|  |
| --- |
| 3GPP TR 33.845 V1.1.0 (2021-05) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Service Aspects;Study on storage and transport of 5G Core (5GC) security parameters for Authentication Credential Repository Processing Function (ARPF) authentication (Release 17) |
|   |
| *5G-logo_175px* | 3GPP-logo_web |
|  |
| 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 Specification 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. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://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.© 2021, 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 members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 6

Introduction 7

1 Scope 8

2 References 8

3 Definitions of terms and abbreviations 9

3.1 Terms 9

3.2 Abbreviations 9

4 Security assumptions relating to communication security in 5G 9

4.1 Overview 9

4.2 Models for ARPF and UDR setup 9

4.2.1 Model #A: Security parameters stored only in the ARPF 9

4.2.2 Model #B: Security parameters stored only in the UDR 10

4.2.3 Model #C: Security parameters stored both in the ARPF and the UDR 10

4.3 Primary Authentication 10

4.4 Secondary Authentication 10

4.5 Privacy 10

5 Parameters relevant to securing 5G communication 11

5.1 Overview 11

5.2 Milenage AKA authentication 12

5.3 TUAK AKA authentication 13

5.4 EAP methods for authentication 13

5.5 Proprietary authentication algorithms 13

5.6 AMF related parameters 13

5.7 Counter related parameters 13

6. Key Issues 14

6.1 Key Issue #1: Separation of authentication subscription data from subscription data 14

6.1.1 Key issue details 14

6.1.2 Security threats 14

6.1.3 Potential security requirements 14

6.2 Key Issue #2: protection of long-term key during storage in UDR 14

6.2.1 Key issue details 14

6.2.2 Security threats 14

6.2.3 Potential security requirements 14

6.3 Key Issue #3: protection of long-term key during transfer out of UDR 15

6.3.1 Key issue details 15

6.3.2 Security threats 15

6.3.3 Potential security requirements 15

6.4 Key Issue #4: protection of Milenage OPc value during storage in UDR 15

6.4.1 Key issue details 15

6.4.2 Security threats 15

6.4.3 Potential security requirements 15

6.5 Key Issue #5: protection of Milenage OPc value during transfer out of UDR 16

6.5.1 Key issue details 16

6.5.2 Security threats 16

6.5.3 Potential security requirements 16

6.6 Key Issue #6: protection of Milenage OP value during storage in UDR 16

6.6.1 Key issue details 16

6.6.2 Security threats 16

6.6.3 Potential security requirements 16

6.7 Key Issue #7: protection of Milenage OP value during transfer out of UDR 17

6.7.1 Key issue details 17

6.7.2 Security threats 17

6.7.3 Potential security requirements 17

6.8 Key Issue #8: protection of sequence number SQNHE during storage in UDR 17

6.8.1 Key issue details 17

6.8.2 Security threats 17

6.8.3 Potential security requirements 17

6.9 Key Issue #9: protection of sequence number SQNHE during transfer out of UDR 17

6.9.1 Key issue details 17

6.9.2 Security threats 18

6.9.3 Potential security requirements 18

6.10 Key Issue #10: protection of TUAK TOPc value during storage in UDR 18

6.10.1 Key issue details 18

6.10.2 Security threats 18

6.10.3 Potential security requirements 18

6.11 Key Issue #11: protection of TUAK TOPc value during transfer out of UDR 18

6.11.1 Key issue details 18

6.11.2 Security threats 18

6.11.3 Potential security requirements 19

7 Solutions 19

7.1 Solution #1: Authorization and Isolation of Authentication Data using existing techniques. 19

7.1.1 Introduction 19

7.1.2 Solution details 19

7.1.3 Evaluation 20

7.2 Solution #2: Protection of LTK during storage in UDR. 20

7.2.1 Introduction 20

7.2.2 Solution details 20

7.2.3 Evaluation 20

7.3 Solution #3: Protection of LTK over Nudr 21

7.3.1 Introduction 21

7.3.2 Solution details 21

7.3.3 Evaluation 21

7.4 Solution #4: Encrypted storage of the long-term key in the UDR 21

7.4.1 Introduction 21

7.4.2 Solution details 22

7.4.3 Evaluation 22

7.5 Solution #5: Encrypted transfer of the long-term key between UDR and UDM/ARPF 22

7.5.1 Introduction 22

7.5.2 Solution details 22

7.5.3 Evaluation 22

7.6 Solution #6: Storage of the LTK in the UDR 23

7.6.1 Introduction 23

7.6.2 Solution details 23

7.6.3 Evaluation 23

7.7 Solution #7: Transfer of the LTK out of the UDR 23

7.7.1 Introduction 23

7.7.2 Solution details 24

7.7.3 Evaluation 24

7.8 Solution #8: Encrypted transfer of Milenage OPc value between UDR and UDM/ARPF 24

7.8.1 Introduction 24

7.8.2 Solution details 24

7.8.3 Evaluation 25

7.9 Solution #9: Encrypted transfer of Milenage OP value between UDR and UDM/ARPF 25

7.9.1 Introduction 25

7.9.2 Solution details 25

7.9.3 Evaluation 25

7.10 Solution #10: Encrypted storage of Milenage OPc value in the UDR 26

7.10.1 Introduction 26

7.10.2 Solution details 26

7.10.3 Evaluation 26

7.11 Solution #11: Encrypted storage of Milenage OP value in the UDR 26

7.11.1 Introduction 26

7.11.2 Solution details 26

7.11.3 Evaluation 27

7.12 Solution #12: Access control for protection of SQNHE during storage in UDR 27

7.12.1 Introduction 27

7.12.2 Solution details 27

7.12.3 Evaluation 27

7.13 Solution #13: Encrypted storage of TUAK TOPc value in the UDR 27

7.13.1 Introduction 27

7.13.2 Solution details 28

7.13.3 Evaluation 28

7.14 Solution #14: OAuth 2.0 secured transfer of SQNHE out of UDR 28

7.14.1 Introduction 28

7.14.2 Solution details 28

7.14.3 Evaluation 28

7.15 Solution #15: Encrypted transfer of TUAK TOPc value between UDR and UDM/ARPF 29

7.15.1 Introduction 29

7.15.2 Solution details 29

7.15.3 Evaluation 29

8 Conclusions 29

Annex A: Models for ARPF deployment 30

A.1 General 30

A.2 ARPF deployment options in 3GPP TS 33.501 [2] and TS 23.501 [10] 30

A.3 ARPF deployment options in UDICOM 31

Annex B (informative): Change history 34

For definitive guidance on drafting 3GPP TSs and TRs, see [3GPP TS 21.801](http://www.3gpp.org/DynaReport/21801.htm) supplemented by the 3GPP web page <http://www.3gpp.org/specifications-groups/delegates-corner/writing-a-new-spec>.

Ensure all blue guidance text is removed before submitting the TS/TR to the TSG for approval.

# 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.

# Introduction

The ability to store various security parameters is standardised for the ARPF and the UDR. However, the security of this storage and the security related to transporting security parameters from the UDR to the UDM/ARPF are not defined.

This document provides the background and lists potential solutions for identified key issues.

# 1 Scope

The present document details the following:

- The security assumptions relating to security communication in 5G.

- The security assumptions related to protecting subscriber privacy.

- The home network parameters that are relevant to securing the communication in 5G and protecting subscriber privacy.

- Key Issues, threats and requirements relevant to securing the communication in 5G and protecting subscriber privacy.

- Solutions that potentially resolve the key issues described.

The present document does not describe the storage of security parameters in the UE or the serving network or the transportation of secure information between the home network and the serving network.

# 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.

NOTE 1: 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] 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].

# 4 Security assumptions relating to communication security in 5G

## 4.1 Overview

As defined in TS 33.501 [2], the UDM plays a key role in primary authentication and the privacy feature by supporting the ARPF and SIDF functionality.

The ARPF and SIDF functionality requires the use of certain security parameters. The security parameters used for the ARPF functionality (authentication subscription data) are specified in clause 5.1. When UDM makes use of the UDR to manage subscription data, part of the security parameters required by the ARPF and SIDF may be stored in UDR as described in clause 4.2.

## 4.2 Models for ARPF and UDR setup

### 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.

### 4.2.2 Model #B: Security parameters stored only in the UDR

Model #B is the model where security parameters for the execution of primary authentication are stored only at the UDR. This model corresponds to a maximally stateless ARPF deployment model where UDR is used for storing all security parameters.

### 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.

## 4.4 Secondary Authentication

3GPP TS 33.501 [2] defines secondary authentication for a DN to authenticate and/or authorize a UE to access the DN. The EAP framework based authentication is introduced for secondary authentication between the UE and the DN-AAA server in the DN.

During the PDU session establishment procedure, the SMF (in non-roaming and Home Routed roaming cases, the H-SMF; in LBO case, the V-SMF) determines whether the secondary authentication is required via exchanging with UDM. If secondary authentication is required, the SMF shall trigger EAP authentication procedure. The UE and the DN AAA server exchange EAP message for secondary authentication. On the network side, the credential of the UE for secondary authentication is stored in DN-AAA.

In the secondary authentication procedure, the ARPF is not involved.

## 4.5 Privacy

3GPP TS 33.501 [2] defines a mechanism for subscription identifier privacy over-the-air. It uses the SUCI which is a privacy preserving identifier generated at the UE and containing the concealed SUPI, using a Home Network Public Key securely provisioned in the USIM and in control of the home network.

The Home Network Private Key used for subscriber privacy is protected from physical attacks in the UDM: TS 33.501 section 6.2.2.1, specifies that "*the ARPF holds the home network private key that is used by the SIDF to deconceal the SUCI and reconstruct the SUPI*".

In the network side, the SIDF (Subscription Identifier De-concealing Function) is responsible for de-concealment of the SUCI using a Home Network Private Key. The SIDF is a service offered by UDM and holds the Home Network Public Key Identifier(s) for the private/public key pair(s) used for subscriber privacy.

# 5 Parameters relevant to securing 5G communication

## 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

## 6.1 Key Issue #1: Separation of authentication subscription data from subscription data

### 6.1.1 Key issue details

The Unified Data Repository (UDR) is located in the same PLMN as the NF service consumers are storing or retrieving data from UDR using Nudr services. Data stored in the UDR are subscription data, authentication subscription data, policy data, structured data for exposure, and application data (see 3GPP TS 29.505).

Nudr is an intra-PLMN interface and allows NF consumers to use its service to retrieve, create, update, subscribe for change notifications, unsubscribe for change notifications and delete data stored in the UDR, based on the set of data applicable to the consumer.

### 6.1.2 Security threats

UDR can be accessed by several NFs. If authentication subscription data is accessible in the same branche of the data model as subscription data, also other NFs than UDM may be able to access those data.

### 6.1.3 Potential security requirements

Sensitive data such as authentication subscription data should be compartmentalized from subscription data.

For authentication subscription data, which are sensitive data, the access shall be limited to UDM only.

## 6.2 Key Issue #2: protection of long-term key during storage in UDR

### 6.2.1 Key issue details

In case the long-term key, which is part of the authentication subscription data needed to generate authentication vectors in the UDM/ARPF, is stored in the UDR separate from the UDM/ARPF, then this key needs to be protected. This key issue addresses this need.

### 6.2.2 Security threats

If the stored long-term key can be modified in the UDR, this can cause a DOS attack by invalidating regular authentication subscription data.

If the stored long-term key is obtained, then it can be used to access previously recorded communications.

If the stored long-term key retrieved from a subscriber's authentication subscription data can be copied to another subscriber's authentication subscription data, then this can result in stealing network access from the first subscriber.

### 6.2.3 Potential security requirements

The long-term key in the UDR shall be protected against retrieval by unauthorized network elements and by unauthorized persons.

The long-term key shall be protected against unauthorized modification after storage in the UDR.

It shall be prevented that the long-term key is copied from one subscriber's authentication subscription data to another subscriber's authentication subscription data.

## 6.3 Key Issue #3: protection of long-term key during transfer out of UDR

### 6.3.1 Key issue details

In case the long-term key, which is part of the authentication subscription data needed to generate authentication vectors in the UDM/ARPF, is transferred out of the UDR to the UDM/ARPF, then this key needs to be protected during its transfer. This key issue addresses this need.

### 6.3.2 Security threats

If the long-term key can be modified during transfer out of the UDR to the UDM/ARPF, this can cause a DOS attack by generating invalid authentication vectors in the UDM/ARPF.

If the long-term key is obtained during transfer out of the UDR, then it can be used to access previously recorded communications.

### 6.3.3 Potential security requirements

The long-term key shall be protected during transfer out of the UDR against eavesdropping by unauthorized network elements and by unauthorized persons.

The long-term key shall be protected against modification during transfer out of the UDR.

## 6.4 Key Issue #4: protection of Milenage OPc value during storage in UDR

### 6.4.1 Key issue details

In case the Milenage OPc value, which is part of the authentication subscription data needed to generate authentication vectors in the UDM/ARPF – in case Milenage [3] is used – is stored in the UDR separate from the UDM/ARPF, then this value needs to be protected. This key issue addresses this need.

### 6.4.2 Security threats

OPc values are one of the sensitive data items needed to populate USIMs. If OPc values are obtained by unauthorized network elements or by unauthorized persons, this increases the risk of unauthorized USIM creation.

If the stored OPc value can be modified in the UDR, this can cause a DOS attack by invalidating regular authentication subscription data.

### 6.4.3 Potential security requirements

The OPc value shall be protected against retrieval by unauthorized network elements and by unauthorized persons.

The OPc value shall be protected against unauthorized modification during storage in the UDR.

## 6.5 Key Issue #5: protection of Milenage OPc value during transfer out of UDR

### 6.5.1 Key issue details

In case the Milenage OPc value, which is part of the authentication subscription data needed to generate authentication vectors in the UDM/ARPF – in case Milenage [3] is used – is transferred out of the UDR to the UDM/ARPF, then this value needs to be protected. This key issue addresses this need.

### 6.5.2 Security threats

OPc values are one of the sensitive data items needed to populate USIMs. If OPc values are obtained by unauthorized network elements or by unauthorized persons, this increases the risk of unauthorized USIM creation.

If the stored OPc value can be modified during transfer out of the UDR, this can cause a DOS attack by invalidating regular authentication subscription data.

### 6.5.3 Potential security requirements

The OPc value shall be protected during transfer out of the UDR against eavesdropping by unauthorized network elements and by unauthorized persons.

The OPc value shall be protected against modification during transfer out of the UDR.

## 6.6 Key Issue #6: protection of Milenage OP value during storage in UDR

### 6.6.1 Key issue details

In case the Milenage OP value, which can be used to generate the OPc value that is part of the authentication subscription data needed to generate authentication vectors in the UDM/ARPF – in case Milenage [3] is used – is stored in the UDR separate from the UDM/ARPF, then this value needs to be protected. This key issue addresses this need.

### 6.6.2 Security threats

If the OP value can be obtained by an unauthorized network element or an unauthorized person, it can be used – in combination with long-term keys – to create subscriber specific Milenage OPc values. These OPc values are one of the data items needed to populate USIMs.

If the stored OP value can be modified in the UDR, this can cause a DOS attack by invalidating regular authentication subscription data.

### 6.6.3 Potential security requirements

If the OP value is stored in the UDR, then the OP value shall be protected against retrieval by unauthorized network elements and by unauthorized persons.

If the OP value is stored in the UDR, then the OP value shall be protected against unauthorized modification after storage in the UDR.

## 6.7 Key Issue #7: protection of Milenage OP value during transfer out of UDR

### 6.7.1 Key issue details

In case the Milenage OP value, which can be used to generate the OPc value that is part of the authentication subscription data needed to generate authentication vectors in the UDM/ARPF – in case Milenage [3] is used – is transferred out of the UDR to the UDM/ARPF, then this value needs to be protected. This key issue addresses this need.

### 6.7.2 Security threats

If the OP value can be obtained by an unauthorized network element or an unauthorized person, it can be used – in combination with long-term keys – to create subscriber specific Milenage OPc values. These OPc values are one of the data items needed to populate USIMs.

If the stored OP value can be modified in the UDR, this can cause a DOS attack by invalidating regular authentication subscription data.

### 6.7.3 Potential security requirements

If the OP value is stored in the UDR, then the OP value shall be protected during transfer out of the UDR against eavesdropping by unauthorized network elements and by unauthorized persons.

If the OP value is stored in the UDR, then the OP value shall be protected against modification during transfer out of the UDR.

## 6.8 Key Issue #8: protection of sequence number SQNHE during storage in UDR

### 6.8.1 Key issue details

In case the sequence number SQNHE, which is part of the authentication subscription data needed to generate authentication vectors in the UDM/ARPF is stored in the UDR separate from the UDM/ARPF, then this sequence number needs to be protected. This key issue addresses this need.

### 6.8.2 Security threats

If the SQNHE can be obtained by an unauthorized network element or an unauthorized person, it can be used to identify and track a subscriber.

### 6.8.3 Potential security requirements

The SQNHE shall be protected against retrieval by unauthorized network elements and by unauthorized persons.

## 6.9 Key Issue #9: protection of sequence number SQNHE during transfer out of UDR

### 6.9.1 Key issue details

In case the sequence number SQNHE, which is part of the authentication subscription data needed to generate authentication vectors in the UDM/ARPF is transferred out the UDR to the UDM/ARPF, then this sequence number needs to be protected. This key issue addresses this need.

### 6.9.2 Security threats

If the SQNHE can be obtained by an unauthorized network element or an unauthorized person, it can be used to identify and track a subscriber.

### 6.9.3 Potential security requirements

The SQNHE shall be protected during transfer out of the UDR against eavesdropping by unauthorized network elements and by unauthorized persons.

## 6.10 Key Issue #10: protection of TUAK TOPc value during storage in UDR

### 6.10.1 Key issue details

In case the TUAK TOPc value, which is part of the authentication subscription data needed to generate authentication vectors in the UDM/ARPF – in case TUAK [4] is used – is stored in the UDR separate from the UDM/ARPF, then this value needs to be protected. This key issue addresses this need.

### 6.10.2 Security threats

TOPc values are one of the sensitive data items needed to populate USIMs. If TOPc values are obtained by unauthorized network elements or by unauthorized persons, this increases the risk of unauthorized USIM creation.

If the stored TOPc value can be modified in the UDR, this can cause a DOS attack by invalidating regular authentication subscription data.

### 6.10.3 Potential security requirements

The TOPc value shall be protected against retrieval by unauthorized network elements and by unauthorized persons.

The TOPc value shall be protected against unauthorized modification during storage in the UDR.

## 6.11 Key Issue #11: protection of TUAK TOPc value during transfer out of UDR

### 6.11.1 Key issue details

In case the TUAK TOPc value, which is part of the authentication subscription data needed to generate authentication vectors in the UDM/ARPF – in case TUAK [4] is used – is transferred out of the UDR to the UDM/ARPF, then this value needs to be protected. This key issue addresses this need.

### 6.11.2 Security threats

TOPc values are one of the sensitive data items needed to populate USIMs. If TOPc values are obtained by unauthorized network elements or by unauthorized persons, this increases the risk of unauthorized USIM creation.

If the stored TOPc value can be modified during transfer out of the UDR, this can cause a DOS attack by invalidating regular authentication subscription data.

### 6.11.3 Potential security requirements

The TOPc value shall be protected during transfer out of the UDR against eavesdropping by unauthorized network elements and by unauthorized persons.

The TOPc value shall be protected against modification during transfer out of the UDR.

# 7 Solutions

## 7.1 Solution #1: Authorization and Isolation of Authentication Data using existing techniques.

### 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.

### 7.1.2 Solution details

As defined in 3GPP TS 23.501 [10] the UDR is located in the same PLMN as the NF service consumers storing in and retrieving data from it using Nudr. This is, Nudr is an intra-PLMN interface.

The only NF service consumers that are defined to use UDR as per 3GPP TS 23.502 [13] are UDM (for subscription data), PCF (for policy subscription data), NEF (for exposure and application data) and NRF/SCP (for NF Group ID mapping data). It is possible however that multiple UDRs are deployed in the network, each of which can accommodate different data sets or subsets, (e.g. subscription data, subscription policy data, data for exposure, application data) and/or serve different sets of NFs. This is, it is possible to deploy a UDR dedicated to store subscription data used and accessed only by UDM. In this case, the UDR profile stored in the NRF can indicate that ONLY UDM NFs are authorized to discover UDR instances storing subscription data (i.e. NF consumers other than UDM will not be able to discover UDR instances handling subscription data nor authentication subscription data).

Even in the case where the same UDR is deployed to support storage of data for multiple NF consumers (e.g. UDM, PCF and NEF), UDR can authorize the access of specific data resources for specific operations (e.g. read, modify) on a per NF type basis using the OAuth 2.0 based Authorization Framework defined in 3GPP 33.501 [2] for Release 16.

The OAuth 2.0 based authorization framework defined in 3GPP 33.501 [2] is being enhanced in Release 16 to support the generation and validation of authorization tokens including authorization not only at service level but also to service operation and resource level. This allows the possibility to generate OAuth 2.0 tokens to retrieve *AuthenticationSubscription* data ONLY to UDM NF type of service consumers.

Finally, based on implementation-specific means, it is possible that the storage of the *AuthenticationSubscription* data resources within a UDR NF instance are managed in specific storage resources within the UDR NF instance as described in 3GPP TS 29.500 [12] and 3GPP TS 29.505 [11]. This can allow that the security parameters defined within the *AuthenticationSubscription* data type could be isolated from the rest of storage resources used for storing other subscription profile information within the UDR NF instance not only from a traffic reference point (i.e. via Nudr) but also from Provisioning and OAM interfaces.

### 7.1.3 Evaluation

This solution proposes that the isolation of authentication subscription data from subscription data can be based on existing capabilities defined by 3GPP TSs without the need for any additional specification work.

The resource-based authorization introduced to the OAuth 2.0 authorization framework during release 16 ensures that the access to the authentication subscription data can be limited.

Authentication subscription data can be additionally compartmentalized from subscription data as described in 3GPP TS 29.500 [12] and 3GPP TS 29.505 [11].

## 7.2 Solution #2: Protection of LTK during storage in UDR.

### 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.

### 7.2.2 Solution details

The OAuth 2.0 based authorization framework defined in 3GPP 33.501 [2] is being enhanced in Release 16 to support the generation and validation of authorization tokens including authorization not only at service level but also to service operation and resource level. This allows the possibility to generate OAuth 2.0 tokens to retrieve *AuthenticationSubscription* data ONLY to UDM/ARPF NF type of service consumers.

UDR will in any case prevent the modification of LTK within the *AuthenticationSubscription* data resource by the UDM/ARPF over Nudr as defined in 3GPP TS 29.505 [11]:

*Table 5.2.1-1 provides an overview of the resources and applicable HTTP methods.*

**Table 5.2.1-1: Resources and methods overview**

|  |  |  |  |
| --- | --- | --- | --- |
| *Resource name* | *Resource URI* | *HTTP method*  | *Description* |
| *AuthenticationSubscription* | */subscription-data/{ueId}/authentication-data/authentication-subscription* | *GET* | *Retrieve a UE's authentication subscription data* |
| *PATCH* | *Update a UE's authentication subscription data**Updates shall be limited to the* ***sequenceNumber*** *attribute. Attempts to patch any other attribute shall be rejected by the UDR.* |

The long-term key should be additionally provisioned and stored encrypted in UDR. This solution does not cover security requirements (e.g. encryption algorithms) for this.

### 7.2.3 Evaluation

Solution#2 in TR 33.845 [1] proposes that the protection of the LTK during storage in UDR relies on the OAuth 2.0 based authorization framework defined in 3GPP TS 33.501 [2].

The capability for resource-based authorization introduced to the OAuth 2.0 authorization framework during release 16, fulfils the related security requirements to protect against unauthorized retrieval or modification of the LTK while stored in the UDR when accessing the UDR from other SBA connected NFs, but it does not fulfill the security requirement to protect against other ways of accessing the UDR.

## 7.3 Solution #3: Protection of LTK over Nudr

### 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.

## 7.4 Solution #4: Encrypted storage of the long-term key in the UDR

### 7.4.1 Introduction

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

In order to protect the long-term key during storage in the UDR, the long-term key is stored in encrypted form in the UDR. During primary authentication, the UDM/ARPF retrieves the authentication subscription data for the UE which includes the encrypted long-term key as stored in UDR. That is, the long-term key is never provided by the UDR in clear text and there is no need for the UDR to decrypt the long-term key.

At generation of a long-term key an encryption key is used that is shared with the UDM/ARPF where it is decrypted during primary authentication. The generation of a long-term key can be performed in the network of an operator or it can be performed at the facility where USIMs are being provisioned.

### 7.4.2 Solution details

The long-term key is stored in encrypted form if stored in the UDR. The encryption algorithm used and the method for the handling of the encryption/decryption key(s) needs to conform to the security policy requirements of the operator. This solution recommends the use of NIST approved algorithms.

NOTE: The selection of the encryption algorithm and the encryption/decryption key(s) is operator dependent.

### 7.4.3 Evaluation

This solution addresses the requirements of the KI by protecting the long-term key in one way:

- storing the long-term key in encrypted form in the UDR

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.

## 7.5 Solution #5: Encrypted transfer of the long-term key between UDR and UDM/ARPF

### 7.5.1 Introduction

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

As described in 3GPP TS 33.501 [2], clause 5.8.1, the long-term key used for authentication and security association setup purposes shall be protected from physical attacks and shall never leave the secure environment of the UDM/ARPF unprotected. If stored in the UDR, the long-term key is always transported in encrypted form during its transfer from UDR to UDM/ARPF.

### 7.5.2 Solution details

The long-term key is transferred in encrypted form between UDR and UDM/ARPF. The encryption algorithm used and the method for the handling of the encryption/decryption key(s) needs to conform to the security policy requirements of the operator. This solution recommends the use of NIST approved algorithms.

NOTE 1: The selection of the encryption algorithm and the encryption/decryption key(s) is operator dependent.

The transfer of the encrypted long-term key over the Nudr interface is protected at transport level using the security mechanisms defined in 3GPP TS 33.501 [2], clause 13.1, as any other SBA interface.

During transfer, a key identifier is associated to the encrypted long-term key to enable identification of the decryption key in the UDM/ARPF.

NOTE 2: The implementation of how to identify the decryption key is out of scope of 3GPP.

### 7.5.3 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 two 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).

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. This 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.

## 7.6 Solution #6: Storage of the LTK in the UDR

### 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.

### 7.6.2 Solution details

The OAuth 2.0 based authorization framework defined in 33.501[2], clause 13.4.1, is enhanced in Release 16 to support the generation and validation of authorization tokens, including authorization at resource level. This allows the possibility of generating OAuth 2.0 access tokens to restrict retrieval of *AuthenticationSubscription* data to UDM/ARPF NF type service consumers only, preventing unauthorised access by other NF type. Such access tokens can be required by the UDM to access the long-term key.

As defined in TS 29.505 [11], Clause 5.2.1, Table 5.2.1-1, any modification of the long term key with the *AuthenticationSubscription* data resource by the UDM/ARPF over Nudr is limited to the *sequenceNumber* attribute, and attempts to modify any other attribute shall be rejected by the UDR.

### 7.6.3 Evaluation

This Solution proposes that the protection of the long-term key during storage in UDR relies on the OAuth 2.0 based authorization framework defined in TS 33.501 [2], and upon the restricted modification of the *AuthenticationSubscription* data type.

The capability for resource-based authorization introduced to the OAuth 2.0 authorization framework during release 16 ensures that the access to the authentication subscription data can be limited, and fulfils the security requirements to protect against unauthorized retrieval or modification of the long-term key while stored in the UDR when accessing the UDR from other SBA connected NFs, but it does not fulfil the security requirement to protect against other ways of accessing the UDR. The *AuthenticationSubscription* data type editing restrictions further protect against modification from any entity.

## 7.7 Solution #7: Transfer of the LTK out of the UDR

### 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.

### 7.7.2 Solution details

The OAuth 2.0 based authorization framework defined in TS 33.501[2], clause 13.4.1, is enhanced in Release 16 to support the generation and validation of authorization tokens, including authorization at resource level. This allows the possibility of generating OAuth 2.0 access tokens to restrict retrieval of *AuthenticationSubscription* data to UDM/ARPF NF type service consumers only, for which the long-term key will be transported along the Nudr interface. As with any other SBA reference point, Nudr is protected at transport level using TLS as defined in 3GPP TS 33.501[2] clause 13.1.

As defined in TS 29.505 [11], any modification of the long term key with the *AuthenticationSubscription* data resource by the UDM/ARPF over Nudr is limited to the *sequenceNumber* attribute, and attempts to modify any other attribute shall be rejected by the UDR.

### 7.7.3 Evaluation

This Solution proposes that the protection of the long-term key during transfer out of the UDR relies on the OAuth 2.0 based authorization framework defined in TS 33.501 [2], and upon the restricted modification of the *AuthenticationSubscription* data type.

The capability for resource-based authorization introduced to the OAuth 2.0 authorization framework during release 16 ensures that the access to the authentication subscription data can be limited, and fulfils the security requirements to protect against unauthorized retrieval or modification of the long-term key while being transferred out of the UDR. The *AuthenticationSubscription* data type editing restrictions further protect against modification from any entity.

## 7.8 Solution #8: Encrypted transfer of Milenage OPc value between UDR and UDM/ARPF

### 7.8.1 Introduction

This solution addresses key issue #5 on "protection of Milenage OPc value during transfer out of UDR".

If stored in the UDR, the Milenage OPc value is always transported in encrypted form during its transfer from UDR to UDM/ARPF.

### 7.8.2 Solution details

If stored in the UDR, the Milenage OPc value is transferred in encrypted form between UDR and UDM/ARPF. The encryption algorithm used and the method for the handling of the encryption/decryption key(s) needs to conform to the security policy requirements of the operator. This solution recommends the use of NIST approved algorithms.

NOTE 1: The selection of the encryption algorithm and the encryption/decryption key(s) is operator dependent.

The transfer of the encrypted Milenage OPc value over the Nudr interface is protected at transport level using the security mechanisms defined in TS 33.501 [2], clause 13.1, as any other SBA interface.

During transfer, a key identifier is associated to the encrypted Milenage OPc value to enable identification of the decryption key in the UDM/ARPF.

NOTE 2: The implementation of how to identify the decryption key is out of scope of 3GPP.

### 7.8.3 Evaluation

This solution addresses the requirements of the KI by protecting the transfer of the Milenage OPc value between the UDR and the UDM/ARPF in two ways:

- transporting the OPc value in encrypted form during its transfer from UDR to UDM/APRF, and

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

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, as specified in TS 33.501 [2], clause 5.8.1. 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.

## 7.9 Solution #9: Encrypted transfer of Milenage OP value between UDR and UDM/ARPF

### 7.9.1 Introduction

This solution addresses key issue #7 on "protection of Milenage OP value during transfer out of UDR".

If stored in the UDR, the Milenage OP value is always transported in encrypted form during its transfer from UDR to UDM/ARPF.

### 7.9.2 Solution details

If stored in the UDR, the Milenage OP value is transferred in encrypted form between UDR and UDM/ARPF. The encryption algorithm used and the method for the handling of the encryption/decryption key(s) needs to conform to the security policy requirements of the operator. This solution recommends the use of NIST approved algorithms.

NOTE 1: The selection of the encryption algorithm and the encryption/decryption key(s) is operator dependent. The transfer of the encrypted Milenage OP value over the Nudr interface is protected at transport level using the security mechanisms defined in TS 33.501 [2], clause 13.1, as any other SBA interface.

During transfer, a key identifier is associated to the encrypted Milenage OP value to enable identification of the decryption key in the UDM/ARPF.

NOTE 2: The implementation of how to identify the decryption key is out of scope of 3GPP.

### 7.9.3 Evaluation

This solution addresses the requirements of the KI by protecting the transfer of the Milenage OP value between the UDR and the UDM/ARPF in two ways:

- transporting the OP value in encrypted form during its transfer from UDR to UDM/APRF, and

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

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, as specified in TS 33.501 [2], clause 5.8.1. 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.

## 7.10 Solution #10: Encrypted storage of Milenage OPc value in the UDR

### 7.10.1 Introduction

This solution addresses key issue #4 on "protection of Milenage OPc value during storage in UDR".

If the Milenage OPc value is stored in the UDR, it is stored in encrypted form in the UDR. During primary authentication, the UDM/ARPF retrieves authentication subscription data for the UE which can include the Milenage OPc value as stored in UDR. That is, the Milenage OPc value is never provided by the UDR in clear text and there is no need for the UDR to decrypt the Milenage OPc value.

At generation of the Milenage OPc value an encryption key is used that is shared with the UDM/ARPF where it is decrypted during primary authentication. The generation of the Milenage OPc value can be performed in the network of an operator or it can be performed at the facility where USIMs are being provisioned.

### 7.10.2 Solution details

If stored in the UDR, the Milenage OPc value is stored in encrypted form. The encryption algorithm used and the method for the handling of the encryption/decryption key(s) needs to conform to the security policy requirements of the operator. This solution recommends the use of NIST approved algorithms.

NOTE: The selection of the encryption algorithm and the encryption/decryption key(s) is operator dependent.

### 7.10.3 Evaluation

This solution addresses the requirements of the KI by protecting the Milenage OPc value in one way:

- storing the OPc value in encrypted form in the UDR.

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, as specified in TS 33.501 [2], clause 5.8.1. 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.

## 7.11 Solution #11: Encrypted storage of Milenage OP value in the UDR

### 7.11.1 Introduction

This solution addresses key issue #6 on "protection of Milenage OP value during storage in UDR".

If the Milenage OP value is stored in the UDR, it is stored in encrypted form in the UDR. During primary authentication, the UDM/ARPF retrieves authentication subscription data for the UE which can include the Milenage OP value as stored in UDR. That is, the Milenage OP value is never provided by the UDR in clear text and there is no need for the UDR to decrypt the Milenage OP value.

At selection of the Milenage OP value an encryption key is used that is shared with the UDM/ARPF where it is decrypted during primary authentication. The selection of the Milenage OP value can be performed in the network of an operator or it can be performed at the facility where USIMs are being provisioned.

### 7.11.2 Solution details

If stored in the UDR, the Milenage OP value is stored in encrypted form. The encryption algorithm used and the method for the handling of the encryption/decryption key(s) needs to conform to the security policy requirements of the operator. This solution recommends the use of NIST approved algorithms.

NOTE: The selection of the encryption algorithm and the encryption/decryption key(s) is operator dependent.

### 7.11.3 Evaluation

This solution addresses the requirements of the KI by protecting the Milenage OP value in one way:

- storing the OP value in encrypted form in the UDR.

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, as specified in TS 33.501 [2], clause 5.8.1. 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.

## 7.12 Solution #12: Access control for protection of SQNHE during storage in UDR

### 7.12.1 Introduction

This solution addresses key issue #8 on " protection of sequence number SQNHE during storage in UDR".

This solution is based on the observation that encrypted storage of the SQNHE value when stored in the UDR is not needed. Standard access control mechanisms are sufficient for protecting the SQNHE value during storage in the UDR.

For access by other NFs, the solution is based on the use of access tokens created using the OAuth 2.0 based authorization framework. The solution trusts these access tokens to protect SQNHE from retrieval by unauthorized NFs.

### 7.12.2 Solution details

The SQNHE value is protected during storage in the UDR via standard access control mechanisms (e.g. username/password, ACL lists, etc.). For access by other NFs, the OAuth 2.0 based authorization framework is used.

The OAuth 2.0 based authorization framework defined in TS 33.501 [2], clause 13.4.1, is being enhanced in Release 16 to support the generation and validation of authorization tokens, including authorization at resource level. This allows the possibility of generating OAuth 2.0 access tokens to restrict retrieval of *AuthenticationSubscription* data to UDM/ARPF NF type service consumers only, preventing unauthorised access by other NF types. Such access tokens can be required by the UDM/ARPF to access SQNHE.

### 7.12.3 Evaluation

For the use of the OAuth 2.0 based authorization framework, capabilities are used that are defined or planned to be defined in 3GPP specifications. This solution does not require (additional) changes to normative specifications.

## 7.13 Solution #13: Encrypted storage of TUAK TOPc value in the UDR

### 7.13.1 Introduction

This solution addresses key issue #10 on "protection of TUAK TOPc value during storage in UDR".

If the TUAK TOPc value is stored in the UDR, it is stored in encrypted form in the UDR. During primary authentication, the UDM/ARPF retrieves authentication subscription data for the UE which can include the TUAK TOPc value as stored in UDR. That is, the TUAK TOPc value is never provided by the UDR in clear text and there is no need for the UDR to decrypt the TUAK TOPc value.

At generation of the TUAK TOPc value an encryption key is used that is shared with the UDM/ARPF where it is decrypted during primary authentication. The generation of the TUAK TOPc value can be performed in the network of an operator or it can be performed at the facility where USIMs are being provisioned.

### 7.13.2 Solution details

If stored in the UDR, the TUAK TOPc value is stored in encrypted form. The encryption algorithm used and the method for the handling of the encryption/decryption key(s) needs to conform to the security policy requirements of the operator. This solution recommends the use of NIST approved algorithms.

NOTE: The selection of the encryption algorithm and the encryption/decryption key(s) is operator dependent.

### 7.13.3 Evaluation

This solution addresses the requirements of the KI by protecting the TUAK TOPc in one way:

- storing the TOPc in encrypted form in the UDR.

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, as specified in TS 33.501 [2], clause 5.8.1. 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.

## 7.14 Solution #14: OAuth 2.0 secured transfer of SQNHE out of UDR

### 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.

### 7.14.2 Solution details

The OAuth 2.0 based authorization framework defined in TS 33.501[2], clause 13.4.1, is enhanced in Release 16 to support the generation and validation of authorization tokens, including authorization at resource level. This allows the possibility of generating OAuth 2.0 access tokens to restrict retrieval of *AuthenticationSubscription* data to UDM/ARPF NF type service consumers only, preventing unauthorised access by other NF types, for which SQNHE will be transported along the Nudr interface. As with any other SBA reference point, Nudr is protected at transport level using TLS as defined in TS 33.501[2] clause 13.1.

### 7.14.3 Evaluation

This solution does not require changes to normative specifications.

## 7.15 Solution #15: Encrypted transfer of TUAK TOPc value between UDR and UDM/ARPF

### 7.15.1 Introduction

This solution addresses key issue #11 on "protection of TUAK TOPc value during transfer out of UDR".

If stored in the UDR, the TUAK TOPc value is always transported in encrypted form during its transfer from UDR to UDM/ARPF.

### 7.15.2 Solution details

If stored in the UDR, the TUAK TOPc value is transferred in encrypted form between UDR and UDM/ARPF. The encryption algorithm used and the method for the handling of the encryption/decryption key(s) needs to conform to the security policy requirements of the operator. This solution recommends the use of NIST approved algorithms.

NOTE 1: The selection of the encryption algorithm and the encryption/decryption key(s) is operator dependent.

The transfer of the encrypted TUAK TOPc value over the Nudr interface is protected at transport level using the security mechanisms defined in TS 33.501 [2], clause 13.1, as any other SBA interface.

During transfer, a key identifier is associated to the encrypted TUAK TOPc value to enable identification of the decryption key in the UDM/ARPF.

NOTE 2: The implementation of how to identify the decryption key is out of scope of 3GPP.

### 7.15.3 Evaluation

This solution addresses the requirements of the KI by protecting the transfer of the TUAK TOPc value between the UDR and the UDM/ARPF in two ways:

# 8 Conclusions

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 3GPP. It is not expected that Model #B will be supported by 3GPP.

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.

9. For supporting the UDICOM option where the HSS generates the 5G authentication vectors (see TS 23.632 [5], clause 5.2.2), it is needed to allow the Home Network Private Key to be stored in the UDM.

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).

# A.2 ARPF deployment options in 3GPP TS 33.501 [2] and TS 23.501 [10]

In TS 33.501 [2], the ARPF is defined as a function to be provided within the UDM.

For interworking with EPC (and IMS), in TS 23.501 [10], the HSS and the UDM are also defined as a combined NF, i.e. HSS+UDM where interactions between the HSS and the UDM are not specified. The HSS also includes the function to generate authentication vectors in EPS, IMS, GBA and GPRS/UMTS domains; i.e. the AuC.

The HSS+UDM may be deployed as a stateful or stateless NF.

Figure A.2-1 shows the ARPF deployment option when the HSS+UDM is deployed as a stateful NF and subscription credentials are stored within the HSS+UDM (i.e. within the AuC+ARPF).



Figure A.2-1: Stateful ARPF deployment

Figure A.2-2 shows the ARPF deployment option when the HSS+UDM is deployed as a stateless NF and subscription credentials are stored in the UDR (i.e. EPS + 5GS UDR).



Figure A.2-2: Stateless ARPF deployment

# A.3 ARPF deployment options in UDICOM

TS 23.632 [5], defines the Stage 2 architecture, procedures, flows and Network Function Services for User Data Interworking, Coexistence and Migration (UDICOM) between the 5G System and EPS (and IMS).

In the context of UDICOM, HSS and UDM are defined as separate NFs interacting with each other using SBA based interactions over a new NU1 reference point. However, since the subscription credentials shall only be stored centralized in one single place within the system, the UDICOM TS 23.632 [5] defines various options for the generation of authentication vectors.

Figure A.3-1 shows the ARPF deployment option in the context of UDICOM when the HSS and the UDM are deployed as stateful NFs and subscription credentials are stored within the UDM/ARPF.



Figure A.3-1: Stateful ARPF+AuC deployment in UDM according to UDICOM (TS 23.632 [5])

Figure A.3-2 shows the ARPF deployment option in the context of UDICOM when the HSS and the UDM are deployed as stateless NFs and subscription credentials are stored within the 5GS-UDR.



Figure A.3-2: Stateless ARPF+AuC deployment in UDM according to UDICOM (TS 23.632 [5])

In these cases (stateful and stateless ARPF+AuC deployment in UDM), the HSS requests authentication vectors for EPS/IMS/GBA-AKA to the UDM via the new UDICOM NU1 reference point using Nudm services. The UDM does not only support the ARPF functionality but also acts as AuC to generate authentication vectors as defined in TS 33.401 [6], TS 33.402 [7], TS 33.203 [8] and TS 33.220 [9].

Figure A.3-3 shows the ARPF deployment option in the context of UDICOM when the HSS and the UDM are deployed as stateful NFs and subscription credentials are stored within the HSS/AuC instead.



Figure A.3-3: Stateful AuC+ARPF deployment in HSS according to UDICOM (TS 23.632 [5])

Figure A.3-4 shows the ARPF deployment option in the context of UDICOM when the HSS and the UDM are deployed as stateless NFs and subscription credentials are kept within the EPS-UDR.



Figure A.3-4: Stateless AuC+ARPF deployment in HSS according to UDICOM (TS 23.632 [5])

In these cases (stateful and stateless AuC+ARPF deployment in HSS), the UDM requests authentication vectors for 5G-AKA or EAP-AKA’ to the HSS via the new UDICOM NU1 reference point using Nhss services. The HSS does not only support the AuC functionality but also acts as ARPF to generate authentication vectors as defined in TS 33.501 [2]. In these cases, the functionality related to the storage of the Home Network Private Key is always a function provided by the UDM.

Note: The separation of ARPF from UDM conflicts with TS 33.501 [2], clause 6.2.2.1 and clause 5.8.2, which state respectfully, that the ARPF holds the Home Network Private Key, whereas the SIDF shall be a service offered by the UDM.

Finally, Figure A.3-5 shows the ARPF deployment option in the context of UDICOM when the HSS and the UDM are deployed as stateless NFs and subscription credentials are stored within a common EPS+5GS-UDR.



Figure A.3-5: Stateless ARPF deployment in UDM according to UDICOM (TS 23.632 [5]

In this case, the ARPF is function provided by the UDM while the AuC remains as a function provided by the HSS. HSS/AuC and UDM/ARPF generates authentication vectors for their respective domains accessing to the subscription credentials stored in the common EPS+5GS UDR. The UDICOM NU1 reference point is not used for authentication vector retrieval but it is still required to fulfil HSS and UDM interworking related to other use cases (e.g. intersystem mobility).

Annex B (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2019-10 | SA3#96Ad-Hoc | S3-193744 | - | - | - | Initial template | 0.0.0 |
| 2019-10 | SA3#96Ad-Hoc | S3-193745 | - | - | - | Version after SA3#96Ad-Hoc incorporating changes from S3-193747 and S3-193748 | 0.1.0 |
| 2019-11 | SA3#97 | S3-194663 | - | - | - | Updated with: S3-194660, S3-194661, S3-194662, S3‑194291, S3-194664, S3-194669 and S3-194670 | 0.2.0 |
| 2020-05 | SA3#99e | S3-201491 | - | - | - | Updated with S3-201025, S3-201428, S3-201027, S3-201170, S3-201171, s3-201362, S3-201364, S3-201174, S3-201175, S3-201184, S3-201404 and S3-201186. | 0.3.0 |
| 2020-08 | SA3#100e | S3-202261 | - | - | - | Added S3-202061, S3-201626, S3-202110, S3-201628, S3-202060 and S3-202059 | 0.4.0 |
| 2020-09 | SA3#100bis-e | S3-203336 | - | - | - | Updated with S3-202675, S3-202676, S3-202677, S3-202680, S3-202311, S3-202671, S3-202405, S3-202672, S3-202407 | 0.5.0 |
| 2020-11 | SA3#101e | S3-203380 | - | - | - | Added S3-203018, S3-203342, S3-203343 and S3-203345. | 0.6.0 |
| 2021-01 | SA3#102e | S3-210721 | - | - | - | Added S3-210037, [S3-210038](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_102e/Docs/S3-210038.zip), [S3-210039](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_102e/Docs/S3-210039.zip), S3-210709, S3-210712, S3-210713, S3-210714, S3-210716, S3-210717, S3-210718, [S3-210076](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_102e/Docs/S3-210076.zip), S3-210077, S3-210715, S3-210085, S3-210708 and S3-210468. | 0.7.0 |
| 2021-03 | SA#91e | SP-210103 | - | - | - | Presented for information | 1.0.0 |
| 2021-05 | SA3#103e | S3-212360 | - | - | - | Added S3-212347, S3-211533 and S3-212350 |  |