|  |  |
| --- | --- |
| 3GPP TR 33.700-32 V0.3.0 (2024-08) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on security aspects of User Identities and Authentication  (Release 19) | |
|  | |
|  |  |
|  | |
| 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 address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 7

1 Scope 9

2 References 9

3 Definitions of terms and abbreviations 9

3.1 Terms 9

3.2 Symbols 10

3.3 Abbreviations 10

4 Architecture and security assumptions 10

5 Key issues 10

5.1 Key Issue #1: Authentication and Authorization of Human User ID 10

5.1.1 Key issue details 10

5.1.2 Security threats 11

5.1.3 Potential security requirements 11

5.2 Key Issue #2: User privacy 11

5.2.1 Key issue details 11

5.2.2 Security threats 11

5.2.3 Potential security requirements 11

5.3 Key issue #3: Authentication and Authorization of one or more non-3GPP devices behind one gateway UE or 5G-RG 11

5.3.1 Key issue details 11

5.3.2 Security Threats 12

5.3.3 Potential security requirements 12

5.X Key Issue #X: <Key Issue Name> 12

5.X.1 Key issue details 12

5.X.2 Security threats 12

5.X.3 Potential security requirements 12

6 Solutions 12

6.0 Mapping of Solutions to Key Issues 12

6.1 Solution #1: User authentication and authorization of human user 13

6.1.1 Introduction 13

6.1.2 Solution details 13

6.1.3 Evaluation 14

6.2 Solution #2: User Authentication and Authorization via AMF 14

6.2.1 Introduction 14

6.2.2 Solution details 14

6.2.3 Evaluation 16

6.3 Solution #3: User Authentication and Authorization over NAS 16

6.3.1 Introduction 16

6.3.2 Solution details 16

6.3.3 Evaluation 17

6.4 Solution #4: Security protection of human user privacy 18

6.4.1 Introduction 18

6.4.2 Solution details 18

6.4.2.1 KUIA deriving 18

6.4.2.2 User\_ID activation and privacy protection 20

6.4.2.3 Derivation of User-ID related material 22

6.4.3 Evaluation 23

6.5 Solution #5: User authentication and authorization 23

6.5.1 Introduction 23

6.5.1 Solution details 23

6.5.3 Evaluation 24

6.6 Solution #6: Human User authentication of through NAS procedure 25

6.6.1 Introduction 25

6.6.2 Solution Details 25

6.6.3 Evaluation 26

6.7 Solution #7: Authentication and Authorization of Human User ID 26

6.7.1 Introduction 26

6.7.2 Solution Details 27

6.7.4 Evaluation 28

6.8 Solution #8: User authentication with preconfigured credential 28

6.8.1 Introduction 28

6.8.2 Solution details 28

6.8.2.1 Description 28

6.8.2.2 User authentication procedure with the UAAF deployed by operator 29

6.8.2.3 User authentication procedure with the AAA-S deployed by third party 31

6.8.3 Evaluation 31

6.10.1 Introduction 36

6.10.2 Solution details 36

6.10.3 Evaluation 37

6.13 Solution #13: Authentication and Authorization procedure of N3D behind gateway UE or 5G-RG 40

6.13.1 Introduction 40

6.13.2.1 Authentication Procedure 40

6.13.2.2 Re-Authentication procedure 42

6.13.2.3 Authentication and Authorization revocation 42

6.13.4 Evaluation 43

6.14 Solution #14: Authentication and authorization of non-3GPP devices 43

6.14.1 Introduction 43

6.14.2 Solution details 43

6.14.3 Evaluation 43

6.15 Solution #15: Authentication of user behind the UE 44

6.15.1 Introduction 44

6.15.2 Solution details 44

6.15.2.1 Concept 44

6.15.2.2 Solution flow 45

6.15.3 Evaluation 48

6.16 Solution #16: User Authentication and Authorization 49

6.16.1 Introduction 49

6.16.2 Solution details 49

6.16.2.1 User Initiated procedure 49

6.16.2.2 Network Initiated procedure 51

6.16.3 Evaluation 53

6.17 Solution #17: Solution for exposure privacy issue 53

6.17.1 Introduction 53

6.17.2 Solution details 53

6.17.2.1 Exposure of user profile information 53

6.17.2.2a Exposure of linked UE subscription information associated with User Identifier 54

6.17.2.2b Exposure of linked UE subscription information associated with User Identifier to AMF/SMF (internal NFs) 55

6.17.3 Evaluation 56

6.18 Solution #18: User privacy during the connection with 5GC 57

6.18.1 Introduction 57

6.18.2 Solution details 58

6.18.2.1 Mobility or attaching to other access scenarios: 59

6.18.3 Evaluation 59

6.19 Solution #19: User privacy protection 60

6.19.1 Introduction 60

6.19.2 Solution details 60

6.19.3 Evaluation 61

6.20 Solution #20: privacy protection for user ID over the air 61

6.20.1 Introduction 61

6.20.2 Details 61

6.20.3 Evaluation 61

6.21 Solution #21: A&A of non-3GPP devices behind UE or 5G-RG based on secondary authentication 62

6.21.1 Introduction 62

6.21.1 Solution details 62

6.21.3 Evaluation 63

6.22 Solution #22: User authentication with credentials derived by AUSF 63

6.22.1 Introduction 63

6.22.2 Solution details 63

6.22.2.1 Description 63

6.22.2.2 User activation procedure with the AUSF and UIMF 64

6.22.2.3 Key hierarchy for user authentication with derived credential 67

6.22.2.4 User authentication procedure with the UAAF 67

6.22.2.5 Derivation of KUIA and KUSER 68

6.22.3 Evaluation 69

6.23 Solution #23: User Authentication with EAP-PSK 70

6.23.1 Introduction 70

6.23.2 Solution details 70

6.23.3 Evaluation 71

6.24 Solution #24: User ID privacy protection based on EAP-TLS protocol using pseudonym mechanism 71

6.24.1 Introduction 71

6.24.1 Solution details 71

6.24.3 Evaluation 72

6.25 Solution #25: User Authentication with Certificate Generated by an authorized UE 73

6.25.1 Solution Introduction 73

6.25.2 Solution Details 73

6.25.3 Evaluation 74

6.26 Solution #26: User authentication with credentials derived by UIMF 74

6.26.1 Introduction 74

6.26.2 Solution details 74

6.26.2.1 Description 74

6.26.2.2 KUIA generation by AUSF and UE during Registration procedure 75

6.26.2.3 KUSER generation by UIMF and UE during User Authentication procedure 76

6.26.2.4 User authentication between UE and UAAF 77

6.26.2.5 Key hierarchy and derivation 78

6.26.3 Evaluation 78

6.27 Solution #27: User privacy protection for UIP exposure based on RNAA 78

6.27.1 Introduction 78

6.27.2 Solution details 78

6.27.3 Evaluation 79

6.Y Solution #Y: <Solution Name> 79

6.Y.1 Introduction 79

6.Y.2 Solution details 79

6.Y.3 Evaluation 79

7 Conclusions 79

7.3 Key issue #3: Authentication and Authorization of one or more non-3GPP devices behind one gateway UE or 5G-RG 79

Annex <A>: <Informative annex title for a Technical Report> 80

Annex <X>: Change history 81

# Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

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

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

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

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

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

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

**can** indicates that something is possible

**cannot** indicates that something is impossible

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

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

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

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

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

In addition:

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

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

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

# 1 Scope

The present document studies the security and privacy aspects for the creation and usage of user identities as studied in 3GPP TR 23.700-32 [2], with the following focus:

1. Study authentication and authorization of:
   1. a user identifier associated with a subscription and used on a UE (i.e., human user) and
   2. an identifier associated with a non-3GPP device behind a UE or 5G-RG.
2. Study privacy and security impacts of usage of user identifiers associated with a subscription or with a non-3GPP device behind a UE or 5G-RG, including exposure of user profile related information.

# 2 References

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

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

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

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

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

[2] 3GPP TR 23.700-32: "Study on User Identities and Authentication Architecture"

[3] 3GPP TS 33.501: "Security architecture and procedures for 5G System"

[4] 3GPP TS 23.502: "Procedures for the 5G System (5GS)"

[5] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[6] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2"

…

[x] <doctype> <#>[ ([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

# 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], TR 23.700-32 [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].

**Non-3GPP device identifier:** an identifier of a non-3GPP device applies to a non-3GPP device connecting to network via a UE or 5G-RG.

Editor’s Note: the non-3GPP device identifier and user identifier may be updated according to the progress in TR 23.700-32 [2].

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 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].

<ABBREVIATION> <Expansion>

# 4 Architecture and security assumptions

This study should be based on the following assumptions:

- The architecture requirements and assumptions as described in TR 23.700-32[2] apply.

- The security architecture, procedures, and security requirements for 5GS as defined in TS 33.501 [3] are used as a baseline.

- For the non-3GPP device behind a UE or 5G-RG:

- Credentials are assumed to be provisioned in the non-3GPP device by an operator, human user or a 3rd party.

NOTE: How this is performed is not in scope of this study. The authentication of the non-3GPP device is not done by the 5GC.

- For the human user of the UE:

- The user authentication and primary authentication are independent. The user authentication procedure will not impact UE primary authentication procedure.

# 5 Key issues

Editor’s Note: This clause contains all the key issues identified during the study.

## 5.1 Key Issue #1: Authentication and Authorization of Human User ID

### 5.1.1 Key issue details

TR 23.700-32 [2], *Key Issue #2: "Authentication and Authorization of Users and Restrictions on Users"* focuses on:

* authentication and authorization of a human user of a subscription and
* restriction on number of simultaneously active user identifiers of a subscription.

With the following NOTE:

*NOTE: Aspects of this key issue will depend on interaction with SA WG3. For example, authentication and Authorization methods are in the remit of SA WG3.*

The architecture assumption and requirement in TR 23.700-32 [2], clause 4.1 related to linkage and activation of user identifier with a UE subscription apply in the human user scenario.

This key issue is to study the authentication and authorization of a user identifier in the human user scenario.

### 5.1.2 Security threats

Without support for an authentication and authorization mechanism for the human user, an attacker may impersonate the human user of a subscription and gain unauthorized access to services normally available for that subscription legitimate user.

### 5.1.3 Potential security requirements

The 3GPP system shall provide means to support authentication and authorization of human user based on a User identifier linked to a 3GPP subscription.

## 5.2 Key Issue #2: User privacy

### 5.2.1 Key issue details

User identifier is a piece of information used to identify one specific User Identity, which is privacy sensitive.

In clause 5.3 of TR 23.700-32 [2], exposure of User Identity Profile information is documented as a key issue, with a NOTE as following:

"*NOTE 1: Aspects of this key issue will depend on interaction with SA WG3. For example, privacy protections related to exposure of User Identity Profile information and authorization/authentication results need to be coordinated with SA WG3.*"

This key issue focuses on the privacy aspect of User Identifier and User Identity Profile information.

### 5.2.2 Security threats

Either during the communication using User Identifier or during the exposure of User Identity Profile information, without proper protection against linkability and trackability attack, the privacy sensitive information may be leaked to undesired party so that the privacy of the user is violated.

### 5.2.3 Potential security requirements

The 5G system shall provide mechanisms for mitigating privacy attacks (e.g. trackability, linkability) against user identifier during the communication between the UE and the network, including the procedures for user authentication and service access.

The 5G system shall provide mechanisms for mitigating privacy attacks (e.g. disclosure) during the exposure of User Identity Profile information by the network to entities outside operator domain.

## 5.3 Key issue #3: Authentication and Authorization of one or more non-3GPP devices behind one gateway UE or 5G-RG

### 5.3.1 Key issue details

This key issue is going to address Authentication and Authorization of one or more non-3GPP devices behind one gateway UE or 5G-RG. It is to address the security issues related to the key issue #4 in the TR 23.700-32 [2], i.e. Identifying non-3GPP Devices Connecting behind a UE or 5G-RG.

### 5.3.2 Security Threats

If the non-3GPP devices behind one gateway UE or 5G-RG are not authenticated and authorized through means supported by the network, the attacker can access the network as a non-3GPP device via one gateway UE or 5G-RG without any authorization and restriction.

### 5.3.3 Potential security requirements

The 3GPP system shall provide means to support authentication and authorization of a non-3GPP device behind UE or 5G-RG based on a non-3GPP device identifier.

## 5.X Key Issue #X: <Key Issue Name>

### 5.X.1 Key issue details

### 5.X.2 Security threats

### 5.X.3 Potential security requirements

# 6 Solutions

Editor’s Note: This clause contains the proposed solutions addressing the identified key issues.

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions |  | | |
|  | <Key Issue #1> | <Key Issue #2> | <Key Issue #3> |
| #1 | x | x |  |
| #2 | x | x |  |
| #3 | x | x |  |
| #4 | x | x |  |
| #5 | x |  |  |
| #6 | x |  |  |
| #7 | x |  |  |
| #8 | x |  |  |
| #9 | x |  |  |
| #10 | x |  |  |
| #11 |  | x |  |
| #12 |  |  | x |
| #13 |  |  | x |
| #14 |  |  | x |
| #15 | x |  |  |
| #16 | x |  |  |
| #17 |  | x |  |
| #18 |  | x |  |
| #19 |  | x |  |
| #20 |  | x |  |
| #21 |  |  | x |
| #22 | x |  |  |
| #23 | x |  |  |
| #24 |  | x |  |
| #25 | x |  |  |
| #26 | x |  |  |
| #27 |  | x |  |

## 6.1 Solution #1: User authentication and authorization of human user

### 6.1.1 Introduction

The solution addresses KI#1 and KI#2.

### 6.1.2 Solution details

The UDM/UDR based on operator policy, manages user authentication requirement information along with SUPI i.e., subscription data. If user authentication is required based on operator policy, the UDM/UDR also stores and manages the user identity profile which can contain user authentication and authorization data such as user identifier, applicable user type (i.e., human user or devices/applications. This is to allow restriction to use only allowed user identifier. Because in SA2 architecture assumptions in TR 23.700-32, it states, *‘When the user identifier applies to a human, only a single user identifier is active with a UE subscription at a given time and it is assumed that the specific user identifier is associated with all of the UE's traffic during the time that specific user identifier is active with the UE's subscription.’*), service information (list of services for which user identifier based user authentication is allowed), and user service access authorization information (e.g., can be a token signed by the operator for it to be verified by the service provider, whose claims can be up to normative details.

During registration, following a successful primary authentication, based on operator policy and UE subscription data fetched from the UDM, it indicates user authentication as required for the user identifier, the AMF/SEAF can initiate user authentication (e.g., like slice authentication). The UE if capable to support user authentication, it can send a related indication to the network along with the existing 5G security capabilities. In such as case, a user authentication is initiated by the network as described in the following steps, if the UE also supports user authentication.

1. The AMF/SEAF sends user identifier request in any NAS transport.
2. The UE sends the user identifier in response, it can also send user type set as ‘human user’.
3. The AMF/SEAF fetches the user authentication and authorization data from the UDM/UDR for the user identifier and user type. Based on the realm of user identifier, the user authentication and authorization data can be sent directly or via other function in the network (e.g., NSSAAF/AAA-P) to the related AAA-S/Application server/function to perform the necessary user authentication and authorization.
4. The user authentication specific messages can be exchanged between the UE and the network. The actual user identifier related user authentication and authorization data can be application level information whose generation and provisioning to UE and network is outside the scope of this present study. The user identifier can take a NAI form.
5. On a successful user authentication, the network AAA-S/Application server/function can send a successful result to the AMF/SEAF and the result is provided to the UE in a NAS transport.

According to S2-2407236, similar to the existing principles, AMF sends the identifier request to initiate user authentication, for the case of user authentication, it is based on user authentication requirement for specific services being managed in UDM as per operator policy and if UE is capable to support User authentication (which can be indicated by the UE to the network).

NOTE: TR 23.700-32 [2], Clause 4.1 Architectural Assumptions states that ‘The User Identifier and any subscription that it links to are assumed to be associated with the same PLMN (e.g. the operator that manages the User Identifier and the operator that manages the subscription is assumed to be the same).’. This clarifies that whatever the user identifier that is linked to SUPI) managed in PLMN for the purpose of user authentication will still be managed by the operator which is referred as operator policy in short.

### 6.1.3 Evaluation

The solution has the following impacts:

UE: The UE sends indication that it supports user authentication, user type and the user identifier to the network to allow further user authentication and authorization. This solution requires an interface between human user and NAS layer.

UDM/UDR: Based on operator policy manages user authentication requirement information along with SUPI i.e., subscription data. If user authentication is required, the UDM/UDR also stores and manages the user identity profile.

AMF: Following a successful primary authentication, if the UE is capable to support user authentication and based on user authentication requirement information fetched from UDM/UDR, the AMF can initiate user authentication similar to NSSAA procedure.

NSSAAF/AAA-P: The user authentication and authorization data may be sent via NSSAAF/AAA-P to the related Server to perform the necessary application-level user authentication and authorization similar to NSSAA procedure.

## 6.2 Solution #2: User Authentication and Authorization via AMF

### 6.2.1 Introduction

This solution addresses *"Key Issue #1: Authentication and Authorization of Human User ID"* reusingan EAP based mechanism similar to Network Slice Specific Authentication and Authorization (NSSAA), as described in TS 33.501 [3], clause 16.

The solution addresses the first requirement of Key Issue #2 in User privacy by reusing the mechanism defined in clause 6.4.6 of TS 33.501 [3].

### 6.2.2 Solution details



Figure 6.2.2.1-1: User authentication and authorization during Registration procedure

1. It is assumed that the User Id is linked to a UE subscription in the UDM/UDR, and the UE is pre-configured with User Id authorization information (e.g., authorized PLMNs, access type)

Editor’s Note: Whether the user ID is linked to a UE subscription in the UDM/UDR depends on SA2 conclusions.

1. The UE checks its authorization configuration to verify if the UE is allowed to use the User Id before sending a Registration Request message including the User Id to be activated.

To protect the privacy of the transmitted User ID the existing mechanism of protection of initial NAS message defined in clause 6.4.6 of TS 33.501 [3] is reused, with User ID is treated as a non cleartext IE.

1. The AMF checks subscription data and user profile for User Id from UDM/UDR to check whether User id is authorized for (i.e., linked to) the UE subscription. The AMF determines whether to initiate User Id authentication and authorization based on authorization data retrieved from UE context or UDM/UDR.

Editor’s Note: Whether authorization of the user ID is performed by UDM/UDR needs to be aligned with SA2.

1. If no valid authorization is found the AMF sends a Registration Accept with an indication that authentication and authorization of user id is pending, and step 4 is skipped. Otherwise, the AMF includes the authorization result information in the message. The UE refrains from requesting a network service (e.g., PDU Session, SMS) regardless of the access network, while the user id authentication and authorization is pending.
2. The AMF initiates the authentication and authorization of user id with authentication server (AAA) via an NSSAAF with User Id authentication functionality. Multiple messages (e.g., EAP) are exchanged between the UE and AAA via NSSAAF. The AMF receives from AAA an authentication and authorization result that may include a user id authorization data (e.g., validity scope such as time, location, access type, authorized PLMNs).
3. The AMF updates UDM/UDR with authorization data and indicate active state for the user id.

Editor’s Note: Whether and how the AMF updates the UDM/UDR and UE after authentication is in SA2's remit.

1. The AMF updates the UE in a UE Configuration Update (UCU) procedure providing the authorization result including an indication of successful activation of user id. Based on the authorization result, the UE can request to use a network service (e.g., setup a PDU Session with a S-NSSAI/DNN combination).

### 6.2.3 Evaluation

The solution addresses the requirement of Key Issue #1 and first requirement of Key Issue #2.

For the authentication and authorization of human user based on a User Id linked to a 3GPP subscription, the solution reuses similar principles as defined in NSSAA procedure in clause 16 of TS 33.501 [3]. The NSSAAF can be reused for the user authentication and authorization functionality.

For User Id privacy during communication between the UE and the network, the User Id transmitted in the Registration Request can be protected reusing the mechanism defined in clause 6.4.6 of TS 33.501 [3].

Human user interaction aspects are not in scope of this solution.

Editor’s Note: it is FFS to clarify how this solution addresses KI#1 without covering having human user interaction aspects.

## 6.3 Solution #3: User Authentication and Authorization over NAS

### 6.3.1 Introduction

This solution addresses *"Key Issue #1: Authentication and Authorization of Human User ID"* reusing an EAP based mechanism similar to Secondary Authentication as described in TS 33.501 [3], clause 11.

The solution addresses the first requirement of Key Issue #2 for User privacy by using existing NAS protection mechanism defined in TS 33.501 [3].

### 6.3.2 Solution details



Figure 6.3.2.2-1: User authentication and authorization during Registration procedure

1. It is assumed that the User Id is linked to a UE subscription in the UDM/UDR, and the UE is pre-configured with User Id authorization information (e.g., authorized S-NSSAI, DNN).

NOTE: Provisioning of user id credentials is assumed to be done by means outside the scope of this solution. It is assumed in this solution that user authorization is performed for services requiring PDU Session but not for services not requiring PDU session (e.g., LCS, SMS over NAS).

Editor’s Note: Whether the user ID is linked to a UE subscription in the UDM/UDR depends on SA2 conclusions.

1. The UE checks the configuration to verify if the UE is allowed to use the User Id before sending a PDU Session Establishment Request message including the User Id to be activated.
2. The SMF checks subscription data and user profile for User Id from UDM/UDR to check whether User id is authorized for (i.e., linked to) the UE subscription. The SMF determines whether to initiate User Id secondary authentication and authorization based on authorization data retrieved from UDM/UDR.

Editor’s Note: Whether authorization of the user ID is performed by UDM/UDR needs to be aligned with SA2.

1. If no valid authorization is found the SMF initiates the authentication and authorization of user id with authentication server (AAA) via UPF. Multiple messages (e.g., EAP) are exchanged between the UE and AAA via SMF. The SMF receives from AAA an authentication and authorization result that may include an authorization data including validity scope information (e.g., location, time). If a valid authorization is found this step and step 4 are skipped.
2. The SMF updates UDM/UDR with authorization data and indicate active state for the user id.

Editor’s Note: Whether and how the SMF updates the UDM/UDR and UE after authentication is in SA2's remit.

1. The SMF sends a PDU Session Establishment Accept message to the UE providing authorization result. Based on the authorization result, the UE can start exchanging traffic over the PDU Session.

### 6.3.3 Evaluation

The solution addresses the requirement of Key Issue #1 and first requirement of Key Issue #2.

For the authentication and authorization of human user based on a User Id linked to a 3GPP subscription, the solution reuses similar principles as defined in PDU Session secondary authentication in clause 11 of TS 33.501 [3]. The solution assumes that the requested User Id by the UE is linked to the UE subscription in UDM/UDR to be retrieved and checked by SMF during the procedure.

For User Id privacy during communication between the UE and the network, the he User Id is transmitted in a protected PDU Session Establishment request using existing NAS protection mechanism defined in TS 33.501 [3].

Human user interaction aspects are not in scope of this solution.

Editor’s Note: it is FFS to clarify how this solution addresses KI#1 without covering having human user interaction aspects.

## 6.4 Solution #4: Security protection of human user privacy

### 6.4.1 Introduction

This solution addresses KI#1 and KI#2.

The UIA can applies a mechanism similar like AKMA to authenticate the User Identity associated with the UE subscription.

### 6.4.2 Solution details

#### 6.4.2.1 KUIA deriving

Figure 6.4.2.1-1 provides a mechanism for user-ID authentication and UIA Anchor Key (KUIA) deriving.

The UIA-Anchor is the anchor function for the UIA service. The UIA-Anchor stores the KUIA and user-ID for UIA service, which is received from the AUSF after the UE completes a successful 5G primary authentication and user authentication. The UIA-Anchor also generates the key material to be used between the UE and the UIA Application Function (UIA-AF) and maintains User UIA contexts.



Figure 6.4.2.1-1: KUIA deriving

1. During the primary authentication, the AMF invokes the Nausf\_UEAuthentication service by sending a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF
2. The AUSF interacts with the UDM in order to fetch authentication information such as subscription credentials and the authentication method using the Nudm\_UEAuthentication\_Get Request service operation
3. The UDM indicates to the AUSF whether the UE has UIA subscriptions and whether the UIA Anchor key needs to be generated for the users. If the UE has UIA subscriptions, the UDM includes the user-ID list and UIA-AnchorID list in the Nudm\_UEAuthentication\_Get Response to AUSF.
4. During the primary authentication procedure, if the AUSF receives the user-ID list from UDM, the AUSF includes the user-ID list in the Hausf\_UEAuthentication\_Authenticate Response message to the AMF.

5a-b. After the successful user-ID authentication, the UE and the AUSF generate the KUIA from KAUSF and generate UIA-KID.

5c. The AUSF selects the UIA-Anchor function and sends a UIA Anchor Key Register request to the UIA-Anchor function with the user-ID, UIA-KID, KUIA.

5d. The UIA-Anchor function stores the received user-ID related material and sends a UIA Anchor Key Register response to the AUSF.

#### 6.4.2.2 User\_ID activation and privacy protection

Figure 6.4.2.2-1 provides a mechanism user-ID activation and privacy protection during the session establishment.



Figure 6.4.2.2-1: User-ID activation and privacy protection during the session establishment

1. The UE is registered andauthenticated.
2. User-ID#1 intends to use the UE. The UE establishes the PDU session using the user-ID#1.
3. The UE sends an UIA Active request to the AMF with the user-ID#1. The AMF forwards the request to the UDM.
4. The UE generates the KUIA and the UIA-KID from the KAUSF before initiating communication with an UIA-AF. When user-ID#1 intends to use the UE, the UE derives UIA Application Key (KUIAAF) from the KUIA..The UE uses KUIAAF to encrypt the user-ID. When the UE initiates communication with the UIA-AF, it includes the UIA-KID and the encrypted user-ID in the Application Session Establishment Request message. If the user-ID is not activated, the UE also indicates the service type to be “active” in the request.
5. If the UIA-AF does not have an active context associated with the UIA-KID, then the UIA-AF selects the UIA-Anchor Function, and sends a UIA ApplicationKey Get request to UIA-Anchor Function with the UIA-KID to request the KUIAAF for the UE. The UIA-AF also includes its identity (UIA\_AF\_ID) in the request.
6. The UIA-Anchor verifies whether the subscriber is authorized to use UIA based on the presence of the UE specific KUIA key identified by the UIA-KID.

If KUIA is present in UIA-Anchor Function, the UIA-Anchor Function derives the UIA Application Key (KUIAAF) from KUIA if it does not already have KUIAAF.

If KUIA is not present in the UIA-Anchor Function, the UIA-Anchor Function continues with step 11 with an error response.

1. The UIA-Anchor Function sends a UIA ApplicationKey Get response to the UIA-AF with KUIAAF, the KUIAAF expiration time and user-ID#1/SUPI/GPSI.
2. The UIA-AF uses the received KUIAAF to get the plain text of user-ID and the service type. If an “active” service type is received, the UIA-AF can check whether the user\_IDs received in step4 and step7 identify the same user of the UE.
3. If an “active” service type is received, the UIA-AF sends a Nuiaa\_UIA\_Active Request to the UIA-Anchor with user-ID#1 to be activated and UE identifier. The UIA-Anchor sends a Nudm\_UIA\_Active Request to the UDM with the user-ID#1 and UE identifier.
4. The UDM check whether the user\_IDs received in step3 and step9 identify the same user of the UE. If the two user-IDs are match and in the UE subscription, the UDM activates this user\_ID. If the two user\_IDs are not match, the user identifier activation fails.
5. The UDM sends Nudm\_UIA\_Active Response to the UIA-Anchor with the user\_ID#1 and activation result. The UIA-Anchor then sends Nuiaa\_UIA\_Active Response to the UE with the user\_ID#1 and activation result.
6. The UDM sends UIA active response to the AMF with the User\_ID#1 and activation result. The AMF forwards the response to the UE.
7. The UIA-AF sends the Application Session Establishment Response to the UE. If the information in step 7 or step 11 indicates failure, the UIA-AF rejects the Application Session Establishment by including a failure cause.

NOTE : If the AF is outside the operator domain, the NEF is needed between the UIA-AF and UIA-Anchor. The NEF enables and authorizes the external AF assessing UIA service and forwards the messages between UIA-AF and UIA-Anchor. The NEF will not send SUPI to the UIA-AF outside the operator domain. The NEF also performs the UIA-Anchor selection.

Editor’s Note: The involved network functions (UIA-Anchor, UIA AF) are to be aligned with SA2.

#### 6.4.2.3 Derivation of User-ID related material

When deriving the specific user-ID related key materials through the Key derivation function, the SUPI of the UE is replaced by the user-ID.

**KUIA derivation function:**

When deriving a KUIA from KAUSF, the following parameters can be used to form the input S to the KDF:

- FC = 0x8C; (just an example for FC value)

- P0 = "UIA"; (just an example for P0 value)

- L0 = length of "UIA"; (i.e. 0x00 0x03)

- P1 = User\_Id;

- L1 = length of User\_Id.

The input key KEY shall be the KAUSF.

**KUIAAF derivation function:**

When deriving a KUIAAF from KUIA, the following parameters can be used to form the input S to the KDF:

- FC = 0x8E; (just an example for FC value)

- P0 = UIA\_AF\_ID;

- L0 = length of UIA\_AF\_ID

The input key KEY shall be KUIA.

UIA\_AF\_ID is constructed as follows:

UIA\_AF\_ID = FQDN of the AF || Ua\* security protocol identifier, where the Ua\* is the interface protocol between UE and UIA\_AF.

### 6.4.3 Evaluation

This solution addresses KI#1 and KI#2 on authentication and privacy protection of human user ID, by introducing a mechanism similar like AKMA. This solution also ensures that the UIA-AF is authorized to receive information about user identity information.

A UIA Anchor function is introduced to store the UIA related materials (e.g. KUIA, user-ID) for UIA service. The UIA materials are generated per user. The UIA Anchor can be a separate NF or co-located with other NFs (e.g. AAnF).

The UDM performs activation check for the user-ID. The user-ID transmitted between the UE and the network is protected by NAS security established by UE subscription.

The UIA-AF can perform the application layer authorization for the specific user to use the user-ID. The UIA-AF is authorized by successfully acquiring the UIA application key KUIAAF form the UIA Anchor Function.

## 6.5 Solution #5: User authentication and authorization

### 6.5.1 Introduction

This solution addresses the key issue #1.

The solution reuses the NSSAA procedure TS 33.501 [3] and adapts it to authenticate and authorize a human user using the UE. It allows restriction to user through authorization outcome.

### 6.5.1 Solution details

Assuming the human user with a user identifier (UID) is using a UE with a 3GPP subscription identified by the UE’s SUPI to access services via the 5GS. Before authentication of the UID, the Primary authentication for the UE needs to be performed. It is also assumed that the networks slice identified by S-NSSAI is supposed to provide the service for the UE and the user.

With reference to the figure 16.2-1 in TS 33.501 [3], the user identity authentication and authorization procedure is described as follows:

1. UE sends a Registration Request which may include the UID.

NOTE 1: How the user triggers the UE to send the registration request is out of scope.

2. For an initial Registration Request, the AMF shall invoke Primary authentication as described in TS 33.501 [3]. For a subsequent Registration Request, the Primary authentication may be skipped if the UE has already been authenticated and the AMF has valid security context.

3. The AMF shall determine whether user identifier authentication and authorization (UIAA) procedure is required, based on information stored locally or from UDM. If yes, the AMF triggers the UIAA procedure. The UIAA procedure can be adapted from NSSAA procedure as shown in 16.3 in TS 33.501 [3] with modification as follows:

NOTE 2: the step “3-x” is corresponding to the step “x” in clause 16.3 in TS 33.501 [3]

3-1: The AMF may trigger the start of the UIAA procedure. The AMF may determine to trigger the UIAA with the corresponding AAA server based on the UE’s subscription information.

3-2: The AMF may request the EAP ID for EAP authentication.

3-3: The UE provides the EAP ID to the AMF. The EAP ID is included in the EAP message which is transparent to the AMF. The UE may provide UID to the AMF as well.

NOTE 3: UID may be the same as or different from EAP ID. In case the UID is different from the EAP ID, the UE and the AAA server must know the mapping between the UID and the EAP ID. The UID format is out of scope of this solution.

3-4: The AMF sends the GPSI, EAP ID and the UID if available to the NSSAAF.

3-5: 5. The NSSAAF forwards the message to the AAA-S directly or through AAA-P if available.

3-6 to 3-11: EAP-messages are exchanged with the UE. One or more than one iterations of these steps may occur.

3-12. EAP authentication completes. The EAP-Success/Failure message is delivered to the NSSAAF/AAA-P along with GPSI and UID. The message may include any restriction information imposed to the UID, e.g. tiers of services/QoS, service duration etc.

NOTE 4: Restriction information that the AAA-S can provide follows conclusions in the TR 23.700-32 [2].

3-13. The NSSAAF sends the UIAA result (Success/Failure), GPSI, UID to the AMF.

3-14. The AMF transmits the UIAA result to the UE.

3-15. Based on the UIAA result, the AMF initiates the UE Configuration Update procedure.

NOTE 5: Whether the UE configuration update is initiated by the AMF initiates and the updated content follows the conclusions in the TR 23.700-32 [2].

### 6.5.3 Evaluation

This solution addresses the key issue #1.

This solution reuses the NSSAA procedure and adapts it to authenticate and authorize a user identifier with few changes highlighted as follows:

* UE: includes the user identifier in the registration request.
* AMF: triggers the user identifier authentication procedure, e.g., based on subscription information at UDM
* AAA: exchanges messages with the UE assisted by the AMF to authenticate and authorize the user identifier.

This solution does not address an interface between the user and the UE’s NAS signaling.

Editor’s Note: evaluation is ffs on how this solution addresses KI#1 without having human user interaction addressed.

## 6.6 Solution #6: Human User authentication of through NAS procedure

### 6.6.1 Introduction

This solution addresses key issue #1: "Authentication and Authorization of Human User ID". The solution focuses on the authentication procedure.

### 6.6.2 Solution Details

The user ID is sent by the UE in the Registration Request message. When the AMF receives the Registration Request message, the AMF first performs the registration procedure for the UE. The user authentication procedure will run after the Primary authentication.



Figure 6.6.2-1: User Authentication Procedure for human user

1. The UE that the user is using may or may not have registered to the 5GC.

2. A user logs onto the UE.

3. The UE sends the Registration Request message to the AMF. If the UE registered to the 5GC before, then the 5G-GUTI is included, otherwise, the SUCI is included. Additionally, the user ID will be carried in the Registration Request message.

4. The AMF continues the Registration Procedure for the UE. If the UE registration fails, the AMF will terminate the procedure the same way as in TS 23.502[4]. If the UE registration completes, the UE runs the user authentication procedure.

5. After completing the UE registration procedure, the AMF starts to run user authentication procedure.

6-10. Comparing to primary authentication procedure define in TS 33.501[3], only EAP method is used for user authentication. AUSF and UDM are reused for user authentication procedure.

NOTE: The primary authentication and the user authentication are separate procedures. There will be no effect on the UE primary authentication method from the user authentication process. In this solution, the specific user authentication method is based on EAP-TLS.

The user authentication procedure based on EAP-TLS method applies to the cases where a credential is preconfigured in the UE and the network for user authentication. The credential associated with the user identifier is preconfigured in the UE before user activation. The credential is also preconfigured in the 5GC (UDM) with the associated user identifier.

11. The AMF sends the Registration Accept message to the UE. The Registration Accept message further contains the authentication result of the user authentication.

12. If EAP-Success is received, the UE will allow the user to use the UE. Otherwise, the UE will drop the user.

It is assumed that, the UE is pre-configured with User Id authorization information (e.g., authorized PLMNs, access type), and the User Id is linked to a UE subscription in the UDM/UDR. The AMF checks subscription data and user profile for User Id from UDM/UDR to check whether User id is linked to the UE subscription.

### 6.6.3 Evaluation

This solution addresses KI#1.

The solution uses the EAP framework so that various authentication methods (e.g, EAP-TLS) can be supported.

Editor’s Note: evaluation is ffs on how this solution addresses KI#1 without having human user interaction addressed.

## 6.7 Solution #7: Authentication and Authorization of Human User ID

### 6.7.1 Introduction

This solution addresses the Key Issue #1 (as defined in clause 5.1) .

This solution proposes to support the authentication and authorization of human user based on a User identifier linked to a 3GPP subscription with the follow assumptions:

- The UE takes role of EAP client, and the SMF takes role of EAP authenticator, and the AUSF takes role of EAP server.

- An authentication data associated with a User identifier is stored in User Profile of UDM/UDR and is used by AUSF to authenticate a human user.

NOTE : How to pre-configure the authentication data associated with the User identifier is out of this solution. It is assumed in this solution that user authorization is performed for services requiring PDU Session but not for services requiring no PDU session (e.g., LCS, SMS over NAS).

Editor’s Note: Whether the user profile is stored in the UDM/UDR is in SA2's remit.

Editor’s Note: Whether user input is required for user authentication FFS. Without user Input, how to ensure user is actually using the device.

### 6.7.2 Solution Details



Figure 6.7.2-1 authentication and authorization of human user based on a User identifier.

1. The UE/5G-RG registers with the network performing primary authentication.

2. The UE send a PDU Session Establishment or Modification Request to SMF via AMF, which contains a User identifier.

Editor’s Note: This solution shall be aligned with the procedure agreed by SA2.

3. Upon receiving the PDU Session Establishment or Modification Request message, the SMF shall obtains the subscription data of the UE and the profile of the User identifier from the UDM. The SMF shall checks the subscription data whether the UE is allowed to use the requested User Identity service, and check the profile of the User identifier whether the User identifier links to the subscription data of the UE. If not allowed and/or not linked, the SMF shall notify the UE that the requested User Identity services is invalid and shall execute the existing PDU Session Establishment or Modification procedure as specified in clause TS 23.502 [4] instead of the rest of the current procedure.

NOTE 1: The failure of authorization verification for User Identity service shall not prevent UE to establish a default PDU Session as existing procedure as specified in clause TS 23.502 [4].

4. The SMF shall trigger EAP Authentication of the human user by sending a EAP authentication request message to AUSF. This message contains the User identifier received in step 3.

Editor’s Note: What’s the relationship of the user authentication and the UE secondary authentication (if required) is FFS.

5. The AUSF shall get the authentication data associated with the User identifier from the UDM or UDR.

6. The AUSF and the UE (human user) shall exchange EAP messages via SMF to complete mutual authentication based on the authentication data.

NOTE 2: The EAP methods and the details of the authentication data is out of this solution. The EAP message are transmit over NAS message between UE and the SMF.

7. After the successful completion of the authentication procedure, the AUSF shall send EAP Success message to the SMF. This message contains the User identifier.

8. The SMF shall store the authentication and authorization result of the human user and add the User identifier to the SM context of the UE mark as authorized by requested service.

9. The SMF may notify the authentication and authorization result of the human user to UDM and/or specific NF where stored the User profile. The SMF then may request the session policy associate with the human from PCF as specified by SA2.

Editor’s Note: Whether the SMF adds the user identifier to the SM context, and whether the SMF requests the session policy from the PCF is in SA2 remit.

10. The SMF shall perform rest of the PDU Session Establishment or Modification procedure.

11. The SMF send a NAS SM PDU Session Establishment or Modification Accept message to the UE via the AMF. This message shall include EAP success message to be sent to the UE (human user).

### 6.7.4 Evaluation

TBD

## 6.8 Solution #8: User authentication with preconfigured credential

### 6.8.1 Introduction

This solution addresses Key Issue #1 on Authentication and Authorization of Human User ID. Specifically, it addresses the requirements for authentication of human user based on a user identifier linked to a 3GPP subscription. The solution applies to the cases where a credential is preconfigured in the UE and the network for user authentication.

### 6.8.2 Solution details

#### 6.8.2.1 Description

According to the requirements in KI#1, users (human user or non-3GPP device) are authenticated based on the identifier of a human user using a UE for using operator or non-operator deployed services, i.e. the user identifier needs to be sent to the network. The solution assumes the following:

NOTE: User authentication hereafter refers to both the authentication of human.

- The user or non-3GPP device identifier is sent from the UE to the network during user activation procedure which takes place after the UE registered into the network.

- There is a User Identity Profile (UIP) containing user identifier(s) and the linked subscription(s), which is maintained by the HPLMN of the linked subscription(s). It can be used for determining whether and how to initiate user authentication. The profile is stored in a User Identity Management Function (UIMF) which can be collocated with an existing NF in HPLMN.

- There is a User Authentication and Authorization Function (UAAF) deployed by the home operator and dedicated to user authentication, which can be a standalone NF or collocated with an existing NF. When authentication is performed by 5GC, the UAAF takes the role of authentication server. When authentication is performed by a third-party service provider, the UAAF undertakes AAA protocol interworking with the third-party AAA server.

- User identifier can be made available to the UE before user activation, e.g. through input of human user which is out of 3GPP scope.

- The credential associated with the user is preconfigured in the UE before user activation. The credential is also preconfigured in the third-party AAA server or the UAAF or stored in the UIP with the associated user.

- EAP framework specified in IETF RFC 3748 [5] may be used for user authentication. The specific method for user authentication can be negotiated between the UE and the network based on UE capability and authentication policy configured in the network.

#### 6.8.2.2 User authentication procedure with the UAAF deployed by operator

If the pair of user identifier and the corresponding credential is created by the operator, the user authentication is performed between the UE and UAAF. The AMF takes the role of the EAP authenticator and communicates with the UAAF, which takes the role of the authentication server.



Figure 6.8.2.2: User authentication procedure with UAAF deployed by operator

0. The UE successfully registered into the network via registration procedure.

1. When a human user logs in the UE with a user identifier, the UE sends the User Activation Request containing user identifier in a NAS message, as well as the UE capability supporting user authentication.

2. Upon receiving user activation request from the UE containing the user identifier, the AMF retrieves the UIP associated with the user identifier from the UIMF.

3. The UIMF or AMF determines whether and how user authentication shall be triggered based on the following information in the UIP:

- If the SUPI of the UE matches one of the SUPIs indicating the linked 3GPP subscriptions, the UIMF/AMF may determine to trigger user authentication. Otherwise, the UIMF/AMF determines to reject the user activation request.

- If there is no existing successful user authentication result or the status of the user is not activated yet, the UIMF/AMF may determine to trigger user authentication. Otherwise, the UIMF/AMF determines not to trigger user authentication.

- If there is authentication policy indicating authentication method(s), the UIMF/AMF checks whether the UE capability supports the indicated authentication method(s), and then determines whether and how to trigger user authentication.

4. If user authentication needs to be triggered and authentication method (e.g. EAP method) determined, the AMF sends a User Authentication Request to the UE via NAS message to request the User ID for EAP authentication (EAP-ID). The AMF also indicates the specific authentication method (e.g. EAP-TLS) to the UE.

5. The UE provides the user identifier as the EAP-ID via EAP-Response in the User Authentication Response towards the AMF. The EAP-Response is protected with the credential associated with the user identifier.

6. The AMF forwards the EAP-Response to the UAAF in an Nuaaf\_UserAuth\_Authenticate Request message and indicates the EAP method.

7. The UAAF verifies the EAP-Response using the preconfigured credential associated with the user identifier. The UAAF may interact with the UIMF for retrieving the corresponding credential if stored in the UIP.

8. Optionally more than one iteration for EAP-message exchange between the UE and the UAAF is performed.

9. EAP authentication completes. An EAP-Success/Failure message is sent by the UAAF to the AMF in the Nuaaf\_UserAuth\_Authenticate Response message. In case of success, the UAAF may send the authentication result to the UIMF to be included in the UIP, indicating the user activation status.

10. Based on the result of user authentication (Success/Failure), the AMF returns User Activation Response to the UE via NAS message. If user authentication is successful, the user is activated on the UE, and subsequent procedures on service usage can be performed for the human user via the UE.

NOTE 1: The involved network functions (UIMF, UAAF) and procedure for user acitivation need to be aligned with the architecture and procedure in TR 23.700-32 [2].

NOTE 2: Whether user input on the UE can be verified by the network depends on the EAP method applied by the network for user authentication.

#### 6.8.2.3 User authentication procedure with the AAA-S deployed by third party

If the pair of user identifier and the corresponding credential is created by a third-party service provider, the user authentication is performed between a UE and an AAA server (AAA-S) owned by the third party. The AMF performs the role of the EAP Authenticator and communicates with the AAA-S via the UAAF. The UAAF undertakes AAA protocol interworking with the AAA-S.

Steps 0-6 refer to steps 0-6 in clause 6.8.2.2.

7. If the UAAF does not have the credential associated with the user identifier, or cannot retrieving the corresponding credential from the UIP, it forwards the EAP-Response/Identity message to the AAA-S via the AAA-P, routed based on the realm portion of the user identifier.

8~12. EAP-messages are exchanged with the UE. One or more than one iterations of these steps may occur.

13. EAP authentication completes. An EAP-Success/Failure message is delivered to the UAAF.

14. The UAAF forwards the EAP-Success/Failure message to the AMF via Nuaaf\_UserAuth\_Authenticate Response message. In case of success, the UAAF may send the authentication result to the UIMF to be included in the UIP, indicating the user activation status.

Step 15 refers to step 10 in clause 6.8.2.2.



Figure 6.8.2.3: User authentication procedure with AAA server deployed by third party.

### 6.8.3 Evaluation

This solution applies EAP framework to fulfill the requirements in KI#1 on authentication of human user based on a user identifier linked to a 3GPP subscription.

The solution only applies to the case where the credential used for user authentication is pre-configured on the UE.

The solution can be used in both the case where the pair of user identifier and the corresponding credential is provided by the operator and the case where the pair of user identifier and the corresponding credential is provided by a third-party service provider. In the former case, whether the user input of user identifier and credential on the UE can be verified by the network depends on the EAP method applied by the network.

The solution is integrated in the user activation procedure which relies on architecture design. Hence most of the impacts on the UE and the network in this solution are inherited from the related procedure. The impacts identified due to user authentication requirements are as below.

Editor’s Note: whether this solution requires an interface between user and NAS layer is FFS.

Impact on the UE:

- To receive and handle user authentication result in User Activation Response from the AMF

Impact on the AMF:

- To interact with the UAAF for user authentication and indicate the EAP method

- To interact with the UE to request user identifier for EAP authentication and indicate the EAP method

- To associate SUPI of the UE with the user identifier sent by the UE

- To include user authentication result to the UE in User Activation Response

Impact on the UAAF:

- To interact with the AMF for user authentication and receive EAP method

- To retrieve the credential associated with the user identifier from the UIMF

- To verifie the EAP-Response by using the credential associated with the user identifier

Impact on the UIMF:

- To provide the credential associated with the user identifier to the UAAF

6.9 Solution #9: User Plane Based Human User ID Authentication and Authorization

6.9.1 Introduction

This solution addresses the requirements identified in key issue #1 (Authentication and Authorization of Human User ID). It is proposed to user plane based authentication and authorization.

6.9.2 Solution details

The figure 6.9.2-1 presents the high-level authentication and authorization architecture. The Portal is a trusted entity from the HPLMN perspective, and can e.g. be managed by the HPLMN operator or a trusted partner. The User Identifier is authenticated and authorized by the UIP server. The UIP server is an Application Function (AF) under control of the HPLMN operator.



Figure 6.9.2-1: High-level authentication and authorization architecture

The figure 6.9.2-2 shows a flow for authentication and authorization of the User Identifier in the UIP server via the UE's UIP client.



Figure 6.9.2-2: User ID authentication over user plane

The preparation step 0. is assumed to be performed in advance, and out of 3GPP scope.

0. Preparation steps on application layer. The admin user of the subscription logs in at the Portal over user plane. The Portal, UIP server and the admin user create the credentials to be used for authentication of a user, potentially different from the admin user, and download the UE part of the credentials to the UE. For example, the credentials could be a user password chosen by the admin user which could be combined with a certificate provisioned at the UE, e.g. in combination with downloading an application to the UE. Alternatively, the credentials could be a user certificate that is locked with a password or biometric verification locally at the UE. The preparation step also links the credentials to the SUPI, e.g. the admin user indicates that the user is allowed to use the subscription associated with the SUPI. By using credentials in the authentication, which can be directly user provided data such as password or can be accessible with only user provided data such as password or biometric data, it is ensured that the later authentication step actually authenticates the user and not only the UE. An operator can also require control of ID or passport before the operator controlled entities (portal, UIP server) generate the credentials, if desired or required.

Steps 1-5 are performed using a user plane connection to a special DNN that gives the user access to the UIP server. Observe that the registration uses the SUPI and primary authentication is performed between UE and network based on the associated long term key.

1. [Locally at the UE] User login to UE and the UIP client, possibly including a local authentication of the user. This step is out of 3GPP scope.

2. [Application layer over 3GPP connection] UIP client requests user login from the UIP server.

3. [Application layer over 3GPP connection] Authentication between user, UE/UIP client and UIP server is performed, using the credentials established in step 0. The UIP server also authorizes the user and checks which 5GC subscription (identified by the GPSI) the user is using. The UIP server can use the IP translation API to learn the GPSI.

4. [3GPP scope studied in TS 23.700-32] After successful authentication of the user, procedures as studied in TR 23.700-32 [2] are performed.

5. [Application layer over 3GPP connection] The UIP server sends the response to the UE/UIP client.

After Step 5, the UE and user have full user plane connectivity.

This solution proposes that Steps 2-5 are performed after activation of AS security. Furthermore, additional security mechanisms on the user plane can be enabled for steps 3 and 5, e.g. TLS with server-side certificates.

The user ID is confidentiality protected over the air interface, because the user ID is sent over the user plane after establishment of AS security. This protection requires to have the confidentiality activation mandatory for the user plane connection to a special DNN that gives the user access to the UIP server. Since the UIP server is inside the HPLMN domain, the communication between UPF and UIP server can be protected by a mechanism chosen by the operator. The confidentiality protection for the communication between UE/UIP client and UIP server can also be done in the application layer by using TLS.

6.9.3 Evaluation

TBD.

Editor’s Note: Whether the interaction at application layer (steps 2,3,5) are in 3GPP scope is FFS.

6.10 Solution #10: Human User ID authentication and authorization

### 6.10.1 Introduction

This solution addresses KI#1 Authentication and Authorization of Human User ID and proposes an overall procedure to achieve these security goals.

### 6.10.2 Solution details

A diagram of a user

Description automatically generated with medium confidence

Figure 6.10.2-1: Human User ID authentication and authorization

The procedure is described in reference to figure 6.10.1-1, as follows:

* In step 1, the User accesses the UE e.g., unlocks ME and SIM.

NOTE 1: Step 1 is outside of 3GPP scope.

* In Step 2, the UE performs initial registration and primary authentication with the 5GC.
* In Step 3, based on the type of services requested/ to be provided and the subscription details, the 5GC (e.g., UDM) can trigger a User Identification procedure by sending a User Identity Request to the UE.
* In Step 4, Upon receiving the User Identity Request, the User may be prompted (e.g., through the user interface) to provide its User Identity and authentication information. If the User approves the request, the User Identity (and optionally) authentication information (e.g., User identifier, user biometric data) is sent protected to the 5GC. If the authentication is local, the UE only returns the User Identifier or User Profile. User profile is a generic identifier identifying the type of user and the type of services required by the user. A user can opt for an incognito profile for privacy protection.

NOTE 2: In case a 3rd party User Identity Management Server (UIMS) is used, the User Identity may be protected based on security materials shared between the UE and the 3rd party UIMS, which are outside of the 3GPP scope.

* In Step 5, the 5GC processes the protected User Identity (and optionally) authentication information received in step 4, authenticating the User based on whether the User Identity is associated with the subscription, as stored at the 5GC (e.g., UDR). In particular, the subscription is associated with one or more user identities and associated authentication token(s) (e.g., a password) which is/are used to authenticate the user(s) using the UE. Alternatively, If the User Identity is managed by a 3rd party UIMS, the User identification and authentication is performed by the 3rd party UIMS and the identification and authentication result is then provided to the 5GC, which may subsequently check whether the identified and authenticated User is associated with a user subscription, as stored in the 5GC (e.g., UDR).
* In Step 6, based on whether the User Identity authentication is successful, and the type of services requested by the user, the 5GC (e.g., PCF) determines whether the User is authorized for such services.

### 6.10.3 Evaluation

This solution addresses KI#1 Authentication and Authorization of Human User ID.

It provides a framework enabling the identification, authentication and authorization of a Human User ID based on either local authentication, 5GC authentication or a 3rd party UIMS authentication.

This solution requires an interface between the user and NAS layer.

6.11 Solution #11: Re-using existing mechanisms for user privacy

6.11.1 Introduction

This solution addresses the requirements identified in key issue #2 (User Privacy).

It is proposed to re-use existing mechanism to protect user identifier during the communication between the UE and the network, including the procedures for user authentication and service access, and to protect User Identity Profile information during the exposure of User Identity Profile information by the network to entities outside operator domain, to prevent privacy attacks (e.g., trackability, linkability, disclosure).

6.11.2 Solution details

For communication between the UE and the network, including the procedures for user authentication and service access, AS security as described in clause 6.5 and 6.6 of TS 33.501[3] is proposed to be used.

For the exposure, the existing security mechanism for network exposure as described in clause 12 of TS 33.501 [3] are proposed to be used.

For the scenario where the UE moves and the user identifier needs to be sent again, this solution proposes that the user identifier is sent after establishment of AS security.

6.11.3 Evaluation

Editor’s Note: Evaluation is FFS.

6.12 Solution #12: authorization of non-3GPP devices behind 5G-RG

6.12.1 Introduction

This solution addresses Key Issue #3 on the authorization of non-3GPP devices behind 5G-RG. It is based on the authentication of FN-RG in clause 7B.3 of TS 33.501 [3], with following changes: a) it is the 5G-RG, not W-AGF, which registers non-3GPP devices to the 5GC; and b) it adds authorization check that the non-3GPP device is under the control of an RG which has been successfully authenticated by 5GC. This ensures that an RG can only represent a non-3GPP device allowed by the RG subscription.

6.12.2 Solution details

A black screen with white text

Description automatically generated

Figure 6.12.2-1. authorization of non-3GPP devices behind 5G-RG

1. A layer-2 (L2) connection is established between the non-3GPP device and the 5G-RG using local authentication (e.g., WPA personal).

2. The 5G-RG sends an AAA message to the W-AGF to indicate that a device with a non-3GPP device identifier has been successfully authenticated locally.

NOTE 1 : The identifier of the non-3GPP device is defined by BBF or CableLabs and is out of scope of 3GPP.

3. The W-AGF sends back a confirmation AAA message to the RG.

NOTE 2 : The AAA messages used between the 5G-RG and the W-AGF in steps 2-3 are defined by BBF or CableLabs and out of scope of 3GPP.

4. The W-AGF shall perform initial registration on behalf of the non-3GPP device. The W-AGF shall generate a Registration Request message and send it to the AMF over N2. The Registration Request message contains the SUCI of the non-3GPP device and the SUCI of the 5G-RG. The N2 message contains an indication that the RG has authenticated the non-3GPP device.

NOTE 3: the SUCI of non-3GPP device is included in the N2 message to be consistent with clause 7B.3 of TS 33.501 [3] where the SUCI of FN-RG is included in the N2 message.

5. The AMF shall select an AUSF based on the received SUCI. The AMF shall send a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF. It contains the SUCI of the non-3GPP device, the SUCI of the 5G-RG, and the SN-name. It also contains the authenticated indication generated by the W-AGF.

6. The AUSF shall send a Nudm\_UEAuthentication\_Get Request to the UDM. It contains the SUCI of the non-3GPP device, the SUCI of the 5G-RG, the SN-name, and the authenticated indication.

7. The UDM shall invoke the SIDF and maps the SUCIs to the SUPIs. The UDM shall verify that the 5G-RG has been successfully authenticated and the non-3GPP device is under the control of the RG based on the subscription profiles of the 5G-RG. The UDM decides the authentication by the home network is not required for the non-3GPP device and the non-3GPP device has been authorized.

8. The UDM shall send a Nudm\_UEAuthentication\_Get Response to the AUSF. It contains the SUPI of the non-3GPP device and an indication that authentication by the home network is not required.

9. After checking the indication set by the UDM, The AUSF shall not perform authentication and shall send a Nausf\_UEAuthentication\_Authenticate Response to the AMF. It contains the SUPI of the non-3GPP device and the indication that authentication by the home network is not required set by the UDM.

This response from AUSF indicates that authentication is not required, and no KSEAF is included.

10. After checking the indication to make sure that the authentication by the home network is not required, the AMF shall estabilish the NAS security for the non-3GPP device between AMF and W-AGF with NULL encryption and NULL integrity protection.

11. The AMF shall send Registration Accept message to the W-AGF. This message contains 5G-GUTI and other parameters.

12. The W-AGF shall send a Registration Complete message back to the AMF. The W-AGF shall store the 5G-GUTI for use in later NAS procedures.

13. The W-AGF and the 5G-RG may establish a PDU session for the non-3GPP device. This is defined by CableLabs and BBF and is out the scope of 3GPP.

6.12.3 Evaluation

This solution is not consistent with the architecture assumption in TR 23.700-32 [X] that non-3GPP devices is not registered to the 5GC.

## 6.13 Solution #13: Authentication and Authorization procedure of N3D behind gateway UE or 5G-RG

### 6.13.1 Introduction

This solution addresses the Key Issue #3 (as defined in clause 5.3).

This solution proposes to support the authentication and authorization of one or more Non-3GPP Device behind gateway UE or 5G-RG by enhancing the EAP based authentication procedure by an external DN-AAA server as specified in clause 11.1 of TS 33.501 [3]. It is assumed there is a Non-3GPP device profile stored in Core network, e.g. UDM.

Editor’s Note: Whether this solution alignment with SA2 conclusions is ffs.

6.13.2 Solution details

#### 6.13.2.1 Authentication Procedure

The authentication and authorization procedure of Non-3GPP Device behind gateway UE or 5G-RG as follow:



Figure 6.13.2.1-1 Authentication and Authorization procedure of Non-3GPP Device behind gateway UE or 5G-RG

0. The UE/5G-RG registers with the network performing primary authentication.

1. The Non-3GPP Device and the UE/5G-RG successfully established direct connection.

NOTE 1: How to establish direct connection is out of 3GPP scope.

2. During direct connection establishment procedure, the UE/5G-RG identify the Non-3GPP Device and confirm its Non-3GPP Device identifier.

NOTE 2: How to identify a Non-3GPP Device based will be specified by SA2.

3. The UE/5G-RG send a PDU Session Establishment or Modification Request to SMF via AMF, which contains the Non-3GPP Device identifier confirmed in step 2.

4. Upon receiving the PDU Session Establishment or Modification Request message, the SMF shall obtains the subscription data of the UE/5G-RG and the profile of the Non-3GPP Device from the UDM. The SMF shall checks the subscription data whether the secondary authentication for UE/5G-RG as specified in clause 11.1 of TS 33.501 [3] is required, and whether the UE/5G-RG is allowed to provide current service, and check the profile of the Non-3GPP Deivce whether the Non-3GPP Device identifier links to the subscription data of the UE or 5G-RG. If not allowed and/or not linked, the SMF will reject UE/5G-RG’s request via SM-NAS signalling and skip rest of the procedure.

NOTE 3: The SMF needs to perform the secondary authentication for UE/5G-RG if required.

5. The SMF shall trigger EAP Authentication of the Non-3GPP Device to obtain authorization from an external DN-AAA server by sending a EAP authentication request message, which contains the Non-3GPP Device identifier.

6. The DN-AAA server and the UE shall exchange EAP messages via the UPF and UE/5G-RG, as required by the EAP method. In addition, it may send additional authorization information as defined in TS 23.501 clause 5.6.6.

7. After the successful completion of the authentication procedure, DN-AAA server shall send EAP Success message to the SMF. This message contains the Non-3GPP Device identifier and a MSK (optional).

8. The SMF shall store the authentication and authorization result of Non-3GPP Device and add the Non-3GPP Device identifier to the SM context of the UE/5G-RG and mark as authorized by requested service.

9. The SMF may notify the authentication and authorization result of Non-3GPP Device to UDM and/or specific NF where store the profile of the Non-3GPP Deivce. The SMF then may request the session policy associate with the Non-3GPP Device from PCF.

Editor’s Note: What the Non-3GPP Device profile contains and where the Non-3GPP Device Profile is stored is FFS and will be defined by SA2.

10. The SMF shall perform rest of the PDU Session Establishment or Modification procedure.

11. The SMF send a NAS SM PDU Session Establishment or Modification Accept message to the UE/5G-RG via the AMF. This message shall include EAP success message to be sent to the UE/5G-RG and the Non-3GPP Device. The SMF shall also include a MSK (if received in step 7) in NAS SM message.

12. The UE/5G-RG shall store the authentication and authorization result of the Non-3GPP Device to do some operation like access control, e.g. restrict the number of devices activated simultaneously. The UE/5G-RG shall store the MSK and associated Non-3GPP Device identifier if received in NAS SM message.

13. The UE/5G-RG may Establish/Re-establish the security protection for direct connection with the Non-3GPP Device based on the received MSK. After successful complete the step 3-12, the UE/5G-RG start to forward the traffic from the Non-3GPP Device to network.

#### 6.13.2.2 Re-Authentication procedure



Figure 6.13.2.2-1 Re-Authentication procedure of Non-3GPP Device behind gateway UE or 5G-RG

0. The UE/5G-RG registers with the network performing primary authentication.

1. The authentication and authorization procedure of Non-3GPP Device was successfully executed.

2a. The SMF decides to initiate Re-Authentication procedure of the Non-3GPP Device.

2b-1. The DN AAA server decides to initiate Re-Authentication of the Non-3GPP Device.

2b-2. The DN AAA shall send a Re-Authentication request to the SMF via UPF. The Re-authentication request contains the Non-3GPP Device identifier and other parameters as specified in clause 11.1.3 of TS 33.501 [3].

3-4. The SMF shall send an EAP Request/Identity message to the UE/5G-RG, which contain the Non-3GPP Device identifier. Upon received this message, the UE/5G-RG stop forwarding the traffic of the Non-3GPP Device to network, and responds an EAP Response/Identity message to the SMF, which contain the Non-3GPP Device identifier.

5-13. Execute the same operation as step 5-13 in clause 6.13.2.

#### 6.13.2.3 Authentication and Authorization revocation

At any time, the DN-AAA server may revoke the authentication and authorization for a PDU Session associated with the Non-3GPP Device, and according to the request from the DN-AAA server, the SMF may modify or release the PDU Session associated with the Non-3GPP Device.

### 6.13.4 Evaluation

TBD

## 6.14 Solution #14: Authentication and authorization of non-3GPP devices

### 6.14.1 Introduction

The solution addresses KI#3.

### 6.14.2 Solution details

The UDM/UDR based on operator policy, stores and manages along with UE/5G-RG subscription, the user identity profile which can contain user authentication and authorization data such as user identifier(s), along with applicable user type (ie., human user or devices/applications). This is to allow restriction to use only allowed user identifier(s). Because in SA2 architecture assumptions in TR 23.700-32, it states, *‘When the user identifier applies to a human, only a single user identifier is active with a UE subscription at a given time and it is assumed that the specific user identifier is associated with all of the UE's traffic during the time that specific user identifier is active with the UE's subscription.’*). For the case of non-3GPP devices behind UE or 5G-RG, authentication can be performed by UE or 5G-RG (outside of 3GPP scope) based on SA2 conclusions in TR 23.700-32 for KI#4.

For authorization check of non-3GPP devices behind UE/5G-RG, the related user identifier and type can be verified by the AMF/SMF against the information stored in the UDM/UDR (such as user identifier, and user type ‘device’, service information) while fetching the user identity profile during the service/PDU session request. Where the user type indicates, as non-3GPP device. If it matches, the authorization is considered as successful for non-3GPP device.

NOTE 1: According to TR 23.700-32 Clause 8.4, the conclusion states, ‘For non-3GPP devices requiring QoS differentiation, Device Identifiers and their corresponding QoS/Policies associated with a UE/5G-RG subscription are provisioned into the UDR by the AF’. So it is evident that, to identify the non-3GPP device if the linked UE/5G-RG has subscription it is sufficient. The non-3GPP device need not have any subscription on its own with the PLMN.

NOTE 2: According to TR 23.700-32 Clause 5.4 in Key Issue #4, the User Identifiers means the identifiers of the devices behind gateway UE or 5G-RG.

### 6.14.3 Evaluation

This solution proposes that the 5GC does not authenticate the non-3GPP device, but still authorizes it. The solution has the following impacts:

Non-3GPP device: Need to send its identifier and type to the network, to let the network to verify if it is authorized to access the service requested related to linked UE/5G-RG subscription being managed in the UDM/UDR.

AMF/SMF: Checks the authorization of the non-3GPP device by verifying its identifier, type, and service information again the information stored and fetched from the UDM/UDR.

UDM/UDR: Need to store the non-3GPP device information along with the linked UE/5G-RG subscription information.

## 6.15 Solution #15: Authentication of user behind the UE

### 6.15.1 Introduction

This solution is targeted to KI#1

### 6.15.2 Solution details

### 6.15.2.1 Concept

The main concept of the solution is to authenticate the user via user identifier at the AUSF/UDM. In the authentication process, both user owned secret/credential and UE owner secret/credential should be used together to authenticate the user.

Please refer to the diagram to understand the same:



Figure 6.15.2.1-1: User, UE and 5GC secret/credential ownership

As shown in the above figure, the user bought the subscription from the operator, and the operator provides the user ID and a changeable PIN or one-time password. The user gets this information or changes this information via the operator-provided portal or other means.

The user-A and the subscribers (B) agreed for the user-A to use the UE-B for a time being. Therefore, the network provisions the TimeBoundCredential and User ID at the UE/USIM-B. So now the user-A and network know the following shared secret related to the user:

* User Id,
* PIN or one-time password

And the UE and network know the shared secret.

* User Id,
* TimeBoundCredential (any shared secret that can be used for a limited time period or a limited number of times)

The user provides a user ID and PIN to the UE, and now the network can authenticate the user via these shared secrets (PIN and TimeBoundCredential). In this way, user A and UE-B are both bound in the authentication process.

### 6.15.2.2 Solution flow



Figure 6.15.2.2-1: user authentication

1. UE-B is authenticated and registered in the network as defined in TS 33.501 [3] and TS 23502 [4].
2. User-A bought the subscription from the operator, and the operator provides the user ID and a changeable PIN or one-time password to User-A. The user gets this information via the operator-provided portal (outside the scope of 3GPP). User-A is also linked with UE#B in the subscription data.
3. UE is provisioned with credentials (out of scope of 3GPP).

Steps 1 and 3 are repeated for every UE where the user wants to be linked.

1. The user logs in to the UE-B and provides a user ID and PIN.

NOTE 1 : How users log in to the UE-B is outside the scope of 3GPP. Maybe it can be achieved via an operator-provided app.

1. Once the User-A logs in to the UE-B, the UE-B initiates the NAS registration request, where the existing 5G-GUTI of the UE-B is provided as is, and additionally, the user ID is also provided as an additional IE.
2. If the AMF decides to perform user authentication, the AMF initiates user authentication. For this, AMF sends Nausf\_UEAuthentication\_Authentication Req with SUPI of the UE-B and User ID of the User-A to AUSF.
3. The AUSF sends the Nudm\_UEAuthentication\_Authentication\_Get request to UDM with SUPI and the user ID. Based on the subscription data, the UDM authorizes that User A can use UE-B. After successful authorization, the UDM provides the TimeBoundCredential and PIN related to user-A to the AUSF.
4. The AUSF sends an EAP challenge packet to UE, which contains a TNonce value and a Message Authentication Code 1 (MAC1) derived by using the user key derived using the TimeBoundCredential, PIN, and User ID.
5. The UE derives an expected MAC1 (XMAC1) of TNonce using a user key derived in a similar fashion and compares XMAC1 with the received MAC1. If they match, the network is authenticated by the UE.

The UE generates a UNonce and derives a MAC2 using the user key, considering UNonce and TNonce.

NOTE: every challenge must be validated, and the UE should provide the response. This is similar to reauthentication challenge by the network.

1. The UE responds with an EAP Challenge containing UNonce, TNonce, and MAC2.
2. The AUSF derives an expected MAC2 (XMAC2) using the user key and with UNonce and TNonce. Compares XMAC2 with the received MAC2. If they match, the UE is authenticated by the AUSF. As mentioned in the step 4, user provides user id and PIN to UE and that is used for authentication for user along with UE credentials.

NOTE: PIN is not transferred over the 3GPP signalling.

1. The AUSF sends an EAP-SUCCESS message to UE.

NOTE 2 : User ID privacy is covered in Solution #18.

NOTE: User 1 sharing the id and password to user 2 is not addressed in this solution.

### 6.15.3 Evaluation

This solution covers KI#1.

UE:

* User provides credential to UE. Then UE sends user credentials to the network.
* UE receives a challenge from the network for user credentials. UE calculates the response and sends the response to the network.

AUSF/UDM:

* Generate a challenge vector for the user authentication.
* Validate the UE response.

NOTE: The user interface between UE and User is not within the within the scope of this solution.

Editor’s Note: it is FFF to clarify that how this solution addresses KI#1 without having human user interaction.

## 6.16 Solution #16: User Authentication and Authorization

### 6.16.1 Introduction

This solution assumes following:

* 5GC plays the role of Identity provider, responsible for identification, authentication and authorization of a (human) user behind a 5G UE.
* A 3rd party which provides services to the users requires an Identity Provider it trusts to validate the identity of (human) users.

To address possible scenarios, the solution proposes to introduce following logical network function to handle user identification, authentication and authorization:

**- User Authentication Function (UAF):** This NF is responsible for selecting and interfacing with UIDF (User Information Database Function) for triggering User Authentication.

In addition, UE subscription data, which is stored in UDM/UDR, may be enhanced to include the Allowed User Identities and/or User Domain Names.

### 6.16.2 Solution details

#### 6.16.2.1 User Initiated procedure

This solution proposes to introduce a for user authentication and authorization procedure where the UE initiates User Authentication Procedure requesting identity certificate.



**Figure 6.16.2.1-1: Control plane based User Authentication and Authorization procedure**

1. The UE is pre-configured with credentials for accessing 3GPP network, bio-metric verification of the user(s) and optionally credentials for accessing the service. The primary authentication is performed as described in clause 6.1 in 3GPP TS 33.501 [3] and the UE is authenticated with the 3GPP core network. A User (e.g. a human user) triggers the device access using implementation specific methods (e.g., by tapping on an option in an App).
2. The UE sends a User Authentication Request to the AMF. This message may include User ID or a temporary Session-ID, and optionally result/token of biometric user-verification. The UE performs the authenticity verification of the user and includes the user ID once it is successfully verified. Further step 1 to 5 could be new NAS message or re-use existing NAS message.

NOTE: How the UE authenticates the User and which user ID is used to initiate the session is based on mechanism outside the scope of 3GPP.

1. Upon receiving the User Authentication Request from the UE, the AMF forwards the User Authentication Request to the UAF.
2. Upon receiving the User Authentication Request, UAF may verify the user credential. i.e., the UAF checks the binding information from the UDM and verifies the user credentials.

Post successful validation, UAF generates a short-term identity certificate. The certificate indicates that User behind the UE has been verified by the network, and hence signed by a CA, and is valid for a certain duration.

1. The UAF sends the user authentication response message to the AMF. This message includes the certificate for the verified user. The message may also be sent directly to the UE over, e.g. data-path
2. Upon receiving the user authentication response message from the UAF, the AMF forwards the user authentication response message to the UE.
3. The UE sends the Application Session Establishment Request to the AF for obtaining the service. This message includes the UE-ID, certificate and the service ID.
4. Upon receiving the Application Session Establishment Request, the AF verifies the certificate provided by the UE and confirms the real user and provides the service. The AF is in possession of valid credentials (public key) to verify the certificate provided by the UAF/CA.

#### 6.16.2.2 Network Initiated procedure

This solution proposes to introduce a procedure for user authentication and authorization where the 3rd party entity or the AF retrieves the user authentication results from the 5GC network. The UDM performs the user authentication based on the request from the AF, where the UDM initiates user authentication and provides the User-ID.



**Figure 6.16.2.2-2: User Authentication and Authorization procedure**

1. The UE is pre-configured with credentials for accessing 3GPP network, bio-metric verification of the user(s) and optionally credentials for services. The primary authentication is performed as described in clause 6.1 in 3GPP TS 33.501 [3] and the UE is authenticated with the 3GPP core network.
2. The UE sends the Application Session Establishment Request to the AF (for e.g. as in AKMA). This message includes the UE ID and the user ID.
3. Based on the received Application Session Establishment Request from the UE, the AF determines that it needs to ensure that the user is indeed the one he is claiming to be (i.e. User-ID), before granting access to application. The AF sends the User Authentication Request to the UDM via NEF. This message includes UE ID and user ID.
4. Upon receiving the User Authentication Request, the UDM sends the User Authentication request to the AMF. This message includes UE ID and a user ID/ a session ID/ an anonymous user ID. The User Authentication message may also include the AF ID. If the UDM is provided with a session ID or an anonymous user ID, then UE ID (SUPI/GPSI) is needed for retrieving the corresponding user ID.
5. Upon receiving the User Authentication Request, the AMF identifies the UE based on the UE ID and sends the User Authentication request to the UE. This message includes UE ID and user ID. The User Authentication message may also include the AF ID.
6. The UE performs the biometric verification (face images and the fingerprints of the user using a mechanism outside the scope of 3GPP) the stored credentials and generates the authentication result.

NOTE: How the UE authenticates the User and which user ID is used to initiate the session and which authentication method is selected is application based and not in the scope of 3GPP.

1. The UE sends the User Authentication Response to the AMF over, e.g. a NAS message. The message includes the result of user-authentication generated by the UE during the verification process.
2. The AMF forwards the User Authentication Response to the UDM. The message includes the result of user-authentication provided by the UE.
3. Upon receiving the User Authentication Response, the UDM initiates the user verification from network side. The UDM may verify the locally stored user information with the authentication result and ensures whether the user is allowed for accessing the service.
4. Once the verification at the UDM is successful, the UDM sends the User Authentication Response to the AF via NEF. This message includes the result of user authentication. Upon receiving the User Authentication Response from the UDM (via NEF) and verifying the user authentication result, the AF sends the Application Session Establishment Response to the UE.

### 6.16.3 Evaluation

This solution proposes to partially address Key Issue #1 on Authentication and Authorization of Human User ID. This solution proposes two approaches (User initiated and network-initiated procedure) for the network to verify the user credentials associated with user of the UE.

For the user-initiated procedure, based on the user authentication request from the UE, the network generates a certificate or is provisioned with the required certificate using out of band mechanism and this certificate indicates that user credentials of the user behind the UE has been verified by the network, and hence signed by a CA, and is valid for a certain duration after successful verification of the user credential authenticity. Further this solution requires the network to store the user authentication credentials e.g., if biometric or password-based authentication is used the network need to store the biometric or password. Further the solution requires interface between human user to NAS layer.

For the network-initiated procedure, the network triggers the UE to perform an application-based validation for the user (e.g., either by performing the biometric verification or by providing user ID and password-based mechanism to verify the real user behind the UE). Upon checking locally stored information and authentication result provided by the UE, network confirms user credentials associated with user of the UE and provides access to the service.

Impacts:

* UE: Requires pre-provisioning of authenticator’s credentials. Further, it requires UE to share the auth result or user credential over the NAS messages.
* Network: Network needs to store binding information of user credential(s).

## 6.17 Solution #17: Solution for exposure privacy issue

### 6.17.1 Introduction

This solution is targeted to KI#2

### 6.17.2 Solution details

The solution believes there are two kinds of privacy issues associated with user profile exposure.

1: Exposure of User Profile Information

2: Exposure of linked UE subscription information associated with the User Identifier

#### 6.17.2.1 Exposure of user profile information

Following rules would be applied:

* Each user profile is assigned a GPSI or external ID, where the GPSI or external ID can be specific to the AF (similar to a subscription-specific GPSI/external ID for a subscriber). It is the responsibility of NEF to map GPSI/external ID to user ID or vice versa.
* The user owning the user-profile can provide permission to the exposure of user-profile specific information. User profile will be like a subscription data for the user owning the user profile. For this, we can reuse the consent framework defined in TS 33.501 [3] annex V and extend this annex V for user profile as well. This can be decided in the normative phase.
* The NEF also has a policy to ensure only public information about the user profile will be exposed to AFs, which is similar to UE subscription exposure.

#### 6.17.2.2a Exposure of linked UE subscription information associated with User Identifier

If user-profile is linked to the UE’s subscription, based on the AF request, the 5GC can expose the linked subscription information, e.g., if User A is registered to 5GC via UE-B, it means User A is using UE-B. Therefore, exposing certain information about the user may lead to a privacy issue of the UE as well. For example,



* User-A is ok to provide the location to AF1 But UE-B is not Ok to provide the location to AF1. Respective data in the UDM/NF contains the respective consent/permission flags. (Step 1,2)
* AF requests NEF and asks for User-A linking (linked subscription) information. And NEF provides the response with User-A is linked with UE-B. (Step 4)
* Then AF requests NEF and asks for the user's location. NEF provides a User-A location (i.e., UE-B location).

Editor’s Note: Assuming user location as subscriber location is FFS.

* AF determines the UE-B location even if AF is not allowed to get UE-B location information. (Step 5)

Therefore, the following rules would be applied:

* If the AF requests 5GC to provide the user location, then 5GC checks the privacy profile (similar to the consent flag) of UE as defined in TS 23.273 [6] and the permission flag of the user as defined in the user profile (Step 5D). When both UE and the user are allowed to share the location, then only the user’s location should be determined and shared with AF.

#### 6.17.2.2b Exposure of linked UE subscription information associated with User Identifier to AMF/SMF (internal NFs)

**Use case 1: Secondary authentication is enabled:**

The user profile contains few IE/properties, like which Slice1/DNN1 (internet) is allowed to the user. Subscription data also contains Subscriber Slice1/DNN1/Slice2/DNN2 information. When the user registers via the UE, then AMF/SMF needs the subscription data to provide the authorization. If AMF/SMF is provided with merge data of subscriber and user, the AMF will receive Slice1/DNN1.

It is possible that user A logs into the UE-B and is able to access enterprise DNN on behalf of subscriber B because secondary authentication is still a legacy method that is based on SUPI.

**Use case 2: Secondary authentication is disabled:**

The user profile contains few IE/properties, like which slice1/DNN1 is allowed to the user. Subscription data also contains Subscriber Slice2/DNN2 information. When the user registers via the UE, then AMF/SMF needs the subscription data to provide the authorization. If AMF/SMF is provided with merge data of subscriber and user, the AMF will receive Slice1/DNN1.

It is possible that user-A logs into the UE-B and is able to access enterprise Slice1/DNN1 on behalf of subscriber-.Lets try to understand this with the below figure.



Therefore, the following rules would be applied:

* The UE subscription defines what services are allowed to be used by the user. i.e., if the user can use a certain service, like slice/DNN.  Therefore, subscription data contains additional IEs example, Allowed Slice/DNN, Allowed User Id, Allowed Services (e.g. SMS, Call) etc.
* These rules should be applied, and only relevant subscriptions related to User +Subscriber should be provided to AMF/SMF (or any requesting node). So that AMF/SMF can restrict the user accessing the Slice1/DNN1 or allow or reject services.

### 6.17.3 Evaluation

This solution provides solution for requirements mentioned in the KI2.

Use profile data exposure: UDM/NF must check both the permissions, user, and subscriber while exposing the sensitive information of the user.

Subscription data enhancement to include additional flags to allow/restrict the user accessing the service and provide this information to AMF/SMF/NFc to apply restrictions on the user accessing the service via the UE.

GPSI or external ID should be assigned to the user profile to perverse the privacy of the user.

Editor’s Note: further evaluation is FFS.

## 6.18 Solution #18: User privacy during the connection with 5GC

### 6.18.1 Introduction

This solution is targeted to KI#2, requirement 1.

### 6.18.2 Solution details



Figure 6.18.2.1-1: User Id privacy during the connection

1. UE-B is authenticated and registered in the network as defined in TS 33.501 [3] and TS 23.502 [4].
2. User-A is attached/linked to UE#B and provides a user ID.
3. Optionally, UE-B matches the User-A ID stored in UE.
4. UE-B sends a NAS registration request with the 5G-GUTI of the subscriber (UE-B) and the User ID (A) of the user.

NOTE: If the AMF finds that the 5G-GUTI is unknown, then the AMF initiates primary authentication of the subscriber, and then, after successful completion of primary authentication, the below steps are performed.

1. AMF/SMF sends a Nausf\_UEAuthentication\_Authenticate Request with the SUPI of the subscriber and the User Id of the user to the AUSF selected for the UE.
2. User authentication is performed.
3. Once user authentication is successful, then AUSF provides authentication result to the AMF.
4. Based on the successful authentication, the AMF generates a new 5G-GUTI that includes user(A) and UE(B) information and provides it to UE-B. UE-B uses this new 5G-GUTI for further communication.

A similar procedure can be executed if user authentication is performed at the PDU session level, where user Id can be provided at the PDU session request, and accordingly, AMF/SMF performs the authentication.

#### 6.18.2.1 Mobility or attaching to other access scenarios:

When User-A attaches to UE-B, User-A is the owner of the UE for the duration. All communication belongs to User-A. Now assume that:

* Scenario 1: Now if User A is not using the UE-B for some time, the UE-B goes into an idle state and then moves to a connected state.
* Scenario 2: User-A + UE-B tries to connect to non-3GPP access.

In both scenarios, UE-B will send the registration request with only integrity protection, not ciphered IE. Therefore, a user ID in plain text cannot be sent in this registration request. As explained in step 8, a new GUTI will be created based on User ID (A) and UE-B information. AMF will be able to identify the registration request is for User A on UE-B, and accordingly, AMF can select relevant subscriptions and apply services.

If GUTI is not known to the AMF, the AMF retrieves the SUCI and performs the subscriber authentication and registration as per TS 33.501 and TS 23.502, and then the user will be authenticated and registered as explained in 6.18.2.

### 6.18.3 Evaluation

The solution addresses the KI2 for privacy and fulfil the requirement

*The 5G system shall provide mechanisms for mitigating privacy attacks (e.g. trackability, linkability) against user identifier during the communication between the UE and the network, including the procedures for user authentication and service access.*

Solution provides new GUTI, which is generated by AMF based on user ID and UE subscription details.

AMF provides the GUTI to UE, and UEs use this GUTI for further communication with the network.

## 6.19 Solution #19: User privacy protection

### 6.19.1 Introduction

This solution addresses the key issue #2.

The solution protects a user identifier (UID) used in 3GPP system by replacing it with the concealed version, i.e. user identifier concealed (UIC). Since UID is not in the realm of 3GPP systems, the mapping between the UID and UIC is out of scope of 3GPP system, i.e. UIC and how UID is mapped to UIC is transparent to the 3GPP systems.

In addition, the mapping between UIC and UID is not fixed and changed from time to time to avoid the user being tracked or linked.

NOTE 1: the UID is concealed by the UE, e.g., through hashing or a mapping table. The AAA knows the mapping between the UID and its concealed version UIC. The 3GPP system is provisioned with the UIC and the linkage between the UIC and the subscription.

NOTE 2: the UIC can be included in the PDU session request by the UE. It is not necessary for the 3GPP system to know the UID.

### 6.19.2 Solution details

A user authentication procedure is exemplified below to illustrate how to use UIC, instead of UID to protect user privacy. It is notable that the authentication procedure is made generic as much as possible to accommodate different authentication methods (this solution is not meant to address authentication procedure).

The exemplified user identity authentication and authorization (UIAA) procedure with user privacy protection is as follows:

1.The UE sends a Registration Request to the AMF.

2. The AMF triggers the UIAA procedure.

3: The AMF sends the AAA-Server the UIAA message with GPSI included.

NOTE: The UID (but not UIC) is transparent to the AMF/UDM. The UIC and the linkage between the UIC and the UE subscription is provisioned in the AMF/UDM.

4. The AAA-S and the UE perform user authentication and authorization with respect to the user, e.g. the user is identified as UIC between AAA-S and the UE. However, the UIC is transparent to the AMF. There can be multiple message exchanges between UE and AAA-S, depending on authentication method used. The authentication method is out of scope of 3GPP.

5. The AAA-S sends the authentication results to AMF, which stores the result identifying the user by UIC, the concealed version of UID. The UIC should be changed for every authentication to avoid being tracked or linked to previous authentication.

6. The AMF sends registration accept to the UE.



Figure 6.19.2-1 illustration of user privacy protection in a user authentication procedure

### 6.19.3 Evaluation

This solution addresses the key issue #2.

This solution provides user privacy protection by using a concealed user identifier (UIC) in place of the real user identifier (UID). The privacy of UID is a end-to-end protected between the UE and the AAA-Server. The 3GPP system uses the protected version, i.e., the UIC in the 3GPP procedures. Therefore, the 3GPP system does not need to provide an additional protection mechanism. The UIC may be updated to the 3GPP system from time to time to avoid the user being tracked or linked.

## 6.20 Solution #20: privacy protection for user ID over the air

### 6.20.1 Introduction

This solution addresses key issue #2: "User privacy". The solution focuses on privacy protection over the air. This solution does not cover the privacy issue for non-3GPP devices behind one gateway UE or 5G-RG.

### 6.20.2 Details

The user ID sent over the air from the UE to the AMF is protected by NAS security. The user ID can be added to a NAS message when the NAS security is activated, e.g. in the ciphered part of the Registration Request message.

### 6.20.3 Evaluation

This solution fulfils the first requirement in KI#2.

This solution requires activation of NAS confidentiality and a new IE for the user ID.

## 6.21 Solution #21: A&A of non-3GPP devices behind UE or 5G-RG based on secondary authentication

### 6.21.1 Introduction

This solution addresses the key issue #3.

The solution reuses the secondary authentication procedure in TS 33.501 [3] and adapts it to authenticate and authorize a non-3GPP device behind a UE or 5G-RG.

### 6.21.1 Solution details

Assuming the non-3GPP device behind a UE is identified by the Device IDentifier (DID) linked to a UE, with a 3GPP subscription identified by the UE’s SUPI/GPSI, to access services via the 5GS. Before authentication of the DID, the Primary authentication for the UE needs to be performed.

NOTE 1: the DID is assigned by the non-3GPP system. The assignment is out of scope of 3GPP.

With reference to the figure 11.1.2-1 in TS 33.501 [3], the DID authentication and authorization procedure is described as follows:

1-3. UE is registered to the network after Primary authentication and security context is established as in TS 33.501 [3].

4-7. The UE sends a PDU session establishment request to the network as in TS 33.501 [3]. The PDU session establishment request may include the DID of the non-3GPP device similar to the procedure in the TS 33.501 [3] (as in the step 10 of the clause 11.1.2).

8. The H-SMF initiates the device authentication procedure for the PDU session as in TS 33.501 [3]. The SMF may trigger the device authentication based on the UE subscription information.

NOTE 2: as in the TS 33.501 [3], the SMF can trigger based on UE subscription information or the DID sent from the UE.

9-13. The EAP authentication starts and is completed after multiple rounds of message exchanges between the UE and the DN, as in TS 33.501 [3].

The EAP Response/Identity message sent to the DN may include the GPSI of the UE.

14. After the successful completion of the authentication procedure, DN AAA server shall send an EAP Success message to the H-SMF, along with the GPSI and the DID. The message may include any restriction information imposed to the DID, e.g. tiers of services/QoS, service duration etc.

The DN AAA server can identify the DID based on the GPSI and/or the EAP ID. The DID may be the same as the EAP ID or may be different from the EAP ID. If the DID is different from the EAP ID, the DN AAA server should be provisioned with the mapping between the DID and the EAP ID.

15. This completes the authentication procedure at the SMF. The SMF may save the DN-specific ID and DNN (or DN's AAA server ID if available) in a list for successful authentication/authorization between UE and an SMF. Alternatively, the SMF may update the list in UDM. The UE (and the non-3GPP device) is identified by the GPSI and DID.

If the authorization is successful, PDU Session Establishment proceeds as described in TS 33.501 [3].

16a-19 The UE-requested PDU Session Establishment authentication/authorization by a DN-AAA server proceeds further as described in TS 33.501 [3].

### 6.21.3 Evaluation

This solution addresses the key issue #3.

The solution reuses the secondary authentication procedure and adapts it to authenticate and authorize a non-3GPP device behind a UE or 5G-RG. It uses the EAP framework so that various authentication methods can be supported. The DID needs to be configured if it is the same as EAP ID.

## 6.22 Solution #22: User authentication with credentials derived by AUSF

### 6.22.1 Introduction

This solution addresses Key Issue #1 on Authentication and Authorization of Human User ID. Specifically, it addresses the requirements for authentication of human user based on a user identifier linked to a 3GPP subscription. The solution applies to the cases where no credential is preconfigured in the UE and the network for user authentication.

### 6.22.2 Solution details

#### 6.22.2.1 Description

According to the requirements in KI#1, users (human user) are authenticated based on the identifier of a human user using a UE for using operator or non-operator deployed services, i.e. the user identifier needs to be sent to the network. The solution assumes the following:

NOTE: User authentication hereafter refers to both the authentication of human user.

- The user identifier is sent from the UE to the network during user activation procedure which takes place after the UE registered into the network.

- There is a User Identity Profile (UIP) containing user identifier(s) (User ID) and linked subscription(s), which is maintained by the HPLMN of the linked subscription(s). It can be used for determining whether and how to initiate user authentication. The profile is stored in a User Identity Management Function (UIMF) which can be collocated with an existing NF in HPLMN.

- Each user is also provisioned with a PIN/one-time passowrd from the network via e.g. operator portal. The pair {User ID, PIN/one-time password} is stored as part of UIP in the UIMF. The PIN/password has a validity time. The user needs to request a new PIN/one-time password when the available PIN/one-time password expires. The secrecy of the PIN/one-time password needs to be ensured by each user that it is not known by any other users.

- There is a User Authentication and Authorization Function (UAAF) deployed by the home operator and dedicated to user authentication, which can be a standalone NF or collocated with an existing NF.

- User identifier can be made available to the UE before user activation, e.g. through input of human user which is out of 3GPP scope.

- There is no credential preconfigured in the UE and UAAF to associate with the user identifier.

#### 6.22.2.2 User activation procedure with the AUSF and UIMF

For human users, if there is no credential preconfigured in the UE and the network for user authentication, the credential can be derived based on KAUSF generated during primary authentication.

0. When the UE registers to the network, primary authentication is successfully performed between the UE and the network, during which the key KAUSF is derived and stored in both the UE and AUSF.

After UE registration, the first human user logs in (User-1) connects to the UE. The user activation procedure starts.

1. The UE sends a User Activation Request in a NAS message, which contains the user identifier of User-1, UE capability supporting user authentication, and optionally an indication of credential absence.

2. If the credential absence indication is sent from the UE, the AMF sends a Nausf\_UserActivation\_Authenticate Request message to the AUSF, which includes the UE’s SUPI, user identifier and UE capability supporting user authentication.

3. Upon receiving the user identifier, the AUSF sends a Nuimf\_UserActivation\_UIP Request message to the UIMF for retrieving the UIP information of User-1.

4. Based on UIP information of User-1, the UIMF determines whether and how to perform user authentication procedure. For example, when the user authentication policy stored in the UIP indicates that user authentication credential shall be generated during user activation procedure, or when the credential associated with the user identifier is not available in the UIP, the UIMF determines that the user authentication method is to generate KUIA for user authentication.

5. If the UIMF determines to trigger user authentication, it returns a Nuimf\_UserActivation\_UIP Response message to the AUSF with the PIN/password of User-1 and the selected user authentication method, which indicates that KUIA needs to be derived for user authentication.

6. If the AUSF received the user authentication method indicating that KUIA needs to be derived, the AUSF derives KUIA from KAUSF of the UE. The AUSF associates KUIA with the UE’s SUPI.

7. Based on the received user identifier of User-1 and the received PIN/password of User-1, the AUSF further derives KUSER-1 from KUIA.

8. The AUSF sends the derived KUSER-1 associated with User-1 to the UIMF. The UIMF includes the KUSER-1 in the UIP associated with User-1.

9. The AUSF returns Nausf\_UserActivation\_Authenticate Response to the AMF with the user authentication method, which indicates that KUIA needs to be derived.

10. The AMF forwards the user authentication method to the UE via User Activation Response in a NAS message.

11. Upon receiving the user authentication method indicating that KUIA needs to be derived, the UE derives KUIA from KAUSF in the same way as the AUSF. The UE associates KUIA with its SUPI.

12. The UE further derives KUSER-1 from KUIA based on the user identifier of User-1. The UE associates KUSER-1 with User-1.

13. The UE initiates User Authentication for User-1 towards the UAAF over application layer, which is protected using the derived KUSER-1 (see clause 6.22.2.4).



Figure 6.22.2.2: User activation procedure with AUSF and UIMF

After the first human user logged in, other human users (e.g. User-2, .., User-n) log in one by one.

14~18. User activation procedure is repeated for each of the logged-in users or connected devices, with the user identifier of User-n.

19. If the AUSF received the user authentication method indicating KUIA needs to be derived and KUIA has already been derived, the AUSF derives KUSER-n from KUIA for User-n.

20. The AUSF sends the derived KUSER-n associated with User-n to the UIMF. The UIMF includes the KUSER-n in the UIP of User-n.

21~22. The user authentication method is delivered to the UE from the AUSF via the AMF.

23. Upon receiving the user authentication method indicating that KUIA needs to be derived and KUIA has already been derived, the UE derives KUSER-n from KUIA for User-n.

24. The UE initiates User Authentication for User-n towards the UAAF over application layer, which is protected using the derived KUSER-n (see clause 6.22.2.4).

#### 6.22.2.3 Key hierarchy for user authentication with derived credential



Figure 6.22.2.3: Key hierarchy for user authentication with derived credential

Based on the procedure in clause 6.22.2.2, KAUSF is used as the root key in the hierarchy of key derivation. KUIA is derived from KAUSF by the UE and AUSF to be used as the intermediate key for all users on the UE. Based on the intermediate key KUIA, the key KUSER can be derived by the UE and the AUSF to be used as the user authentication credential for each specific user on the UE.

#### 6.22.2.4 User authentication procedure with the UAAF

After the UE derives KUSER-n during user activation procedure, the UE is able to initiate user authentication for User-n towards the UAAF.

1. The UE sends a User Authentication Request message to the UAAF (e.g. over application layer) which is protected with the KUSER-n. The message includes the user identifier of User-n.

2. Upon receiving the User Authentication Request, the UAAF sends an Authentication Key Request to the UIMF, which contains the user or device identifier of User-n.

3. The UIMF retrieves the UIP based on the received user or device identifier, from which KUSER-n can be retrieved. If the User Authentication Result associated with User-n is stored in the UIP, the Authentication Result is also retrieved.

4. The UIMF returns the retrieved KUSER-n or Authentication Result to the UAAF.

5. If the UAAF receives Authentication Result, the UAAF proceeds to step #8.

If the UAAF receives KUSER-n, the UAAF authenticates User-n using the KUSER-n received from the UIMF.

6. The UAAF sends the Authentication Result of User-n to the UIMM.

7. The UIMF stores the User Authentication Result associated with User-n in the UIP.

NOTE: Steps 6 and 7 are optional and to be aligned with architectural procedure in 23.700-32 [2].

8. The UAAF sends the User Authentication Response with the Authentication Result of User-n to the UE.



Figure 6.22.2.4: User authentication procedure with the UAAF

#### 6.22.2.5 Derivation of KUIA and KUSER

When deriving a KUIA from KAUSF, the following parameters are used to form the input S to the KDF:

- FC = TBD;

- P0 = "UIA";

- L0 = length of "UIA";

- P1 = SUPI;

- L1 = length of SUPI.

The input key KEY is the KAUSF.

When deriving a KUSER from KUIA, the following parameters are used to form the input S to the KDF:

- FC = TBD;

- P0 = User identifier;

- L0 = length of user identifier;

- P1 = PIN/one-time password;

- L1 = length of PIN/one-time password.

The input key KEY is the KUIA.

With the PIN/one-time password associated with the User ID being an input to the KUSER derivation function, the AUSF needs to retrieve the PIN/one-time password from the UIMF for deriving KUSER. If e.g. a dishonest User-A inputs a User ID of User-B, the KUSER derived by the AUSF is computed with PIN-B, while the KUSER derived by the UE is not computed with PIN-B as it is unknown to User-A. With asymmetric KUSER derived by the UE and network, the user authentication will fail, hence the dishonest user is not able to log in the network via successful user authentication.

### 6.22.3 Evaluation

This solution uses key derivation for generating user authentication credential to fulfill the requirements in KI#1 on authentication of human user based on a user identifier linked to a 3GPP subscription. The details on how the user is authenticated using the UE after user credential derivation are not explained.

The solution applies to the case where the credential used for user authentication is not available in the UE. As the user authentication credential is derived from UE credential rather than being input by the user, the trustworthiness of the credential is ensured.

The solution can be used in both the case where the user identifier is provided by the operator and the case where the user identifier is provided by a third-party service provider. In the former case, the user input of user identifier on the UE can be verified by the network. In the latter case, the the user input of user identifier on the UE cannot be verified by the network but needs to be verified by the third party.

The solution is integrated in the user activation procedure which relies on architectural design. Hence many of the impacts on the UE and the network in this solution are inherited from the related procedure in TR 23.700-32 [2]. The impacts identified due to user authentication requirements are as below.

Impact on the UE:

- To derive KUIA and KUSER and associate the derived KUSER with user identifier

- To interact with the UAAF for user authentication

Impact on the AMF:

- To interact with the AUSF for user authentication and receive the selected user authentication method

- To indicate the selected user authentication method to the UE

Impact on the AUSF:

- To interact with the AMF for user authentication and indicate the selected user authentication method

- To indicate with the UIMF to determine the user authentication method and store KUSER

- To derive KUIA and KUSER

Impact on the UIMF:

- To provide information to the AUSF to determine the user authentication method

- To receive KUSER from the AUSF

- To provide KUSER to the UAAF

Impact on the UAAF:

- To retrieve KUSER from the UIMF

- To interact with the UE for user authentication

## 6.23 Solution #23: User Authentication with EAP-PSK

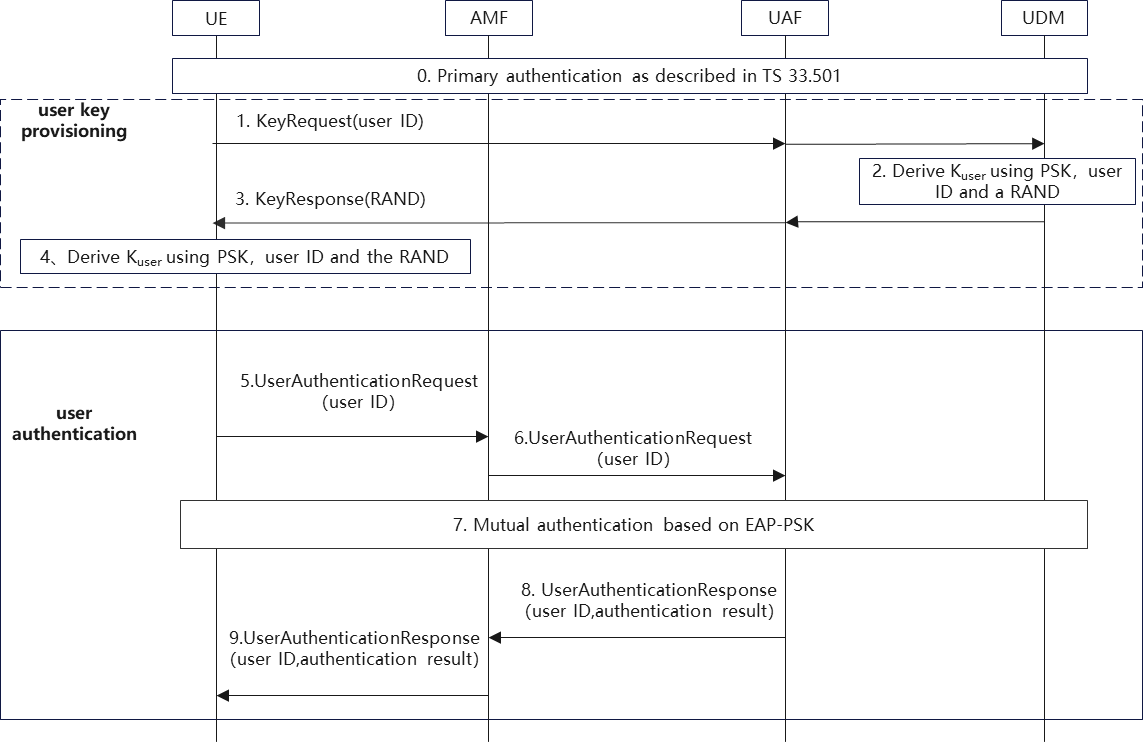
### 6.23.1 Introduction

This solution addresses KI#1. In this solution, the user authentication procedure is based on the EAP framework similar to NSSAA in TS 33.501 [3]. Specifically, this solution proposes to use the EAP-PSK (i.e., Pre-Shared Key).

ESP-PSK is an Extensible Authentication Protocol (EAP) method for mutual authentication a using a Pre-Shared Key (PSK). In this solution, the PSK is derived by the UE and the UDM based on the long-term key of the UE.

A logical function i.e., User Authentication Function (UAF) is introduced as the EAP authentication server, responsible for key derivation for the user. The UAF may be co-located with another NF, e.g., AUSF or AAA.

### 6.23.2 Solution details



**Figure 6.23.2-1 user authetication procedure**

Figure 6.23.2-1 illustrates the user authentication procedure.

1. Primary authentication as described in TS 33.501 [3].

The user key should be provisioned to UE. The following step 1-4 gives an example to show how the network function such as the UDM perform the steps. There are ways to provision the user key (e.g., Kuser). The specific step can be left to operator’s implementation.

1. The UE sends NAS Request to, via the AMF, the UAF. The request contains the user ID. Optionally, the request may indicate a valid time for the user key Kuser. UAF sends the request to the UDM.

2. The UDM uses the provisioned PSK, the user ID, and a generated RAND to derive a user key Kuser for the UE. For example, the Kuser can be derived by using key derivation function (KDF).

3. UDM returns a response to UAF with the RAND, and optionally includes a valid time, and UAF sends the response to the UE to notify the UE to calculate the Kuser based on RAND.

4. The UE uses the PSK, the user ID, and RAND to derive the Kuser.

5. The UE sends an authentication message to the AMF with the user ID.

6. The AMF triggers the user authentication procedure by sending a User Authentication Request to the UAF with the user ID.

7. Mutual authentication between UE and UAF/UDM is performed based on the user ID and Kuser. The UAF checks the valid time, if available.

8. The UAF sends a User Authentication Response to the AMF. This message contains the user ID and the authentication result.

9. The AMF sends the final result to the UE.

### 6.23.3 Evaluation

TBD

## 6.24 Solution #24: User ID privacy protection based on EAP-TLS protocol using pseudonym mechanism

### 6.24.1 Introduction

This solution addresses the key issue #2. The user’s privacy protection is based on a pseudonym mechanism to protect the User Identifier (ID). The user ID is replaced with a Member ID (MID) and a different MID is computed each time; hence increases the anonymity and avoid a user ID being tracked. In this solution, the EAP-TLS protocol is used to illustrate how the MID can replace the user ID to achieve anonymity.

### 6.24.1 Solution details

Aiming at the problem of identity information leakage during the authentication procedure, the solution introduces a new pseudonym mechanism. Users’IDs are grouped in advance and assigned Group User ID (GID ) to the UE. In the identity authentication phase, the EAP-TLS uses Member ID (MID) to replace the unique identity of the user and sent MID to the authentication server (AAA). In order to preserve the privacy of the unique identifier of the user, the AAA utilizes the GID to determine the users’ IDs group and the MID to determine the user's identifier.

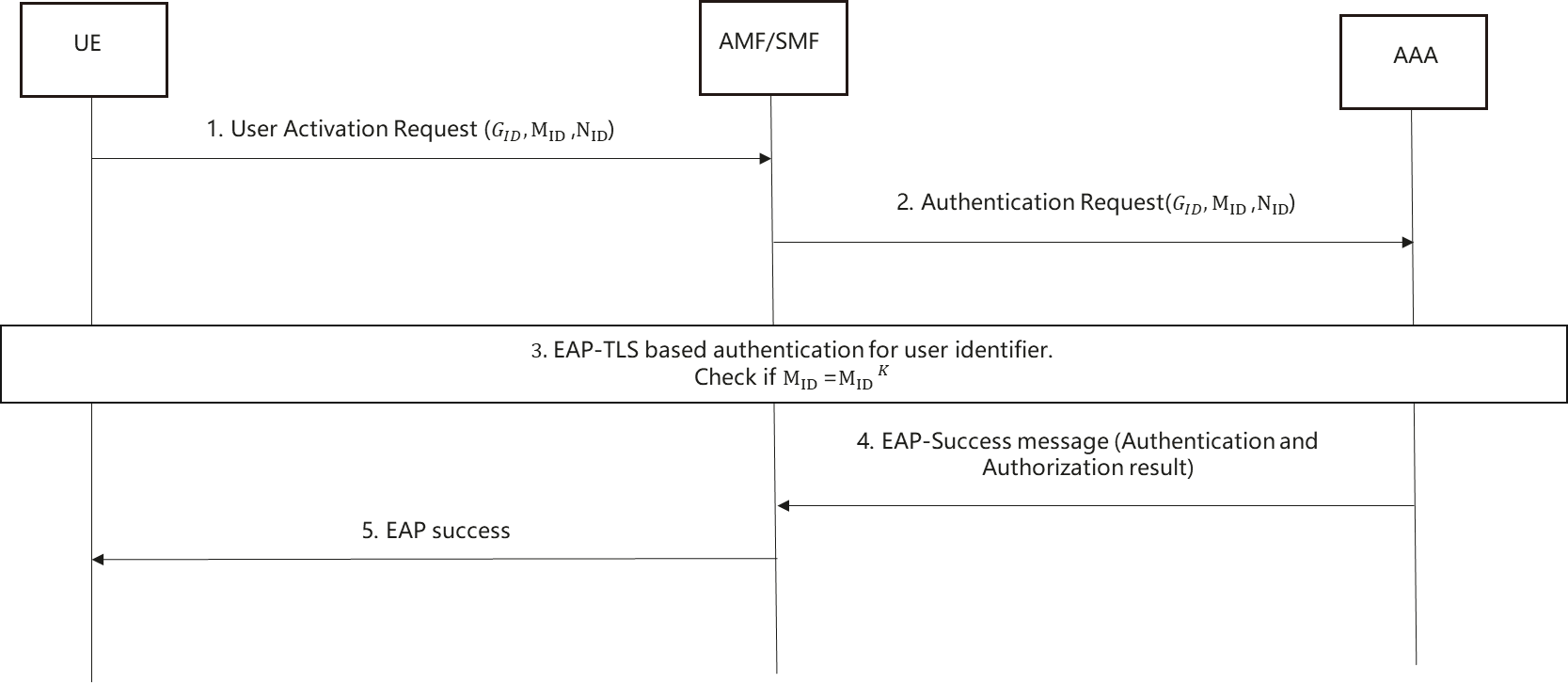


Figure 6.24.1 Illustration of user ID privacy protection based on pseudonym mechanism.

0. Provisioning: before the user authentication procedure, the authentication server (e.g., AAA) and the UE are provisioned with the Group User ID (GID)

1. After Primary authentication, the UE sends to the SMF a User Activation Request message including the GID, a random number NID, the Member ID (MID). The UE uses the user ID, NID and GID as input to perform a hash operation to obtain the Member ID (MID).

NOTE: The purpose of the random number NID is to ensure the UE calculates a different MID each time; hence it increases the anonymity and avoids User ID being tracked or linked to previous authentication.

2. The SMF initiates the user authentication and sends to AAA the Authentication Request, including MID, NID and GID.

3. The AAA determines the users’ IDs groupGID, finds the User ID k of each user in the group, and the AAA calculates MIDK with the NID, User ID k and GID. Then AAA compares whether MID and MIDK are equal. If they are equal, the AAA performs the subsequent user identity authentication and authorization based on the user ID. Otherwise, a failure message is generated.

4. After the EAP authentication completes, the AAA sends an EAP-Success message to the SMF, including authentication/authorization result.

5. Based on the result of user authentication (Success/Failure), the SMF returns User Activation Response to the UE.

### 6.24.3 Evaluation

This solution addresses the key issue #2.

The solution provides user privacy by using a Member ID (MID) instead of the real user identifier. Since the user identifier is not in the realm of 3GPP systems, how user identifier is mapped to MID is transparent to the 3GPP systems. To prevent tracking or linking of the user, the MID may occasionally be updated to the 3GPP system.

Editor’s Note: Further evaluation is FFS.

## 6.25 Solution #25: User Authentication with Certificate Generated by an authorized UE

### 6.25.1 Solution Introduction

This solution addresses KI#1: Authentication and Authorization of Human User ID. This solution is based on the EAP framework similar to NSSAA as in TS 33.501 [3]. Specifically, this solution enables linking a UE’s subscription to the user, through creating a user identity certificate by the UE and using the user identity certificate in EAP framework (e.g., EAP-TLS) for user authentication.

In the solution, the following logical function is introduced:

**Identity Certificate Authentication Function (ICAF)**: assuming a new logical function responsible for verifying a public key certificate generated by a UE for a user. It can be collocated with the existing NF, e.g., AUSF.

### 6.25.2 Solution Details

After UE primary authentication, the User ID is sent in a User Registration message to the AMF. The AMF triggers the user authentication procedure with the EAP framework (e.g., EAP-TLS) where a user identity certificate generated by UE is used as the client certificate.



**Figure 6.25.2-1: User authentication procedure with user identity certificate in EAP framework (e.g., EAP-TLS)**

1. The UE is provisioned with a key pair, i.e., a private key and the corresponding public key from the 3GPP network, used to generate a user identity certificate. The key pair provisioning is out of scope of this document and left to operator’s implementation. The ICAF is provisioned with the public key.

NOTE 1: If the key pair are stored in the UICC, the UE needs to fetch the key pair through the interface between the UICC and the UE.

1. The UE registers to the 3GPP network. The primary authentication is performed as described in clause 6.1 in TS 33.501 [3].
2. The UE locally generates a user identity certificate signed by the private key provisioned in Step 0. The user identity certificate includes the public key of the user, User ID and a valid period with the signature of the UE.
3. The UE sends a User Registration Request message to the AMF with the user ID.
4. The AMF triggers the user authentication procedure by sending a User Authentication Request including the User ID to ICAF.

NOTE 2: AMF acts as an EAP authenticator.

1. Mutual authentication between the User and the network using the EAP-TLS. The first part is the User authenticating the network. A network certificate is provided and the UE is able to verify the network certificate. The second part is the network authenticating the User and the ICAF can verify the UE generated user identity certificate by using the public key of the UE.

NOTE 3: ICAF acts as an EAP server.

1. The ICAF sends a user authentication response to the AMF including the User ID and the authentication result.
2. The AMF sends the authentication result to the UE.

### 6.25.3 Evaluation

## 6.26 Solution #26: User authentication with credentials derived by UIMF

### 6.26.1 Introduction

This solution addresses KI #1 on Authentication and Authorization of Human User ID. Specifically, it addresses the requirements for authentication of human user based on a user identifier linked to a 3GPP subscription. The solution applies to the cases where no user credential is preconfigured in the UE and the network for user authentication. The difference between this solution and solution #22 is that the user credential is generated by the UIMF instead of AUSF.

### 6.26.2 Solution details

#### 6.26.2.1 Description

The solution assumes the following:

NOTE: User authentication hereafter refers to the authentication of human user.

- The root key for user credential derivation is generated during UE registration procedure.

- The user credential is derived during user authentication procedure when the user identifier is sent from the UE to the network. The procedure takes place after the root key is generation.

- The User Identity Profile (UIP) is stored in a User Identity Management Function (UIMF), which can be collocated with an existing NF in HPLMN.

- Each user is also provisioned with a PIN/one-time password from the network via e.g. operator portal. The pair {User ID, PIN/one-time password} is stored as part of UIP in the UIMF. The PIN/password has a validity time. The secrecy of the PIN/one-time password needs to be ensured by each user that it is not known by any other users.

- There is a User Authentication and Authorization Function (UAAF) deployed by the home operator and dedicated to user authentication, which can be a standalone NF or collocated with an existing NF.

- User identifier can be made available to the UE before user authentication, e.g. through input of human user which is out of 3GPP scope.

- There is no credential preconfigured in the UE and UAAF to associate with the user identifier

#### 6.26.2.2 KUIA generation by AUSF and UE during Registration procedure

For human users, if there is no credential preconfigured in the UE and the network for user authentication, the credential can be derived based on KAUSF generated during primary authentication.

0. Each user is provisioned with a User ID and a corresponding PIN from the network via e.g. operator portal.



Figure 6.26.2.2: KUIA generation during Registration procedure

1. The UE sends the Registration Request, which contains at least SUCI or GUTI of the UE and UE capability supporting User Authentication.

2. Primary authentication is successfully performed between the UE and the network, during which KAUSF is derived by the AUSF.

3. If the UE capability supports user authentication via user credential derivation, the AMF sends a Nudm\_SDM\_Get Request message to the UDM to retrieve UE subscription from the UDM.

4. If the UE does not subscribe the user authentication feature, the AMF proceeds to step #9 without indicating user authentication method.

If the UE subscribes the user authentication feature and user authentication policy indicates credential (KUIA) derivation, the AMF determines to interact with the AUSF to trigger user credential derivation.

5. The AMF sends a Nausf\_UserAuthentication\_Authenticate Request message to the AUSF, which includes the SUPI of the UE, etc.

6. Upon receiving Nausf\_UserAuthentication\_Authenticate Request from the AMF, the AUSF determines that user authentication requires the KUIA to be derived from KAUSF of the UE. The AUSF derives KUIA and associates it with SUPI of the UE.

7. The AUSF sends the pair of {SUPI, KUIA} to the UIMF. The UIMF could be a separate network function or collocated with the UDM. The UIMF associates the KUIA with the GPSI mapped from the SUPI. The mapping between GPSI and SUPI could be stored in the UIMF or retrieved from the UDM/UDR.

8. The AUSF returns Nausf\_UserAuthentication\_Authenticate Response to the AMF with the indication that KUIA is derived.

9. The AMF sends Registration Accept to the UE, optionally with the User Authentication Method.

10. Upon receiving the User Authentication Method indicating that KUIA needs to be derived, the UE derives KUIA from KAUSF in the same way as the AUSF. The UE associates KUIA with its GPSI.

11. User Authentication is performed between the UE and the UAAF (see clause 6.26.2.3). The UAAF can be the AUSF or a separate NF.

#### 6.26.2.3 KUSER generation by UIMF and UE during User Authentication procedure



Figure 6.26.2.3: KUSER generation during User Authentication procedure

After the UE derives KUIA, the UE is able to initiate user authentication procedure towards the network each time a user logs on the UE.

1. The UE sends the User Authentication Request message to the UAAF which includes at least the User ID and GPSI. The message can be sent over control plane via the AMF or over user plane.

2. Upon receiving the User Authentication Request, the UAAF sends an Authentication Key Request to the UIMF, which contains the User ID and GPSI.

3. The UIMF retrieves KUIA based on the received GPSI. Then the UIMF retrieves the PIN/one-time password of the user based on the received User ID. Based on the retrieved Kuia and PIN/one-time password, the UIMF generates KUSER.

4. The UIMF returns the derived KUSER to the UAAF.

NOTE X: It is possible that the UAAF and UIMF can be collocated. In this case, steps #2 & #4 are not needed.

5. The UE and UAAF performs user authentication based on the User ID and KUSER (see clause 6.26.2.4).

6. The UAAF registers the User Authentication Result obtained using KUSER with the UIMF.

7. The UIMF stores the User Authentication Result associated with the User ID.

NOTE Y: Steps 6 and 7 are optional and to be aligned with architectural procedure in TR 23.700-32 [2].

8. The UAAF sends the User Authentication Response with the Authentication Result to the UE.

#### 6.26.2.4 User authentication between UE and UAAF



Figure 6.26.2.4: User Authentication between UE and UAAF

1. After the UAAF receives KUSER from the UIMF in step #4 of clause 6.26.2.3, the UAAF sends an EAP challenge to the UE, which contains the UAAF ID, random number RAND-N, and MAC\_N. The MAC\_N is the message authentication code of UAAF ID and RAND-N, computed using the KUSER.

2. Upon receiving the EAP challenge from the UAAF, the UE derives KUSER based on KUIA in the same way as the UIMF in step #3 of clause 6.26.2.3.

3. The UE computes the message authentication code XMAC\_N for the received UAAF ID and RAND-N using the KUSER, and compares XMAC\_N with the received MAC\_N. If XMAC-N matches MAC-N, the network is authenticated by the UE on behalf of the user.

4. The UE responds with an EAP challenge, which contains the RAND-U and User ID, and MAC\_U. The MAC\_U is the message authentication code of UAAF ID, User ID, RAND-U and RAND-N, computed using the KUSER.

5. The UAAF computes the message authentication code XMAC\_U for the received User ID, RAND-U and its own UAAF ID, RAND-N, using the KUSER, and compares XMAC\_U with the received MAC\_U. If XMAC-U matches MAC-U, the UE is authenticated by the network.

#### 6.26.2.5 Key hierarchy and derivation



Figure 6.26.2.5: Key Hierarchy for User Authentication with Derived Credential

Based on the procedure in clause 6.26.2.2, KAUSF is used as the root key in the hierarchy of key derivation. KUIA is derived from KAUSF by the UE and AUSF to be used as the intermediate key for all users on the UE. Based on the intermediate key KUIA, the key KUSER can be derived by the UE and the UIMF to be used as authentication credential for each specific user on the UE.

The KDFs and input parameters for KUIA and KUASER are the same as in solution #22.

### 6.26.3 Evaluation

TBD.

## 6.27 Solution #27: User privacy protection for UIP exposure based on RNAA

### 6.27.1 Introduction

This solution addresses Key Issue #2 on user privacy. Specifically, it addresses the requirements that the 5G system shall provide mechanisms for mitigating privacy attacks during the exposure of User Identity Profile information by the network to entities outside operator domain.

### 6.27.2 Solution details

According to TR 23.700-32 [2], User Identity Profile (UIP) information needs to be exposed to an AF. The information that can be exposed may include the content of the UIP, authorization/authentication results, linkage between User Identifier and a 3GPP subscription, etc. As all these information is related to the log-in user or the UE subscriber, user privacy needs to be ensured when exposing any of the information. It means that, in addition to the AF authorization for service access, the AF also needs to be authorized by the log-in user or UE subscriber for privacy protection.

Although TS 33.501 [3] Annex V already defines the consent framework that can be used for privacy protection via static user authorization based on UE subscription, it can only be used for protecting the privacy of UE subscriber. For protecting the privacy of log-in user, it is proposed to reuse the security mechanisms defined for RNAA (Resource owner-aware Northbound API Access) in TS 33.122 [x], by regarding the UIP information (including authentication results) as the resource of the log-in user and UE subscription information as resource of UE subscriber. The API invoker on the AF requesting the UIP information can only be authorized if the authorization function (CCF) obtains permission from the resource owner.

Editor’s Note: Terminology and architecture alignment with those in TR 23.700-32 [2] is FFS.

### 6.27.3 Evaluation

TBD.

## 6.Y Solution #Y: <Solution Name>

### 6.Y.1 Introduction

Editor’s Note: Each solution should list the key issues being addressed.

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled. The evaluation of the solution should include the impact to the 3GPP system.

# 7 Conclusions

Editor’s Note: This clause contains the agreed conclusions of the study.

## 7.3 Key issue #3: Authentication and Authorization of one or more non-3GPP devices behind one gateway UE or 5G-RG

Based on the architecture assumption, authentication of non-3GPP device is not done by 5GC. Authentication for non-3GPP devices performed by UE or 5G-RG is not in the scope of 3GPP. Thus, no normative work is needed.

Editor’s Note: conclusions on authorization of non-3GPP devices behind UE/5G-RG is FFS.

Annex <A>:  
<Informative annex title for a Technical Report>

Annex <X>:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-04 | SA3#115Adhoc-e | S3-241221 |  |  |  | Draft TR 33.700-32 skeleton | 0.0.0 |
| 2024-04 | SA3#115Adhoc-e | S3-241565 |  |  |  | Draft TR 33.700-32 skeleton (revised) | 0.0.1 |
| 2024-04 | SA3#115Adhoc-e | S3-241545 |  |  |  | S3-241565, S3-241122, S3-241556, S3-241514, S3-241515, S3-241543, S3-241566 | 0.1.0 |
| 2024-05 | SA3#116 | S3‑242515 |  |  |  | S3‑242495, S3‑242496, S3‑242497, S3‑242498, S3‑242499, S3‑242500, S3‑242501, S3‑242502, S3‑242503, S3‑242668, S3‑242504, S3‑242505, S3‑242506, S3‑242507, S3‑242508, S3‑242509, S3‑242610, S3-242611, S3-242612, S3‑242613, S3-242614, S3-242615­­­ | 0.2.0 |
| 2024-8 | SA3#117 | S3-243445 |  |  |  | S3-242887, S3-242888, S3-242925, S3-242926, S3-242927, S3-242941, S3-242942, S3-243037, S3-243128, S3-243146, S3-243147, S3-243208, S3-243209, S3-243440, S3-243441, S3-243442, S3-243443, S3-243444, S3-243446, S3-243447, S3-243448, S3-243449, S3-243450, S3-243451, S3-243452, S3-243453, S3-243454, S3-243455, S3-243456, S3-243457, S3-243458, S3-243459, S3-243460, S3-243461, S3-243462, S3-243463, S3-243465, S3-243466 | 0.3.0 |