ETSI TR 133 935 V18.0.0 (2024-04)

TECHNICAL REPORT

LTE;
5G;
Study on detailed Long Term Key Update Process (LTKUP) detailed solutions
(3GPP TR 33.935 version 18.0.0 Release 18)

Reference
RTR/TSGS-0333935vi00

Keywords
5G,LTE,SECURITY

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

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

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

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.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

1 Scope

The present document describes LTKUP solution 4b and LTKUP solution 5 from 3GPP TR 33.834 [2] in implementable detail.

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] 3GPP TR 33.834: "Security Aspects; Study on Long Term Key Update Procedures (LTKUP)".

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

[4] 3GPP TS 31.116: "Remote APDU Structure for (U)SIM Toolkit applications".

[5] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 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 TR 21.905 [1].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

LTKUP Long Term Key Update Procedure

4 LTKUP solutions

4.1 Overview

TR 33.834 [2] recommends the production of detailed implementation for:

- Solution 4b - Diffe-Hellman based key agreement over SIM OTA
- Solution 5 - multiple sets of parameters on the USIM

Both solutions meet all of the key issues identified in TR 33.834 [2]:

- Key Issue 1: individual subscription - K exposed
- Key Issue 2: batch of subscriptions - K exposed
- Key Issue 3: LTK Derivation vs. LTK Transport
- Key Issue 4: Loss of synchronisation of long term keys
- Key Issue 5: undetected leakage of K

Both solutions can be implemented in GSM, UMTS, LTE and 5G and both require SIM/USIM changes and Home network HSS/AuC/UDM changes.

4.2 Solution 4b - Diffe-Hellman based Key agreement over SIM OTA

4.2.1 Solution overview

This solution involves a key exchange protocol being run between the USIM/ISIM and the home network HSS, in order to create a newly agreed Ki value to replace the existing one. This key agreement protocol is transported over USIM OTA (TS 31.115 [3] and TS 31.116 [4]).

4.2.2 Architecture overview

The Architecture consists of a HSS / UDM, and OTA server and the USIM/UICC.

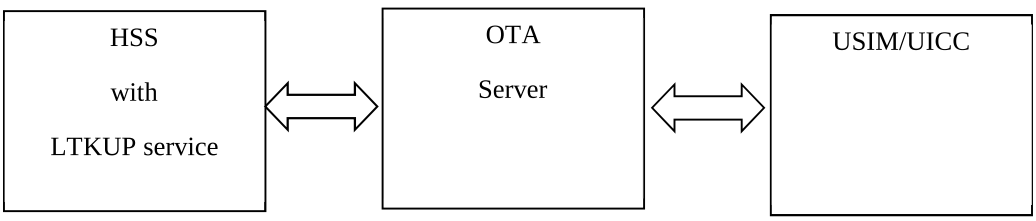

Figure 4.2.2-1

The HSS to OTA interface is proprietary.

The OTA server interface to the USIM/UICC is as specified in TS 31.115 [3] and TS 31.116 [4].

4.2.3 Implementation recommendations

Elliptic Curve Diffie Hellman is recommended as a suitable key exchange algorithm.

Exposing the HSS to update introduces risks, and so should be handled with great care. It is possible to run the key exchange protocol with a proxy for the HSS rather than with the HSS directly.

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 USIM/ISIM, 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.

In this solution, the key exchange protocol is 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 is 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 USIM/ISIM and HSS already share Ki), then this existing shared secret is 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 TS 33.220 [5], 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 USIM/ISIM and the HSS before the protocol was run, and that was used to authenticate the key exchange.

4.2.4 Example implementation

4.2.4.1 OTA Transport

The LTKUP messages are securely transported to and from the USIM using APDUs within SIM OTA messages (see TS 31.115 [3]).

The APDUs are FFS.

4.2.4.2 LTKUP Message Flow

The LTKUP service is delivered using a Diffie-Hellman key agreement process as follows:

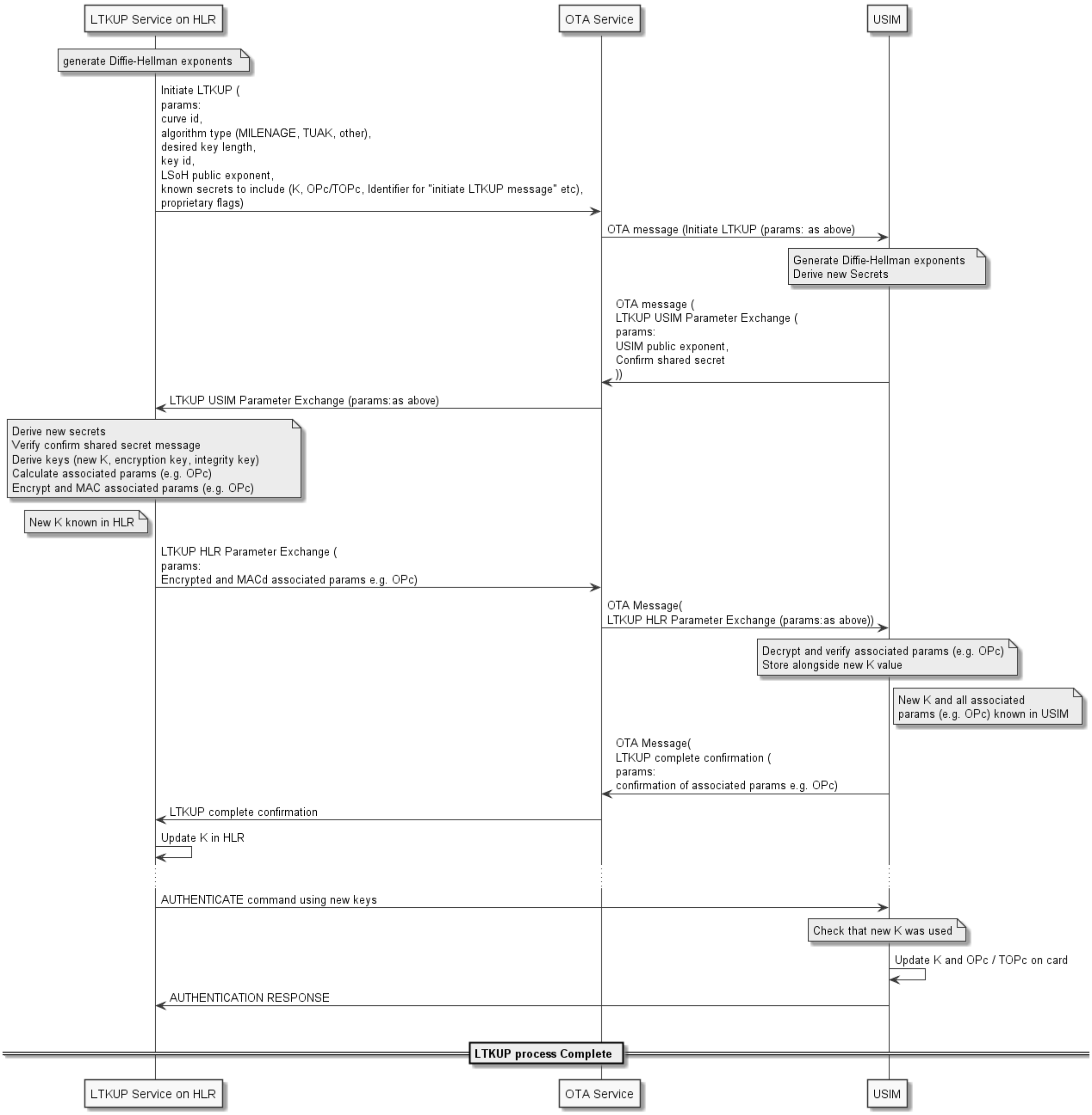

Figure 4.2.4.2-1: LTKUP key agreement process diagram

Initiate LTKUP

parameters:

curve/ECIES profile id:

- Length: 1
- Values: 0 - 5 + proprietary/reserved

algorithm type:

- Length: 1

- Values: MILENAGE, TUAK, other

desired key length:

- Length: 1
- Values: 16, 32

key id:

- Length: 1
- Values: 0 - 127

LSoH public exponent:

- Length: 32, 48 (or 64)
- Values: Random

known secrets to include:

- Length: 4
- Values: Identifiers for K, OPc/TOPc, "initiate LTKUP message", others

proprietary flags:

- Length: Any
- Values: Any

LTKUP USIM Parameter Exchange

parameters:

USIM public exponent

- Length: 32, 48 (or 64)
- Values:Random

Confirm shared secret

- Length: 8
- Values: Random

LTKUP HLR Parameter Exchange

parameters:

Encrypted Associated Params

- Length: 16 for OPc, 32 for TOPc, Any for Other
- Values: Random

MAC-tag for Encrypted Associated Params

- Length: 8
- Values: Random

LTKUP Complete Confirmation

parameters:

Confirm Associated Params

- Length: 8
- Values:Random

The "confirm" messages from the USIM are best done by MACing all the parameters to be confirmed, using an integrity key derived from the shared secret. TBC: whether it is acceptable to use the same integrity key that was already derived for use in the "HLR Parameter Exchange" message (with some additional flags like a message id included as part of the data to be MACed), or whether it is better to derive an additional key just for the USIM confirmation.

4.3 Solution 5 - Multiple sets of parameters on the USIM

4.3.1 Solution Overview

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.

The decision to launch the procedure to replace the long term key K in the USIM is taken by the home network operator.

4.3.2 Solution description

4.3.2.0 Overview

The solution requires steps when the UICC is in the personalisation centre and then when the UICC is in the field.

4.3.2.1 UICC 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 of parameters is active at a time in this USIM.

The personalisation centre sends to the network operator an output file, which 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 may be retrieved on demand from the personalisation centre.

The OTA command sent to the USIM/UICC is secured thanks to secured packet mechanism specified in TS 31.115 [3]. Optionally, a shared key called "replacement mechanism protection" key is provisioned in the UICC in order to protect in integrity the payload of the OTA command. This "replacement mechanism protection" key offers an additional level of security due to the sensitivity of the procedure. This "replacement mechanism protection" key, if present, is securely stored in the personalisation centre and never exits the personalisation center.

4.3.2.2 UICC in the field

Once the UICC is in a User Equipment in the field, the network operator can launch when he wants the replacement procedure as follows:

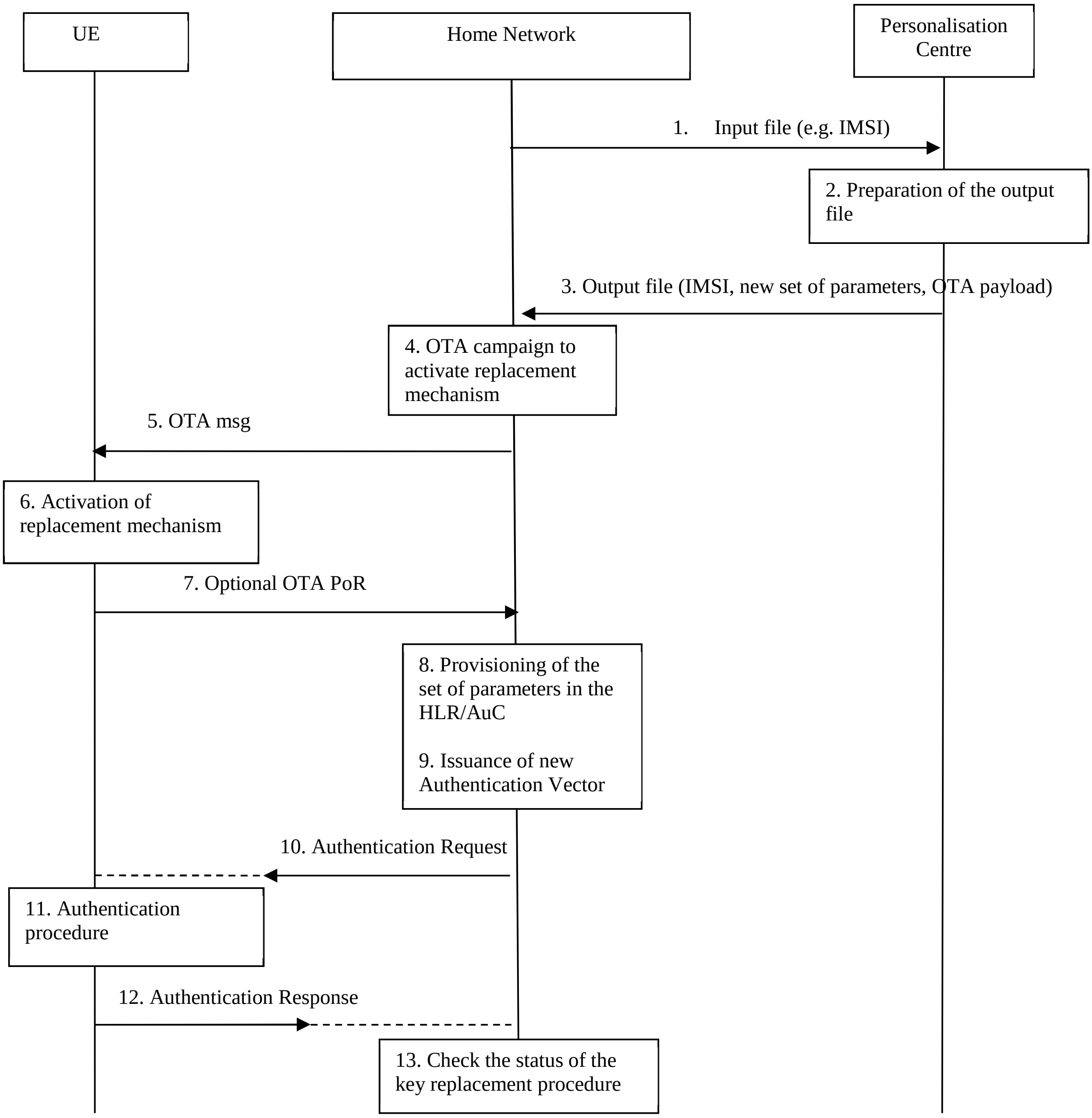

Figure 4.3.2.2-1: Key replacement procedure

The procedure to replace the long term key K works as follows:

1) When the network operator decides to update the long term key K of a given USIM within a UICC, the network operator sends an input file requesting the personalisation centre to deliver an output file containing a new set of parameters for a given USIM/UICC. The input file contains at least an identifier enabling the personalisation centre to retrieve new set of parameters (e.g. IMSI or ICCID).

2. The personalisation centre generates a new output file. This new output file contains the IMSI, a new set of parameters for this USIM (K and eventually OPc or TOPC), and the OTA payload that the network operator will have to send to the USIM. The OTA payload contains the request to activate the replacement mechanism, and an index identifying the corresponding set of parameters provisioned in the USIM.

   Optionally, in case that the "replacement mechanism protection" key was generated and stored in the personalisation centre, the personalisation centre protects the OTA payload in integrity.

3. The personalisation centre sends securely the output file to the network operator.

4. At reception of the output file, the network operator launches an OTA campaign targeting the corresponding USIM/UICC. The OTA campaign does not intend to immediately update the parameters in the USIM; the OTA campaign only activates the replacement mechanism for the targeted USIM.

5. The network operator sends to the USIM/UICC the OTA command activating the replacement mechanism in the USIM and providing the index of the new set of parameters.

6. The USIM/UICC in the UE receives the OTA command activating the replacement mechanism.

   If the USIM is provisioned with the "replacement mechanism protection" key, then the USIM verifies the protection in integrity of the OTA payload. The replacement mechanism remains inactive if the if the OTA payload verification is unsuccessful.

   If the OTA playload is not protected in integrity or if the OTA payload verification is successful, then the USIM activates the replacement mechanism and stores the index of the corresponding set of parameters.

   Once the replacement mechanism is active, the USIM 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.

7. The USIM sends OTA Proof of Receipt to the network operator, if requested by the operator in step 4.

8. The network operator provisions the received set of parameters (K and eventually OPc or TOPC) in the backend using usual mechanism. Only one single set of parameters (K and eventually OPc or TOPc) is active at a time in the network operator for a given USIM.

9. The network operator issues an authentication vector with the new set of parameters.

NOTE: 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 this authentication vector. The authentication failure aims to trigger the replacement mechanism in the USIM/UICC.

10. The network operator sends an authentication procedure request.

11. The USIM receives an AUTHENTICATE command and performs the authentication procedure. If the USIM detects an authentication failure due to wrong key K and if the replacement mechanism has been activated in the USIM, then the USIM tries to perform the MAC verification of the AUTHENTICATE command with the new set of parameters (K/OPc or K/TOPc) provisioned identified by the index received in step 6.

    If the MAC verification with the new set of parameters is successful, then:

    - the new set of parameters becomes active and the previous set of parameters may be deleted,

    - the USIM continues the authentication procedure with the new set of parameters, and

    - the USIM deactivates the replacement mechanism.

    Otherwise:

    - the USIM increments a retry counter associated to the replacement mechanism,

    - the USIM deactivates the replacement mechanism if the retry counter has reached its maximum value, and

    - the USIM abandons the authentication procedure with MAC failure error.

12. The UE sends the results of the authentication procedure.

13. The network operator knows the status of the key replacement procedure thanks to the results of the authentication procedure sent by the USIM. If the result of the authentication procedure sent by the USIM indicates a MAC failure, then the network operator knows that the replacement mechanism failed.

If the replacement mechanism failed, the network operator can decide to perform a new replacement procedure starting from step 9, or to perform a full procedure starting from step 1, or to restore the existing set of parameters active in the USIM.

Annex A: Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2019-03	SA3#94AH	S3-190956	-	-	-	First Draft includes: S3-191024, S3-190953, S3-190954 and S3-190955.	0.1.0
2019-11	SA3#97	S3-194634	-	-	-	Updated with S3-193988	0.2.0
2020-05	SA3#99e	S3-201451	-	-	-	Added S3-201311	0.3.0
2020-06	SA#88-e	SP-200378				Edithelp review Presented for information and approval	1.0.0
2020-07	SA#88-e					Upgrade to change control version	16.0.0
2022-03	-	-	-	-	-	Update to Rel-17 version (MCC)	**17.0.0**
2024-03	-	-	-	-	-	Update to Rel-18 version (MCC)	**18.0.0**

History

Document history		
V18.0.0	April 2024	Publication