**3GPP TSG-SA3 Meeting #103-e *draft\_S3-211531-r1***

**e-meeting, 17 - 28 May 2021** Revision of S3-20xxxx

**Source: Vodafone**

**Title: pCR to TR 33.845 - Editorial updates**

**Document for: Approval**

**Agenda Item: 5.6**

# 1 Decision/action requested

***Approve the pCR***

# 2 References

[1] 3GPP TS 33.845 version 1.0.0 : "Study on storage and transport of 5G Core (5GC) security parameters for Authentication Credential Repository Processing Function (ARPF) authentication"

# 3 Rationale

*TR 33.845 is to be sent for approval. This pCR corrects editorial issues such as formatting, spaces and consistency.*

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* First Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 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.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of First Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Second Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 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 TS 33.501: "Security Architecture and Procedures for 5G System".

[3] 3GPP TS 35.205: "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".

[4] 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 ".

[5] 3GPP TS 23.632: "User Data Interworking, Coexistence and Migration".

[6] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[7] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

[8] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[9] 3GPP TS 33.220: "3G security; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[10] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2"

[11] 3GPP TS 29.505: "5G System; Usage of the Unified Data Repository services for Subscription Data".

[12] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture".

[13] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2"

[14] 3GPP TS 33.102: "Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture".

# 3 Definitions of terms and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1], 3GPP TS 33.501 [2], 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], or 3GPP TS 33.501 [2].

**Subscription data**: data required by UDM/ARPF for supporting authentication, access and mobility, session management and other procedures within the 5GC. Subscription data can be stored in and retrieved from UDR over Nudr as defined in 3GPP TS 29.505 [11].

**Authentication subscription data**: part of the subscription data supporting authentication.

**DOS attack**: Denial of service attack where a service is unavailable due to too many requests to use the service.

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1], 3GPP TS 33.501 [2], 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] and 3GPP TS 33.501 [2].

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of second Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Third Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 4.2.1 Model #A: Security parameters stored only in the ARPF

Model #A is the model where security parameters for the execution of primary authentication are stored only at the ARPF. This model corresponds to a fully stateful ARPF deployment model where UDR is not used for securing security parameters.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of third Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Fourth Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 4.2.3 Model #C: Security parameters stored both in the ARPF and the UDR

Model #C is the model where the security parameters for the execution of primary authentication common across subscribers within a PLMN are stored in the ARPF and the security parameters specific to individual subscribers are stored in the UDR. This model corresponds to a stateless ARPF deployment model where UDR is used for storing subscriber specific security parameters.

NOTE: Security parameters common across subscribers are, e.g., OP value – if Milenage is used, TOP value – if TUAK is used. Security parameters specific to individual subscribers are, e.g., long term key, SQN, OPc value – if Milenage is used, TOPc – if TUAK is used.

## 4.3 Primary Authentication

3GPP TS 33.501 [2] defines primary authentication to enable mutual authentication between the UE and the network. It uses the pre-shared long-term Key which is bind to a unique SUPI to authenticate each other. The long-term Key is stored in the USIM and the ARPF of home network separately. The ARPF shall process the K only in its secure environment, the ARPF is a service offered by UDM.

Two methods including EAP-AKA' and 5G-AKA are defined for primary authentication, which method is used for mutual authentication is determined by the ARPF/UDM. The authentication methods are stored in the ARPF. The other security parameters (e.g. SQN, AMF) in addition to the K required for the primary authentication are also held by the ARPF.

During the registration procedure, the AMF determines to trigger the primary authentication on–demand for the UE. If the primary authentication is required, the AMF requests it from the AUSF. Upon request from the AMF, the AUSF shall execute authentication of the UE. In the primary authentication procedure, the ARPF is required for key storage, authentication methods storage, and key derivation.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of fourth Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Fifth Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 5.1 Overview

Authentication subscription data is data that:

- is needed for the generation of authentication vectors in the UDM/ARPF (as described in 3GPP TS 33.501 [2]); and

- is stored in the 5G core network.

NOTE 1: Other data related to authentication, but that does not need to be stored in the 5G core network is not authentication subscription data.

For AKA-based authentication, the authentication subscription data consists of:

- the long term key K;

- the sequence number SQN;

- (optionally) the authentication management field AMF;

NOTE 2: it is an operator policy whether the authentication management field AMF is stored or generated; therefore it is optionally included in the set of authentication subscription data.

- additional parameters depending on the authentication algorithm used (e.g. OP or OPc if MILENAGE (cf. 3GPP TS 35.205 [3]) is used, TOP or TOPc if TUAK (cf. 3GPP TS 35.231 [4]) is used, other parameters for proprietary algorithms);

- the authentication method used;

- the authentication algorithm used (e.g. MILENAGE, TUAK, proprietary algorithm).

Authentication subscription data may be specific per SUPI (e.g. long term key K, sequence number SQN, MILENAGE parameter OPc, TUAK parameter TOPc), or it may be generic (e.g. MILENAGE parameter OP, TUAK parameter TOP).

TS 29.505 [11] specifies the usage of the Unified Data Repository, Nudr, services for subscription data. This specification provides the resource definition and data model for subscription data used over the Nudr Service Based Interface.

When it comes to the definition of resources related to subscription authentication material, TS 29.505 [11] defines the *AuthenticationSubscription* data type supporting primary authentication as follows:

NOTE 3: The term 'authentication subscripion data' as used in this document does not correspond exactly to the use of the term *AuthenticationSubscription* data as used in TS 29.505 [11].

Table 4.2.3-1: TS 29.505 [11], Table 5.4.2.2-1: Definition of type AuthenticationSubscription

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Attribute name* | *Data type* | *P* | *Cardinality* | *Description* |
| *authenticationMethod* | *AuthMethod* | *M* | *1* | *String containing the Authentication Method ("5G\_AKA" , "EAP\_AKA\_PRIME, "EAP\_TLS"...)."* |
| *encPermanentKey* | *string* | *C* | *0..1* | *The encrypted value (hexstring) of the permanent authentication key (K) (see 3GPP TS 33.501 [9]).**It shall be present if the authentication method is "5G\_AKA" or "EAP\_AKA\_PRIME".* |
| *protectionParameterId* | *string* | *C* | *0..1* | *Identifies a parameter set securely stored in the UDM(ARPF) that can be used to decrypt the encPermanentKey (and encOpcKey or encTopcKey if present). Values and their meaning are HPLMN-operator specific.**It shall be present if the authentication method is "5G\_AKA" or "EAP\_AKA\_PRIME".* |
| *sequenceNumber* | *SequenceNumber* | *C* | *0..1* | *String containing the SQN as defined in 3GPP TS 33.102 [14].**It shall be present if the authentication method is "5G\_AKA" or "EAP\_AKA\_PRIME".* |
| *authenticationManagementField* | *string* | *C* | *0..1* | *Hexstring containing the Authentication management field as defined in 3GPP TS 33.501 [9].**It shall be present if the authentication method is "5G\_AKA" or "EAP\_AKA\_PRIME".**Pattern: '^[A-Fa-f0-9]{4}$'* |
| *algorithmId* | *string* | *C* | *0..1* | *Identifies a parameter set securely stored in the UDM(ARPF) that provides details on the algorithm and parameters used to generate authentication vectors. Values and their meaning are HPLMN-operator specific.**It shall be present if the authentication method is "5G\_AKA" or "EAP\_AKA\_PRIME".* |
| *encOpcKey* | *string* | *O* | *0..1* | *Hexstring of the encrypted OPC Key.**Presence indicates that the provided value (decrypted) shall be used instead of the value derived from OP and K.* |
| *encTopcKey* | *string* | *O* | *0..1* | *Hexstring of the encrypted TOPC Key.**Presence indicates that the provided value (decrypted) shall be used instead of the value derived from TOP and K.* |

As shown, the *AuthenticationSubscription* data type includes only the security parameters defined at individual subscriber’s basis required for the execution of AKA such as:

- Long term Key(s), including *encPermanentKey* and optionally *encOpcKey/encTopcKey*.

- Sequence Number, SQN (*sequenceNumber*).

- Authentication Management Field, AMF (*authenticationManagementField*).

- The identifier of the authentication algorithm (*algorithmId*).

The *algorithmId* attribute does not contain all the related information but it rather contains a string which refers to a parameter set securely stored in the UDM/ARPF. The *algorithmId* attribute identifies the authentication algorithm as well as other related parameters associated to the authentication algorithm which do not need to be specific for individual subscriber’s (e.g. settings for the constants *c* and/or *r* for MILENAGE) are referred to in the *AuthenticationSubscription* data resource by the *algorithmId* attribute.

## 5.2 Milenage AKA authentication

To enable Milenage authentication algorithm, the following parameters are needed:

- OP (the operator variant algorithm configuration field);

- OPc (value derived from OP and K);

- c1,c2,c3,c4,c5 (value XORed onto intermediate variables);

- r1,r2,r3,r4,r5 (value used to define amounts by which intermediate variables are cyclically rotated);

## 5.3 TUAK AKA authentication

To enable TUKA authentication algorithm, the following parameters are needed:

- TOP (the operator variant algorithm configuration field);

- TOPc (value derived from TOP and K);

- ALGONAME (value specified as the ASCII representation of the string "TUAK1.0");

- the length of K (K is a 128-bit or 256-bit subscriber key that is an input to the functions *f1*, *f1\**, *f2*, *f3*, *f4*, *f5* and *f5\**);

- the length of MAC-A (MAC-A is a 64-bit, 128-bit or 256-bit network authentication code that is the output of the function *f1*);

- the length of MAC-S (MAC-S is a 64-bit, 128-bit or 256-bit resynchronization authentication code that is the output of the function *f1\**);

- the length of RES (RES is a 32-bit, 64-bit, 128-bit or 256-bit signed response that is the output of the function *f2*);

- the length of CK (CK is a 128-bit or 256-bit confidentiality key that is the output of the function *f3*);

- the length of IK (IK is a 128-bit or 256-bit integrity key that is the output of the function *f4*);

## 5.4 EAP methods for authentication

This document covers the AKA based authentication mechanisms. Thus EAP-AKA’ is covered by this document.

## 5.5 Proprietary authentication algorithms

The definition of the *AuthenticationSubscription* data type allows for the use of proprietary authentication algorithms and SQN schemes. These proprietary authentication algorithms may use additional parameters from the ones currently stored in UDR as defined in TS 29.505 [11]. The API extensibility mechanisms defined in TS 29.500 [12] for any JSON object of any API can be used to store these additional parameters in UDR if needed.

The analysis of additional parameters required by proprietary authentication algorithms is out of scope of this document.

## 5.6 AMF related parameters

To enable AKA-based authentication, the following AMF related parameters are needed: SUCI or SUPI;

The serving network name;

## 5.7 Counter related parameters

To enable AKA-based authentication, the following counter related parameters are needed:

- sqnScheme (scheme for generation of Sequence Numbers);

- sqn (value containing the SEQ part of SQN, and the IND part which is filled with 0's. When the sqnScheme is "TIME\_BASED", the SEQ part is the DIF value.);

- lastIndexes (a map of integer values map(integer), where the integer is the last used value of IND);

- indLength (number of bits of the IND part of SQN);

# 6. Key Issues

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of fifth Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* sixth Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 7.1.1 Introduction

This solution addresses key issue #1 on "Separation of authentication subscription data from subscription data".

The solution proposes the use of a UDR dedicated for subscription data and further isolation of the authentication data within this UDR based on internal implementation techniques.

This solution is based on capabilities defined or planned to already to be defined in 3GPP TSs and does not require any additional specification work.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of sixth Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* seventh Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 7.2.1 Introduction

This solution addresses key issue #2 on "protection of long-term key during storage in UDR ".

The solution describes how the long-term key in the UDR can be protected against modification by any network function and retrieval by unauthorized network elements over Nudr using the OAuth 2.0 based authorization framework defined in 3GPP TS 33.501 [2] in Release 16.

This solution is based on capabilities defined or planned to already to be defined in 3GPP TSs and does not require any additional specification work.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of seventh Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* eighth Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 7.3.1 Introduction

This solution addresses key issue #3 on "protection of long-term key during transfer out of UDR".

The solution is based on storing the long-term key encrypted in UDR and transferring it also encrypted over Nudr. As any other SBA reference point, Nudr is additionally protected using TLS as defined in 3GPP TS 33.501 [2].

This solution is based on capabilities defined or planned to already to be defined in 3GPP TSs and does not require any additional specification work.

### 7.3.2 Solution details

The OAuth 2.0 based authorization framework defined in 3GPP 33.501 [2] is being enhanced in Release 16 to allows the possibility to generate OAuth 2.0 tokens to retrieve *AuthenticationSubscription* data ONLY to UDM/ARPF NF type of service consumers.

This solution proposes that the protection of the long-term key while provided to the UDM/ARPF over Nudr is two-fold:

- In the first place, the long-term key is provisioned and stored in UDR in encrypted form. This solution does not cover actual mechanisms to perform such encryption (e.g. encryption algorithms, key length, etc …).

- Secondly, as any other SBA reference point, the Nudr is protected using TLS as defined in 3GPP TS 33.501 [2].

These two protection levels make impossible for any intermediate actor to eavesdrop or modify the long-term key while in transit over Nudr.

### 7.3.3 Evaluation

This solution addresses the requirements of the KI by protecting the transfer of the long-term key between the UDR and the UDM/ARPF in three ways:

- transporting the long-term key in encrypted form during its transfer from UDR to UDM/APRF, and

- additionally, protecting the transfer of the long-term key over Nudr based on secure encrypted transport mechanisms (such as HTTPS).

- the OAuth tokens allow for the long-term key to only be retrieved by the UDM/ARPF

This solution requires that the UDM/ARPF stores the decryption key. The storage of the decryption key at the UDM/ARPF is subject to the same security requirements as if the ARPF would store the long-term keys. That is, the decryption key is required to be protected from physical attacks and never leave the secure environment of the UDM/ARPF unprotected. This required security of the decryption key can be achieved as it is done in pre-5G networks (e.g. by using a Hardware Security Module in the UDM/ARPF). It may be desirable to export a protected copy of the decryption key to a backup location, to aid recovery if necessary.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of eighth Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* nineth Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 7.6.1 Introduction

This solution addresses key issue #2, "protection of long-term key during storage in UDR ".

The solution trusts the access tokens created using the OAuth 2.0 based authorization framework to protect the long-term key from retrieval by unauthorised NFs, and that modification of the long-term key is restricted to the *sequenceNumber* attribute.

This solution is based on capabilities defined or planned to be defined in 3GPP and does not require any additional specification work.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of ninth Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* tenth Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 7.7.1 Introduction

This solution addresses key issue #3, "protection of long-term key during transfer out of UDR ".

The solution trusts the access tokens created using the OAuth 2.0 based authorization framework to protect the long-term key from retrieval by unauthorised NFs and to ensure it is only transported along the Nudr interface, the TLS protection on the Nudr interface, and that modification of the long-term key is restricted to the *sequenceNumber* attribute.

This solution is based on capabilities defined or planned to already to be defined in 3GPP and does not require any additional specification work.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of tenth Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* eleventh Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 7.14.1 Introduction

This solution addresses key issue #9, "protection of sequence number SQNHE during transfer out of UDR".

The solution trusts the access tokens created using the OAuth 2.0 based authorization framework to protect SQNHE from retrieval by unauthorised NFs and to ensure it is only transported along the Nudr interface, along with the TLS protection on the Nudr interface.

This solution is based on capabilities defined or planned to be defined in 3GPP TSs and does not require any additional specification work.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of eleventh Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Twelfth Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 8 Conclusions

Editor's Note: it may be needed to update the conclusions depending on the completion of this study.

The conclusions of the study are the following:

1. With respect to ARPF deployment, Model #A and Model #C as defined in clause 4.2 of this document need to be supported by normative text in 3GPP specifications. It is not expected that Model #B will be supported by normative text in 3GPP specifications.

2. Regarding the separation of authentication subscription data from other subscription data (Key Issue #1), it is concluded that there is no need for new normative text (according to the evaluation of Solution #1).

3. Regarding the protection of the long-term key, Milenage OPc values, and TUAK TOPc values during storage in UDR (Key Issues #2, #4, #10), it is concluded to add normative text based on Solution #4 (for long-term key), Solution #10 (for OPc), and Solution #13 (for TOPc)

4. Regarding the protection of the SQNHE during storage in UDR (Key Issue #8), it is concluded that there is no need for new normative text (according to the evaluation of Solution #12).

5. Regarding the protection of the long-term key, Milenage OPc values, and TUAK TOPc valuesduring transfer between UDR and UDM/ARPF (Key Issues #3, #5, and #11), it is concluded to add normative text based on Solution #5 (for long-term key), Solution #8 (for OPc), and Solution #15 (for TOPc).

6. Regarding the protection of the SQNHE during transfer between UDR and UDM/ARPF (Key Issue #9), it is concluded that there is no need for new normative text (according to the evaluation of Solution #9).

7. Regarding the protection of the Milenage OP value during storage in UDR and during transfer between UDR and UDM/ARPF, the conclusion is there is no need for new normative text, since ARPF deployment Model #B is not expected to be supported by normative text in 3GPP specifications. However, if operators/vendors want to store the OP value in, or transfer the OP value out of, the UDR, thenit is recommended to be done in encrypted form according to solutions #9 and #11.

8. All decryption keys relating to the long-term key, Milenage OPc values and TUAK TOPc values are required to be protected from physical attacks and never leave the secure environment of the UDM/ARPF unprotected, which can be achieved as done in pre-5G networks. Using a Hardware Security Module in the UDM/ARPF would be one method for achieving this. Exporting a protected copy of the decryption keys to a backup location is recommended.

# Annex A

## Models for ARPF deployment

### A.1 General

This clause describes the different deployment models for ARPF considering the following aspects:

- Existing architectural decision in TS 33.501 [2] that defines the ARPF as a function provided by the UDM.

- Deployment of the UDM as a fully stateless NF, where subscription data (including the subscription credentials) is stored in the UDR. Stateful deployment options where subscription credentials are stored within the UDM/ARPF are depicted but these do not require any further analysis within the scope of this TR.

- Coexistence with Authentication vector generation functions in other domains (i.e. HSS/AuC).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Twelfth Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*