|  |  |
| --- | --- |
| 3GPP TR 33.741 V0.2.0 (2022-07) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on home network triggered primary authentication (HONTRA);  (Release 18) | |
|  | |
| *5G-logo_175px* | 3GPP-logo_web |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal 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.  © 2021, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its 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 3

Introduction 4

1 Scope 5

2 References 5

3 Definitions of terms, symbols and abbreviations 5

3.1 Terms 5

3.2 Symbols 5

3.3 Abbreviations 6

4 Use Cases 6

4.1 Use Case #1: Security of Interworking 6

4.2 Use Case #2: SoR/UPU Counter Wrap around 6

4.3 Use Case #3: KAKMA refresh 6

4.X Use Case #X: <Use Case Name> 6

5 Key issues 7

5.1 Key Issue #1: Ability of the home network to trigger primary authentication 7

5.1.1 Key issue details 7

5.1.2 Security threats 7

5.1.3 Potential requirements 7

5.X Key Issue #X: <Key Issue Name> 8

5.X.1 Key issue details 8

5.X.2 Security threats 8

5.X.3 Potential security requirements 8

6 Solutions 8

6.Y Solution #Y: <Solution Name> 8

6.Y.1 Introduction 8

6.Y.2 Solution details 8

6.Y.3 Evaluation 8

7 Conclusions 8

Annex A (informative): Change history 9

# Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

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

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

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

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

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

**should** indicates a recommendation to do something

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

**may** indicates permission to do something

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

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

**can** indicates that something is possible

**cannot** indicates that something is impossible

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

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

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

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

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

In addition:

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

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

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

# Introduction

Editor’s Note: This clause contains some background information for the study.

# 1 Scope

The present document studies the use cases which needs Home Network initiated primary authentication and the associated security threats and requirements. As part of this investigation, the study aims at identifying which network function in the HN is better suitable to trigger the primary authentication, corresponding procedures, the potential impacts on visited and home network, and the potential impacts on existing procedures. Moreover, solutions for potential normative work are also in the scope of this study.

# 2 References

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

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

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

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

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

[2] 3GPP TS 23.502: “Procedures for the 5G System (5GS)”

[3] 3GPP TS 33.501: “Security architecture and procedures for 5G system”

[4] 3GPP TS 29.509: "5G System; Authentication Server Services; Stage 3".

[5] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA)  
based on 3GPP credentials in the 5G System (5GS)".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

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

**example:** text used to clarify abstract rules by applying them literally.

## 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 Key issues

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

## 4.1 Key Issue #1: Ability of the home network to trigger primary authentication

### 4.1.1 Key issue details

In the 5G System, the home network control over the security of the UE has been strengthened compared to previous generations by many new mechanisms such as SUPI privacy, termination of the authentication procedure in the home network and the provisions for increased home network control and linkage to subsequent procedures. However, when it comes to triggering the authentication, then this is still under the control of the serving network.

The home network uses K\_AUSF or keys derived from K\_AUSF to provide protection for various services, (e.g. interworking from 4G to 5G, SoR/UPU and AKMA services) and hence the home network would benefit from having the ability to be able to ensure a fresh K\_AUSF is available by tiggering an authentication, in particular to prevent counter wrap in SoR/UPU or after interworking from 4G when there might be no K\_AUSF available.

### 4.1.2 Security threats

Editor's Note: This clause is expected to describe the security threats for each use case.

### 4.1.3 Potential requirements

The home network may be able to trigger a primary authentication.

The messages in home network triggered primary authentication should be confidentiality protected, integrity protected, and anti-replay protected.

Note: All the solutions will be evaluated specific to the use case in the Annex X of this present document.

## 4.2 Key Issue #2: Signalling overload due to running the primary authentication for Kaf refresh

### 4.2.1 Issue details

The current 33.501[3]v17.3,0 doesn’t consider the scenario where the provisioned key KAF expires in trusted or untrusted AF for the AKMA usecase, then how to renew the keys. i.e., via primary authentication. It is a leftover issue and is going to addressed in [S3-220538](https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_106e/Docs/S3-220538.zip) with following objectives.“*It is desirable for the HN to be able to trigger primary authentication. This study is proposed to investigate the support of such a capability in 5GS. This study can provide home network control and address issues but not limit to, for example , UPU/SoR COUNT wrap around, refresh of KAUSF*’’.

If AF is allowed to request the 5G core to perform primary reauthentication, then there may be multiple primary reauthentications because of multiple AFs being involved with the UE. Multiple primary authentications may also result in an energy drain at the UEs.

And these multiple primary authentications obviously lead to signaling overhead and cause a refresh of the entire key hierarchy impacting both core and access security. The situation will be bad if the AUSF and the UDM handle the request for authentication every time, and it will be worse if more than one request is received in a very short period.

### 4.2.2 Security Threats

If the UDM or the AUSF handles the request for primary authentication every time without determining and if the more than one request is received in a very short of period, the signaling overhead inside 5GC may happen

### 4.2.3 Potential security requirements

The 5GS may reduce the impact on the signaling overhead when Home Network triggered authentication is supported.

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

### 4.X.1 Key issue details

### 4.X.2 Security threats

### 4.X.3 Potential security requirements

# 5 Solutions

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

## 5.1 Mapping of Solutions to Key Issues

Table 5.0-1: Mapping table

|  |  |
| --- | --- |
|  | Key Issues |
| Solutions | X |
| Y |  |

5.1 Solution #1: HN triggering primary authentication for various scenarios

5.1.1 Introduction

This solution provides a framework where the home network can trigger a primary authentication due to various scenarios, i.e.,

- SOR/UPU Counter wraparound;

- EPC to 5G interworking where KAUSF would not be available at UE and AUSF. And due to this, a few services will not work;

- Any other scenarios where any authorized NF can invoke the primary reauthorization.

The solution provides an advanced detection solution where the SoR/UPU wraparound situation is detected in advance, i.e., the AUSF detects that the UPU/SoR counter will reach its max value in the next SoR/UPU case and takes precautionary measures in advance.

5.1.2 Solution details

5.1.2.1 Procedure for detection of SoR/UPU Counter wraparound in advance and perform reauthentication

Figure 6.X.2.1: detection of SoR/UPU Counter wraparound in advance and perform reauthentication

1. When an AMF registers with UDM and invokes the Nudm\_UECM\_Registration API, the AMF shall provide a new AMF re-authentication callback URI. UDM shall store the same along with AMF registration.

2. The UDM decides to perform the UE parameter update procedure or SoR procedure. Therefore, the UDM invokes the Nausf\_UPUProtection or Nausf\_SoRProtection procedure. The AUSF tries to increment the Counterupu/CounterSoR and figures out that the Counterupu/CounterSoR is about to wrap around or will reach the max value at the next trigger. Therefore, AUSF shall provide an indication of "Counterupu Reaching Max value" or "/CounterSoR Reaching Max value" to UDM along with the successful result of the Nausf\_UPUProtection or Nausf\_SoRProtection procedure. This alerts the UDM that the current UPU/SoR procedure is OK to continue, but the next follow-up UPU procedure update will cause a wraparound failure. The UDM shall store the received indication.

3. The UDM completes the UPU/SoR procedure as defined in TS 33.501[3].

4. If "Counterupu Reaching Max value" or "CounterSoR Reaching Max value" indication is received in step 2, the UDM uses the callback URI received during the Registration and shall send a notification to the AMF with SUPI and the "reauthentication required" flag set to true.

Editor's Note: Either to use reauthentication required cause or to use a new service is FFS.

5. Based on the received indication, the AMF shall start the primary reauthentication procedure.

6. AMF shall invoke Nausf\_UEAuthetication\_Authenticate Request with SUPI and SN-Name.

7. The AUSF sends the Nudm\_UEAuthentication\_Get Request with SUPI and SN-Name to the UDM.

Steps 8-10 are the same as defined in TS 33.501[3] clause 6.1.3. After Key KAUSF is generated, the CounterUPU and CounterSoR shall be reset. Therefore, any further UPU/SoR trigger at the UDM will be successful.

5.1.2.2 Reauthentication due to EPC to 5G mobility

When UE moves from EPC to 5GC, the AMF performs Registration with UDM and invokes Nudm\_UECM\_Registration API. UDM should check if there is no authentication result stored in the UDM, then the UDM shall send a notification to the AMF with SUPI and the "reauthentication required" flag set to true as defined in clause 5.1.2.1. Step 4. It ensures KAUSF is available in AUSF and UE when a user moves from EPC to 5GC so that different services work smoothly, i.e., SoR, UPU, and/or a user accessing the AKMA AF.

5.1.2.3 Reauthentication invoked by other NFs

If any NF (i.e. AAnF) other than UDM wants to invoke the UE Reauthentication, the NF shall request the UDM to perform re-authentication.



Figure 6.X.2.3: Reauthentication invoked by other NFs

1. NF wants to perform re-authentication. Therefore, NF shall send a Nudm\_EventExposure\_Subscribe request to UDM with a new flag for Reauthentication Required.

Editor’s Note: Which NFc invokes the UDM service is FFS.

2. The UDM authorizes the request based on existing means (e.g. Oauth2.0).

3. If authorization is successful, the UDM checks whether the primary authentication for the UE to be initiated or request to be rejected, based on the operator policy. Operator policy includes the details of the "waiting period before initiating new reauthentication". If the check is passed, the UDM shall invoke the reauthentication procedure as defined in Steps 4 to 9 of clause 5.1.2.1.

Editor's Note: Either use the existing subscribe API at the UDM or define a new request is FFS.

Editor's Note: The factors considered by the AAnF to determine if a UE re-authentication is required or not is FFS.

Editor's Note: How the AAnF knows such factors which helps to determine re-authentication requirement is FFS.

5.1.3 Solution Evaluation

TBD.

## 5.2 Solution #2: UDM triggered primary authentication

## 5.2.1 Introduction

This solution is to address the KI#1 by providing a basic procedure on Home network triggering authentication.

The solution introduces a new service exhibited by the AMF and to be used only by the UDM to request primary authentication. This is because in 5GC the UDM knows which AMF is serving the UE. Upon a request from the UDM, the AMF triggers primary authentication using the existing services and NAS procedures.

### 5.2.2 Solution details

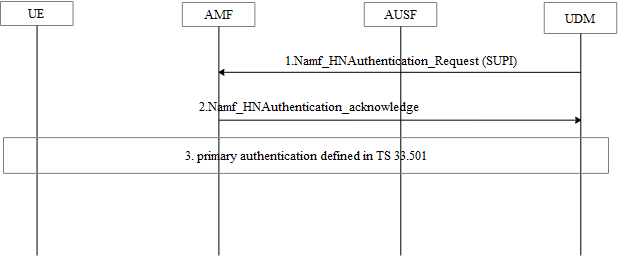


Figure 5.2.2.4-1: Home network trigger primary authentication procedure

1. The UDM decide to run primary authentication based on decision at the UDM or is requested by the AUSF or the AanF. . The UDM selects the AMF that is serving the UE from the UE context.

Editort’s Note: Whether a new service operation is provided by AMF is FFS.

Editort’s Note: How UDM will trigger this primary authentication is FFS

2. The AMF replied the Namf\_HNAuthentication\_acknowledge message to the UDM.

3. The AMF starts the primary authentication procedure defined in TS 33.501[3].

### 5.2.3 Evaluation

TBD

## 5.3 Solution #3: Home network triggered authentication solution for 4G to 5G interworking

### 5.3.1 Introduction

This solution addresses the KI #1: Ability of the home network to trigger primary authentication. And it relates to use case #1: Security of Interworking

### 5.3.2 Solution details

During the mobility and handover procedures from EPS to 5GS, the UE sends Registration Request to 5G network with registration type set to "Mobility Registration Update".

In the registration procedure, after the AMF registers with the UDM using Nudm\_UECM\_Registration, UDM checks if it supports home network services requiring KAUSF, for example, UPU, SoR and AKMA. UDM also checks for the corresponding AUSF instance ID. If UDM supports the home network services but doesn’t have AUSF instance (or doesn’t keep track of AUSF that stores the latest KAUSF generated after successful completion of the latest primary authentication reported to the UDM), it replies error information to AMF and indicates AMF to initiate UE (re-)authentication before continuing the registration procedure. For example, it responds with 403 Forbidden with the cause “REAUTHENTICATION\_REQUIRED”.

Editor’s Note: Impact on current system on reusing the error code is FFS.

NOTE: No AMF’s reaction on this error code in stage 3.

NOTE: this error code is only used for interworking.

### 5.3.3 Evaluation

Editor’s Note: Evaluation is FFS.

## 5.4 Solution #5: UDM initiated primary authentication based on a NF request

### 5.4.1 Introduction

This solution addresses KI#1. The home PLMN triggers re-authentication of the UE, based on the request from an internal NF (AUSF) which needs to refresh the KAUSF or KAKMA.

### 5.4.2 Solution details

A new primary authentication may require for certain events at the network, resulting in refresh of the latest home key KAUSF. In such scenarios, an internal Network Function (AUSF) requests the UDM to trigger the re-authentication procedure.



Figure 5.X.2-1: Home PLMM initiated primary authentication

1. A UE initiates registration procedure and the primary authentication is performed as specified in TS 33.501[3] as a part of registration procedure. After successful primary authentication, a KAUSF is derived at the AUSF and at the UE.
2. A NF (e.g. AUSF, AAnF) checks whether there is need to refreshing the KAUSF key (e.g. due to SoR or UPU count wrap around) for the UE.

Editor's Note: Which NF and under which conditions triggers the UDM to perform primary authentication is FFS

1. The NF (e.g. AUSF,) requests the UDM to initiates re-authentication procedure for the UE by sending a Nudm\_re-authentication message including the SUPI of the UE to initiate the primary authentication to refresh the home key (e.g.KAUSF).
2. Upon receiving the Nudm\_re-authentication message from the NF (e.g. AUSF) for the SUPI, the UDM checks whether the primary re-authentication for the UE to be initiated or request to be rejected, based on the operator policy.

Editor’s Note: if a SoR or UPU transmission procedure is ongoing then how the UDM handles the current SoR or UPU transmission is FFS.

1. If the operator policy allows, then the UDM sends a Nudm\_UDM\_message (e.g. an existing message between UDM and AMF) containing the SUPI of the UE and an indicator re-authentication required to the current serving the AMF to initiate the primary authentication for the UE.

Editor’s Note: The specific service used for the UDM triggering the AMF to perform authentication is FFS.

1. Upon receiving the request from the UDM, the AMF(SEAF) initiates the primary authentication as described in clause 6.1.2 of TS 33.501 [3]. A new KAUSF is established after primary authentication procedure. The AMF intiates Security Mode Command procedure after successful primary authentication procedure to take the recently KAUSF as the current KAUSF.

### 5.4.3 Solution Evaluation

TBD

5.5 Solution #5: Using the UDM to start home triggered authentications

5.5.1 Introduction

This solution addresses KI#1 and KI#2.

5.5.2 Solution details

This solution uses the UDM to trigger an authentication with the possibility of an NF requesting the UDM to trigger the authentication. Having the UDM as a single point of control to trigger authentications allows the amount of home triggered authentications to be controlled, e.g. the UDM can reject request for a new authentication from the AKMA function if there has been a suitably fresh authentication.



Figure 5.5.2-1: UDM triggered authentications

The home triggered authentication proceeds as follow:

Step 0: The UE is currently registered to either a 3GPP or non-3GPP access.

Step 1: An NF decides that a home triggered authentication is necessary and sends a request to the UDM including either the GPSI or SUPI of the UE (depending on what is available to the NF) to trigger an authentication for that UE.

NOTE 1: Step 1 is not needed in the case that the UDM unilaterally decides that a home triggered authentication is needed.

Editor’s Note: The NFs that can trigger the UDM are FFS. A possible example is the AKMA function which could decide that a particular UE’s AKMA key needs refreshing. : It is FFS, based on what AKMA function determines to refresh AKMA Key.

Editor’s Note: Possible cases for UDM triggering authentication are the UDM may require a refresh of the keys to protect UPU or SOR or may notice SOR/UPU counter may be close to max value. These cases are FFS.

Editor’s Note: It is currently assumed that NF can trigger the UDM using either SUPI or GPSI as it is not clear (and won’t be clear to final list of NFs that can trigger UDM is decided) whether all NFs that will be allowed to trigger the UDM will have access to SUPI. It is FFS, if GPSI need to be used for authentication trigger request and in what scenarios.

Step 2: If the UDM agrees to the request from the NF or decides on its own that a home triggered authentication is needed, the UDM selects an AMF that the UE is registered to and sends a request to the AMF/SEAF including the SUPI to trigger an authentication for that UE.

NOTE 2: It is left up to implementation which AMF is selected if the UE is registered to more than one. It is also left to the UDM implementation whether to try the second AMF if the request to the first one fails.

Editor’s Note: The specific service used for the UDM triggering the AMF to perform authentication is FFS.

Step 3: If the AMF/SEAF agrees to run an authentication, then AMF/SEAF the acknowledges the request from the UDM.

Step 4: If the UDM triggered the authentication due to a request from an NF, then the UDM responds to the NF with an acknowledgement.

NOTE 3: Another possibility is to delay the responses to after a successful authentication but the UDM will get such an acknowledgement from the existing procedures.

Step 5: The AMF/SEAF starts an authentication using existing procedures as described in clause 6.1.2 of TS 33.501 [3].

5.5.3 Evaluation

Editor’s Note: Evaluation is FFS.

## 5.6 Solution #6: UDM initiated primary authentication based on AUSF request

### 5.6.1 Introduction

This solution addresses KI#1. The UDM triggers re-authentication of the UE, if an internal NF request (AUSF) to initiate re-authentication to refresh the UE specific home key (KAUSF).

### 5.6.2 Solution details

A new primary authentication may require for certain events at the network, resulting in refresh of the latest home key KAUSF. In such scenarios, an internal Network Function (AUSF) requests the UDM to trigger the re-authentication procedure.



Figure 5.6.2-1: UDM initiated primary authentication

1. The primary authentication is performed as specified in TS 33.501[3]. After successful authentication, KAUSF is derived at the AUSF and at the UE.

2. AUSF determines (due to long time availability of same key, etc) the need of refreshing the KAUSF key.

Editor’s Note: Under which conditions the AUSF triggers the UDM to perform authentication is FFS.

3. If the AUSF determines that there is a need to refresh the KAUSF, it decides to request UDM to initiate the primary authentication to refresh the home key KAUSF. AUSF sends a re-authentication request to the UDM by providing SUPI of the UE.

4. Upon receiving the re-authentication request from the AUSF, UDM checks whether the requesting AUSF is the one that holds the latest KAUSF and whether the primary re-authentication for the UE to be initiated or not, based on the operator policy. Operator policy includes the details of the wait period for the new request, after the last successful authentication.

5. If the operator policy allows, then the UDM requests the AMF currently serving the UE to initiate the primary authentication for the UE. Upon receiving the re-authentication message from UDM, the AMF acknowledges the request

6. Upon receiving the request from the UDM, the AMF (SEAF) initiates the primary authentication as described in clause 6.1.2 of TS 33.501 [3], resulting in generation of fresh key material in the UE and in the network as described in clause 6.2 of TS 33.501 [3], if the primary authentication is performed successfully.

### 5.6.3 Solution Evaluation

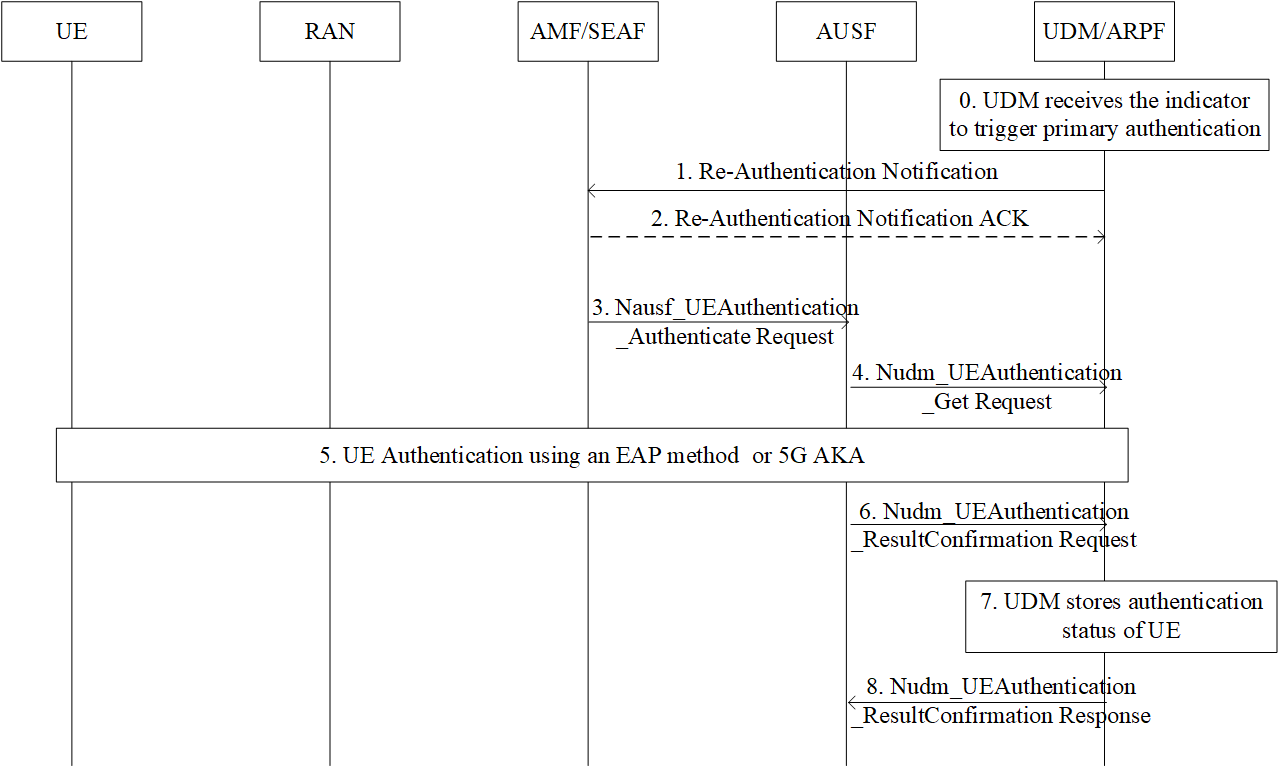
TBD

## 5.7 Solution #7: UDM initiated Primary Authentication

### 5.7.1 Introduction

This solution describes how the UDM initiates a primary authentication to refresh the long lived key KAUSF. The solution addresses Key Issue #1: Ability of the home network to trigger primary authentication.

### 5.7.2 Solution details



0. Upon receiving a message that contains an application error, the UDM triggers a primary authentication procedure. For example, the UDM receives the Nausf\_SoRProtection\_response/ Nausf\_UPUProtection\_response including an application error COUNTER\_WRAP indicating the CounterSoR/CounterUPU associated with the KAUSF of the UE is about to wrap around. To refresh the KAUSF, the UDM could initiate a new primary authentication procedure.

Editor’s Note: Which use case this solutions addresses is FFS.

1. The UDM sends the Re-Authentication Notification, e.g. Nudm\_UECM\_ReAuthenticationNotification, (incl. SUPI, Access Type, Re-Authentication reason) message to the AMF. According to the core network status, the Re-Authentication reason can be set to SoR counter wrap around, UPU counter wrap around, etc.

Editor’s Note: It is FFS if SoR/UPU Counter wrap around reason need to be provided to AMF and what does AMF do with this.

2. If the UDM has requested an acknowledgement from the AMF, the AMF returns the Re-Authentication Notification ACK message to the UDM.

3. The SEAF invokes the Nausf\_UEAuthentication service by sending a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF. The Nausf\_UEAuthentication\_Authenticate Request message shall contain SUCI or SUPI and the Serving network name, as defined in TS 33.501 [3].

4. The Nudm\_UEAuthentication\_Get Request sent from AUSF to UDM includes SUPI and the serving network name. Based on SUPI, the UDM/ARPF shall choose the authentication method.

5. Based on the decision of UDM, the UE and the network performs the EAP-AKA’ or 5G AKA procedure.

6. The AUSF shall store the new Kausf and inform UDM about the result and time of the authentication procedure with the UE using a Nudm\_UEAuthentication\_ResultConfirmation Request. The AUSF also resets the CounterSoR/CounterUPU once the new Kausf is generated.

7. The UDM shall store the authentication status of the UE (SUPI, authentication result, timestamp, and the serving network name).

8. The UDM shall reply to AUSF with a Nudm\_UEAuthentication\_ResultConfirmation Response.

### 5.7.3 Evaluation

## 5.8 Solution #8: Solution to enable UDM in the HN to trigger Primary Authentication

### 5.8.1 Introduction

The Solution address key Issues #1 and #2. The solution enables the UDM in the Home Network (HN) to trigger the primary (re-)authentication and further also describes various security context handling (i.e., for SoR, UPU and AKMA) associated with the Kausf resulting from a successful primary (re-)authentication.

### 5.8.2 Solution details

The Solution discuss two main aspects as follows:

(A) HN Triggering Primary (re-)authentication: The solution describes various factors that need to be considered by the AUSF to determine if a primary (re-) authentication is required and if a primary (re-)authentication is required, the solution further explains how a primary (re-)authentication is triggered by the UDM (on a request from AUSF) in the home network as shown in Figure 5.8.2-1.

Figure 5.8.2-1: HN triggered primary authentication with AUSF

The steps showns in Figure 5.8.2-1 is described as follows:

0. Primary authentication as in TS 33.501 Clause 6.1.3. The expiration time for the primary authentication related to the SUPI can be set in the UDM based on local policy.After a successful primary authentication, a successful registration may occur and multiple UE Parameter Update (UPU) procedure and/or Steering of Roaming (SoR) procedure may happen.

1. At any point of time, the AUSF can determine to notify any of the following factors such as (i) if the SoR counter is about to wrap around or (ii) if the UPU counter is about to wrap around:

Editor’s Note: Under which conditions the AUSF triggers the UDM is FFS

2a. The AUSF sends to UDM a notification message which can include SUPI, cause value (as suitable to the condition met such as any of: SoR Counter wrap around indication / UPU Counter wrap around indication).

2b. The UDM on receiving any of SoR Counter wrap around indication, UPU Counter wrap around indication, checks if is valid based on local policy. If a Counter wrap around indication is received related to SoR or UPU which is ongoing or required to be sent, the UDM/UDR can locally store the SoR or UPU data until a successful primary (re-authentication) is completed and (re-)initiate SoR/UPU accordingly.

2c. The UDM can send an acknowledgement indication in the notificationresponse message.

Further irrespective of the SoR/UPU wrap around conditions, based on the expiration time locally stored for the primary authentication of UE related to the SUPI, the UDM can trigger primary (re-)authentication with step 7-8.

3. The UDM sends to the serving AMF/SEAF of the UE an authentication request with SUPI.

4. The AMF/SEAF initiates primary (re-)authentication as described in TS 33.501[3] Clause 6.1.2.

(B) AKMA Key handling without signalling overhead:

Setting AKMA Key expiry: The solution describes how an AKMA Key expiration and AF key expiration are handled in relation to the primary authentication to enable efficient AKMA related key handling with limited signalling. Figure 6.Y.2-2 shows setting of AKMA Key expiry.



Figure 5.8.2-2: Deriving KAKMA and Setting expiry time after primary authentication

The steps shown in Figure 6.Y.2-2 is described below.

0. Initiation of authentication and authentication method selection is based on TS 33.501[3] Clause 6.1.2.

1-3. Based on the selected authentication method, generate the authentication vector (AV) as in 33.501[3] Clause 6.1.3. The UDM/UDR based on operator policy set an expiry time related to the primary authentication and AUSF Key to be used by the AUSF to set the AKMA key lifetime. The UDM sends to AUSF, Nudm\_UEAuthentication\_Get Response message which can include AV, SUPI, an expiry time (i.e, exp Time) indication, AKMA indication and Routing Indicator (i.e., if a subscriber has an AKMA subscription UDM includes AKMA indication and Routing Indicator according to TS 33.501[3] Clause 6.1.3). The AUSF performs authentication method specific message exchange (i.e., one or more message exchanges related to the authentication) with the UE as in TS 33.501[3] Clause 6.1.3. On successful primary authentication, the AUSF derives AUSF Key (i.e., KAUSF) and based on home network operator policy stores the KAUSF as in TS 33.501[3] Clause 6.1.3 along with the SUPI.

4. If the AUSF receives AKMA indication from UDM, then AUSF derives AKMA Anchor Key (i.e., KAKMA) and A-KID from the AUSF Key (i.e., KAUSF) as in TS 33.535[5]. The AUSF sets the expiry time for the AKMA Key (i.e., KAKMA) based on the expiry time received from the UDM.

Editor's Note: The need for KAKMA expiry time is FFS.

The UE can generate the AKMA Anchor Key (KAKMA) and the A-KID from the KAUSF before initiating communication with an AKMA Application Function as in TS 33.535[5].

5a. The AUSF selects the AKMA Anchor Function (AAnF) and sends the generated A-KID, KAKMA and AKMA Key expiry time to the AAnF together with the SUPI of the UE using the Naanf\_AKMA\_KeyRegistration Request service operation. The AAnF can store the latest information (such as latest A-KID, KAKMA and AKMA Key expiry time) sent by the AUSF.

NOTE 1: When re-authentication runs, the AUSF generates a new A-KID, and a new KAKMA and sets the new AKMA Key expiry time and sends the new generated A-KID, new KAKMA and new AKMA Key expiry time to the AAnF. After receiving the new generated A-KID, KAKMA and new AKMA Key expiry time, the AAnF deletes the old A-KID, KAKMA, and AKMA Key expiry time and stores the new generated A-KID, KAKMA and new AKMA Key expiry time.

5b. The AAnF stores the received SUPI, A-KID, KAKMA and AKMA Key expiry time (i.e., KAKMA exp time).

5c. The AAnF sends the response to the AUSF using the Naanf\_AKMA\_AnchorKey\_Register Response service operation as in TS 33.535[5].

Setting AF Key expiry:

The expiry time for the AF Key is set based on the expiration time of the AKMA Key as shown in Figure 5.8.2.3.

The steps shown in Figure 5.8.2-3 is described as follows:



Figure 5.8.2-3: AF Expiration handling and HN triggered primary authentication

1-2. The pre-requisite and steps 1-2 are same as in TS 33.535[5] Clause 6.2.1.

3. Derive AF key as in TS 33.535[5].

Then the AAnF sets the expiration time for the KAF considering the locally stored expiration time of the AKMA Key (Where the expiration time for the KAF can be same as the expiration time of the AKMA Key).

4-5. Steps 4-5 are same as in TS 33.535[5] Clause 6.2.1.

Following a successful AF key establishment, the UE can securely communicate with the AF and use the application. At a later point of time, following steps may be performed on AF key expiry.

6a-b. If the UE request the AF for access and if the KAF expires or is about to expire, then the AF request the AAnF for the AF key by sending Naanf\_AKMA\_ApplicationKey\_Get request, which may include indication for key refresh.

NOTE 2: As the AF key expiration is bound to the expiration of the AKMA Key and inturn to the expiration of the AUSF Key, by the time AF key expires, the AUSF Key will also be expired and the AUSF would have triggered primary (re-) authentication and the primary (re-)authentication would be running meanwhile.

6c. The AAnF checks the locally available AKMA Key expiration time for the associated A-KID, if it is expired, then the AAnF can determine not to refresh the AF Key and determines to waits for the new AKMA key to be provided by the home network (i.e., AUSF);

6d. The AAnF sends to AF a Naanf\_Response message, which can include a waiting time(r) if the AAnF finds that the AKMA Key available is expired for the A-KID.

The waiting time(r) can be used by the AF to retry the key request procedure with AAnF. During this time, the already running primary (re-)authentication if succeed, results in a new AKMA key and new AF key establishment.

7a-b. If the AUSF key expires, the AUSF triggers primary (re-)authentication as described in (A) step 5-8 of this clause.

### 5.8.3 Evaluation

TBD

## 5.9 Solution #9: AMF initiated primary authentication based on AUSF request

### 5.9.1 Introduction

This solution addresses KI#1. A new primary authentication may require for certain events at the network, resulting in refresh of the latest home key KAUSF. In such scenarios, an internal Network Function (AUSF) requests the AMF to trigger the re-authentication procedure. The AMF initiates re-authentication of the UE, if an internal NF requests (AUSF) to initiate re-authentication to refresh the UE specific home key (KAUSF).

### 5.9.2 Solution details



Figure 5.9.2-1: AMF initiated primary authentication

1.The primary authentication is performed as specified in TS 33.501 [3]. After successful authentication, KAUSF is derived at the AUSF and at the UE.

2. AUSF determines (for e.g., due to long time availability of same key, etc) the need of refreshing the KAUSF key.

Editor’s Note: The analysis of multiple AUSFs triggering at this step is FFS.

3. If the AUSF determines that there is a need to refresh the KAUSF, it decides to perform primary authentication to refresh the home key KAUSF. AUSF requests UDM to provide UE’s current AMF by sending Nudm\_UECM\_Get request.

4. Upon receiving the request for the details of the current serving AMF from the AUSF, UDM provides UE’s current AMF details in Nudm\_UECM\_Get response message.

5. The AUSF prepares to indicate re-authentication and requests the AMF to initiate primary authentication for the UE by invoking Namf\_UEAuthentication\_Authenticate service operation. Upon receiving the re-authentication message from UDM, the AMF acknowledges the request.

Editor’s Note: The details of Step 5 are FFS.

6. Upon receiving the request from the AUSF, the AMF (SEAF) initiates the primary authentication as described in clause 6.1.2 of TS 33.501 [3], resulting in generation of fresh key material in the UE and in the network as described in clause 6.2 of TS 33.501 [3], if the primary authentication is performed successfully.

Editor’s Note: How this solution will solve the EPC interworking use case is FFS

### 5.9.3 Solution Evaluation

TBD

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

### 5.Y.1 Introduction

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

### 5.Y.2 Solution details

### 5.Y.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

# 6 Conclusions

Editor’s Note: This clause contains the agreed conclusions that will form the basis for any normative work.

# Annex A (informative): Use cases

## A.1 Use Case #1: Security of Interworking

As an evolution of LTE networks, the 5G system supports backward compatibility, providing seamless voice and data services continuity. According to TS 23.502 [2], the 5G core enables interworking between EPS and 5GS, allowing the UE to move between two systems. During interworking between 5GS and EPS, the MME and the AMF perform the handover procedure, which provides the IP address continuity and the security context mapping on inter-system mobility to UEs.

As per TS 33.501 [3], when the UE moves from EPS to 5GS, the handover procedure is initiated by the source MME to provide the target AMF with the UE identity and UE's EPS security context. If the source MME has the UE NR security capabilities stored, it forwards the UE NR security capabilities as well to the target AMF.

For the UE moving to 5GS for the first time, the AMF derives a mapped KAMF' key from the received KASME, then derives the mapped 5G NAS keys (i.e., KNASenc and KNASint) and KgNB using the mapped KAMF' key. In this situation, the target AMF has no native 5G security context, it will use the mapped 5G security context constructed from the EPS security context to protect the subsequent messages, which does not include a KAUSF key. As specified in TS 33.501 [y], if the AMF has no native 5G security context available, when the UE performs the Registration Request following the handover procedure, the AMF via the SEAF should run a primary authentication depending on local operator policy.

## A.2 Use Case #2: SoR/UPU Counter Wrap around

The counters for SoR and UPU procedure are maintained by the AUSF as specified in 3GPP TS 33.501 [2]. However, there is no mechanism to refresh the counters unless by running the primary authentication. When the counters are about to wrap around, there is currently no mechanism by which the home network can trigger primary authentication in order to refresh the KAUSF key and safely reset the counters in time. In roaming situations, the home network has no control on when to trigger such procedure unless by forcing a deregistration may cause a service disruption for the user.

The maximum value of the counters is 65536 according to TS 29.509[3], and the wrap around of the counter is a corner case due to the infrequent use of the UPU and SoR procedures. The probability is low for the case of a primary authentication not happening before 65536 SoR/UPU messages are transmitted from the network to the UE.

## A.3 Use Case #3: KAKMA refresh

In TS 33.535[5], the KAF can only be refreshed by UA\* protocol, there is no other method to refresh it. That’s because if the UA\* protocol does not support the KAF refresh, and KAKMA is unchanged, the same KAF will be generated again. If the KAKMA can be refreshed, then the issue is solved. However, the AKMA feature specified in 3GPP TS 33.535 [5] does not support refresh of the KAKMA key. In fact, refresh of AKMA keys is not possible during the lifetime of the KAUSF key even when the life time of KAF has expired. By triggering the primary authentication from the home network, the AUSF will generate a new KAUSF and a new KAKMA.

# Annex B (informative): Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-05 | SA3#107-e |  |  |  |  | S3-220831,S3-220832,S3-221205, S3-221261, S3-221240, S3-221239, S3-221219 | 0.1.0 |
| 2022-07 | SA3#107Adhoc-e |  |  |  |  | S3-221663,S3-221664,S3-221524,S3- |  |