profile format definition does not address packaging of specific individual profile elements (e.g., LTK).

The following threats may manifest themselves due to the lack of ability for selective LTK update.

As this solution may change the whole USIM profile there is a possible loss of application-specific credentials and/or user data stored in the eSIM.

Possible denial-of-service to third party services from eSIM hosted third party applications.

#### 9.6.3.7 Conclusion

This solution needs more detail.

# 10 Conclusions

Based on the solutions and evaluations in the present document, no normative specifications are required in 3GPP.

It is recommended that solutions 4b and 5 be detailed in a 900 series 3GPP TR.

Annex A:
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2017-06 | SA3 #88 | S3-171749 | - | - | - | First Draft – Skeleton Document | 0.1.0 |
| 2017-06 | SA3 #88 | S3-172159 | - | - | - | updated with S3-172160, S3-172161, S3-172162 and S3-172163 | 0.2.0 |
| 2017-12 | SA3 #89 | S3-173504 | - | - | - | Updated with S3-173500, S3-173501, S3-173502, S3-173252 and S3-173503 | 0.3.0 |
| 2018-03 | SA3#90bis | S3-180931 | - | - | - | Updated with S3-180932, S3-180933, S3-180934, S3-180935, S3-180843 and S3-181007 | 0.4.0 |
| 2018-04 | SA3#91 | S3-181521 | - | - | - | Updated with S3-181523, S3-181525, S3-181527, S3-181528, S3-181530, S3-181531, S3-181532, S3-181534, S3-181526 and S3-181535 | 0.5.0 |
| 2018-05 | SA3#91bis | S3-182058 | - | - | - | Updated with S3-181884 and S3-181886 | 0.6.0 |
| 2018-08 | SA3#92 | S3-182702 | - | - | - | Updated with S3-182696 | 0.7.0 |
| 2018-09 | SA3#92bis | S3-183153 | - | - | - | Updated with S3-183152 | 0.8.0 |
| 2018-11 | SA3#93 | S3-183753 | - | - | - | Updated with S3‑183752 and editorial changes | 0.9.0 |
| 2018-12 | SA#82 | SP-181033 |  |  |  | EditHelp/MCC review. Presented for approval | 1.0.0 |
| 2018-12 | SA#82 |  |  |  |  | Upgrade to change control version | 16.0.0 |
| 2019-03 | SA#83 | SP-190099 | 0001 | - | D | Editorial changes suggested by edithelp | 16.1.0 |