|  |  |
| --- | --- |
| 3GPP TR 33.741 V0.3.0 (2022-10) | |
| 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)".

[6] 3GPP TS 29.503: "5G System; Unified Data Management Services; Stage 3".

# 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. The UE is authenticated and registered at the 5GC.

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 sends a notification to the AMF with SUPI and the "reauthentication required" flag set to true.

Note: In the existing specs, UDM contacts AMF on Namf\_communication service to trigger the re-registration required or reauthentication required with deregistration first. Therefore, UDM can use the same Namf\_communication service for reauthentication without performing the deregistration.

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 AAnF

If the AAnF wants to invoke the UE Reauthentication, the NF shall request the UDM to perform re-authentication.

Whenever KAF has expired at the (internal or external) AF and the AF wants to refresh the KAF via 5GC, the AF request AAnF for UE reauthentication so that KAF can be refreshed. The AAnF maintains the "wait time before initiating new reauthentication". For example, suppose a configured value of "wait time before initiating new reauthentication" is 30 min then AAnF shall not invoke the UDM reauthentication service/API if primary (re) authentication is performed less than 30 min ago and returns an error to AF. If the interval is 30 minutes or more, then AAnF invokes the UDM service/api to start the primary reauthentication. Alternatively, "wait time before initiating new reauthentication" can be maintained at the UDM as well.



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

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

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.

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

#### 5.2.2.1 Procedure

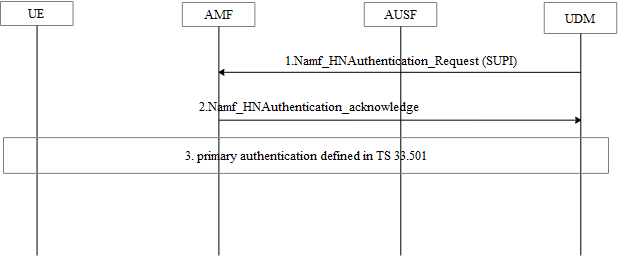


Figure 5.2.2.4-1: Home network trigger primary authentication procedure

1. The UDM decides to run primary a authentication based on the request from the UDM or AUSF or the AAnF . For example, when the UDM needs to send the UPU data or SoR data but cannot find a valid AUSF instance which means there is no valid KAUSF. Another example is when the AAnF needs to refresh KAKMA based on the cause value sent by the AF due to any reason.

The AUSF and the AAnF sends Nudm\_HNAuthenticate-Request message to the AMF for this purpose.

After receiving the request, the UDM needs to further consider the local policy before determine to run the primary authentication, such as whether the primary authentication has successfully run in a very short period. Then the UDM selects the AMF that is serving the UE from the UE context. The UDM sends Namf\_HNAuthentication\_Request message to the AMF the message contains the SUPI of the UE.2. The AMF may reply the Namf\_HNAuthentication\_acknowledge message to the UDM.

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

Editor’s Note: How the solution addresses the different use cases is FFS

#### 5.2.2.2 Service provided by AMF

##### 5.2.2.2.1 General

The AMF provides Home Network Authentication service to the requester NF, i.e. UDM, by Namf\_HN Authentication.

##### 5.2.2.2.2 Namf\_HN Authentication service

###### 5.2.2.2.2.1 Namf\_HNAuthentication service operation

**Service operation name:** Namf\_ HNAuthentication \_Request.

**Description:** Request the AMF starts the primary authentication procedure.

**Input, Required:** SUPI

**Output, Required:** None

**Output, Optional:** None

#### 5.2.2.2 Service provided by UDM

##### 5.2.2.2.1 General

The UDM provides Home Network Authentication service to the requester, i.e. AUSF and AAnF, NF by Nudm\_HN Authentication. The service consumer uses this service to request the UDM to trigger the primary authentication for requesting the KAUSF.

##### 5.2.2.2.2 Nudm\_HN Authentication service

###### 5.2.2.2.2.1 Nudm\_HNAuthentication service operation

**Service operation name:** Nudm\_ HNAuthentication \_Request.

**Description:** Request the UDM to trigger the primary authentication.

**Input, Required:** SUPI

**Output, Required:**None

**Output, Optional:** None

### 5.2.3 Evaluation

This solution addresses KI#1.

This solution can address the 4G-5G interworking case, KAKMA refresh use case, SoR/UPU counter wrap around use case, and other potential use case that needs to refresh the KAUSF.

A new AMF service and a new UDM service are defined, because there is no existing SBA message can be reused.

This solution impacts on AMF and UDM.

Editors Note： further evaluation is FFS.

## 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: Steps 1 and 4 are not needed in the case that the UDM unilaterally decides that a home triggered authentication is needed and in the overall solution if it is determined that no NF needs to be able to request a triggering of an authentication.

NOTE 2: The AKMA function could request a trigger of authentication to refresh the AKMA key. The AKMA function determines the need to request a trigger of the authentication based on its local policy, e.g. the AKMA key of a particular subscription has not been updated sufficiently recently.

NOTE 3: Whether both GPSI and SUPI are needed as options to request the UDM to triggering an authentication will be determined based on the decision on whether and which NFs are allowed to make that request.

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 4: The UDM has sufficient information to trigger a primary authentication due to needing to refresh keys used to protect SoR/UPU traffic, mobility from 4G in the serving network or possible wrap-around of SoR/UPU counters (as it receives these values from AUSF). Hence these scenarios that are under discussion can be supported by this solution with no further changes.

NOTE 5: 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.

NOTE 6: This solution is agnostic to the specific SBI service used by the UDM to trigger the AMF to perform an authentication, e.g. whether is it better to add a new service or modify an existing service.

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. Based on the operator policy, the AUSF can determine when to refresh the KAUSF for the scenarios such as SoR/UPU Counter wraparound, due to long lived KAUSF and and other case where any authorized NF (for e.g., AAnF) invokes primary authentication.

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

This solution proposes to address the following security requirement of KI#1:

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

AUSF determines to refresh the KAUSF in various scenarios such as SoR/UPU Counter wraparound, due to long lived KAUSF and other case where any authorized NF (for e.g., AAnF) invokes primary authentication. This solution proposes a mechanism for the UDM to trigger a primary authentication if an internal NF request to initiate primary authentication which results in the refresh of the latest home key KAUSF.

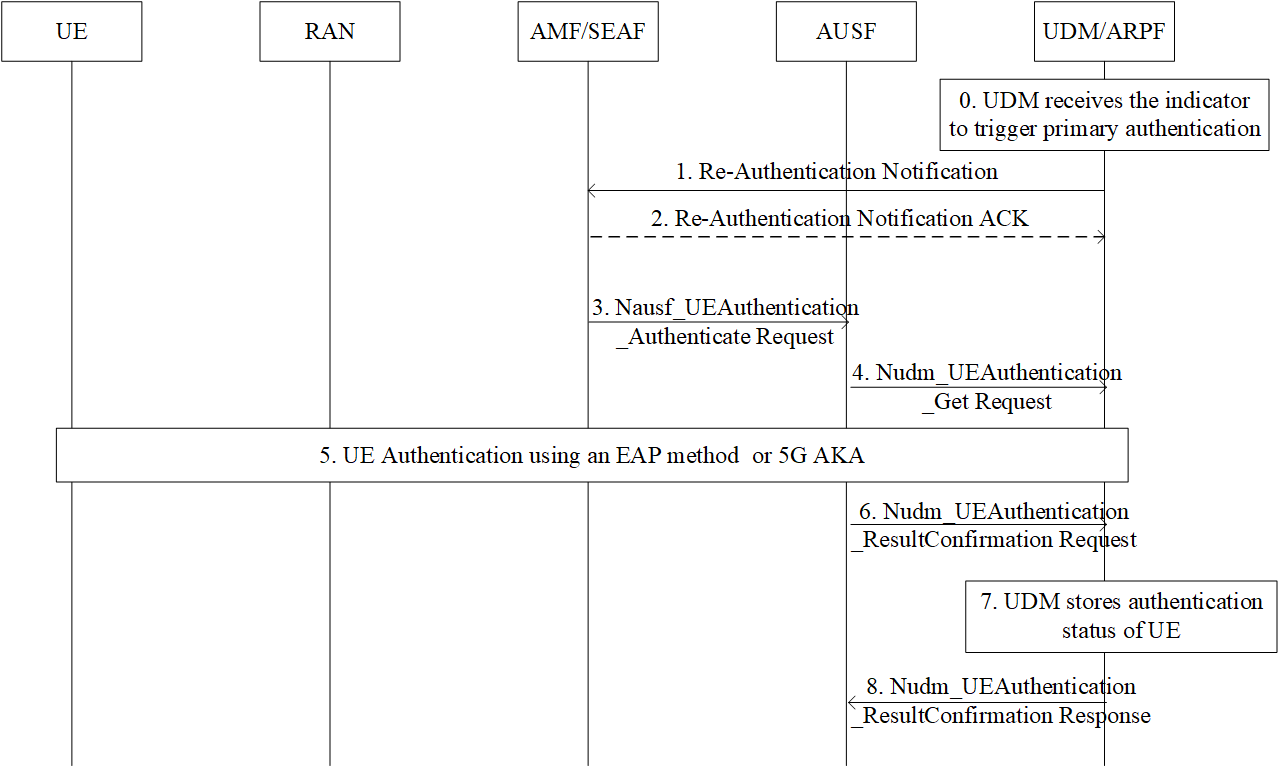
Editor’s Note: The evaluation details about how the solution addresses the different use cases is FFS.

## 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 and relates to use case #2: SoR/UPU Counter Wrap around.

### 5.7.2 Solution details



0. Upon receiving a message that contains an application error in the SoR/UPU Counter wrap use case, 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.

1. The UDM sends the Re-Authentication Notification, e.g. Nudm\_UECM\_ReAuthenticationNotification, (incl. SUPI, Access Type, Re-Authentication reason) message to the AMF. Same as the Nudm\_UECM\_DeregistrationNotification service, the UDM provides the reason for sending the reauthentication notification to the consumer NF. According to the core network status, the Re-Authentication reason can be set to SoR counter wrap around, UPU counter wrap around, etc.

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

This solution fulfills the security requirements of Key Issue #1 and relates to use case #2: SoR/UPU Counter Wrap around.

The proposed solution ensures that the home network is able to trigger a primary authentication. In addition, the HN-triggered Re-Authentication request/response messages exchanged between the UE and 5GC is confidentiality protected, integrity protected and anti-replay protected.

This solution has no impact on the UE.

This solution has impact on the HPLMN. The UDM needs to support a new service operation to notify the AMF of the need for Re-Authentication. If necessary, the UDM also needs to receive the Re-Authentication ACK sent by the AMF to acknowledge the success of the triggered Re-Authentication.Editor’s Note: The impact on the AMF/SEAF is FFS.

Editor’s Note: Further evaluation is FFS.

## 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(This part is applicable to use-case such as a home network triggers a primary (re-)authentication based on any of: operator policy, or SoR/UPU counter is about to wrap around):

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:

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(This part is applicable only for use-case related to AF key expiry and service outage issue):

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.

NOTE 1: The need for AKMA Key exiry time is applicable only when this study conclusions takes into account the ‘AF key expiry’ without UE impacts as one of the aspects to be addressed as part of KI#1 and KI#2. Setting of AKMA key expiry based on operator policy allows, the AAnF to set AF key expiry time same as AKMA key expiry. So, before an AF key expire, the home operator would have performed a home triggered primary authentication based on operator policy.

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 3: 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

The solution has the following impacts:

AUSF: On SoR/UPU wrap around, it notifies the UDM about the wrap around condition, along with the SUPI. If an expiry time is received from the UDM, it needs to set the AKMA key validity using the received expiry time.

UDM: The UDM need to initiate primary (re-)authentication for a UE by sending a request to the serving AMF when it receives any SoR/UPU wrap around notification from the AUSF or when the earlier primary authentication validity is about to expire based on local configuration. Further the UDM based on local policy need to set an expiration time for the primary authentication validity as well as an expiry time for the AKMA related key usage.

AMF: Based on request from the UDM, it need to initiate a primary authentication.

AAnF: If an AKMA key expiry time is received, based on local policy, the AF key expiry time should be set considering also the received AKMA key expiry time.

Editor’s Note: Further evaluation is FFS.

Editor’s Note: Usecase specific evaluation is FFS.

## 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.

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. If the request is not from the latest AUSF, the UDM rejects the request. Only the latest AUSF in which UE is authenticated will be provided with the AMF ID.

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 requests the AMF to initiate primary authentication for the UE by invoking Namf\_UEAuthentication\_Authenticate service operation as defined in clause 5.9.2.2. Upon receiving the re-authentication message from UDM, the AMF acknowledges the request.

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.

#### 5.9.2.1 EPC interworking usecase

The security procedure for the case when the UE was already registered to the same PLMN via another System (E-UTRA/EPS) registers with VPLMN AMF is described below in figure 5.9.2.1-1:



Figure 5.9.2.1-1: Procedure for reauthentication during mobility registration update

1) The UE initiates registration by sending a Mobility Registration Update message to the VPLMN AMF.

2) The VPLMN AMF executes the mobility registration update procedure as defined in sub-clause 4.2.2.2.2 of 3GPP TS 23.502 [2] and retrieves a mapped security context as defined in TS 33.501[3] 8.1.

3) The VPLMN AMF invokes Nudm\_UECM\_Registrationservice operation message to the UDM to get, amongst other information, the Access and Mobility Subscription data for the UE (see step 14a in sub-clause 4.2.2.2.2 of 3GPP TS 23.502 [2]).

Editor’s Note: Whether the existing proposed procedure is sufficient, and no normative work is required are FFS

4-5) UDM sends a notification Nudm\_UECM\_Registration Response to the AMF with the " Reauthentication Required’ indication set to true.

6) Upon receipt of the Nudm\_UECM\_Registration Response notification in 5, the AMF shall initiate a Nausf\_UEAuthentication\_Authenticate service operation.

#### 5.9.2.2 Namf\_UEAuthentication\_Authenticate

#### 5.9.3.2.1 Namf\_UEAuthentication\_Authenticate service operation

**Service operation name:** Namf\_UEAuthentication\_authenticate.

**Description:** The AUSF triggers the Re-authentication procedure.

**Input, Required:** SUPI.

**Output, Required:** Acknowlegement.

### 5.9.3 Solution Evaluation

Based on the local operator policy and annex A.1, solution provides reauthentication procedure for the case when the UE was already registered to the same PLMN via another System (E-UTRA/EPS) registers with VPLMN AMFThis solution proposes to address the following security requirement of KI#1:

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

AUSF determines to refresh the KAUSF in various scenarios like SoR/UPU counter wraparound, due to long lived KAUSF and other case where any authorized NF invokes primary authentication. This solution proposes a mechanism for the AUSF to send a re-authentication request to the AMF and AMF performs the primary authentication which results in the refresh of the latest home key KAUSF.

Editor’s Note: An evaluation specific to the use cases in this document is FFS

### 5.9.3 Solution Evaluation

TBD

5.10 Solution #10: UDM initiated primary authentication based on AAnF request for Kaf refresh scenario

5.10.1 Introduction

This solution addresses key issues #1 for KAKMA the refresh use case and key issues #2 in TR 33.741 [1]. To meet the requirements of both KI 1# and KI #2, the basic idea of this solution is to make HN trigger primary authentication for Kaf refresh only when necessary.

The solution determines whether to perform primary (re)-authentication according to whether there are newly generated KAKMA, and corresponding A-KID for the UE. If the HN has already performed primary (re)-authentication for the UE just before the KAF of a certain AF expired and the primary (re)-authentication has already generated a new available KAKMA, then there is no need to perform primary (re)-authentication again, thereby mitigating multiple primary (re)-authentications; otherwise, the HN does need to trigger primary authentication to generate new KAKMA to refresh the expired KAF.

The solution makes the AF notify the AAnF rather than directly request UDM to perform primary (re)-authentication. Even if more than one AF key expiry notification is received in a very short period, the signaling overhead on UDM will be reduced due to the mediation of the AAnF.

5.10.2 Solution details



Figure 5.10.2-1: UDM initiated primary authentication based on AAnF request for Kaf refresh scenario

1. An AF detects that the KAF of a UE is expiry or about to expire, and decides to refresh the KAF.

NOTE1: How AF detects the AF key expiry and when to send a notification to the AAnF is implementation specific.

1. The AF selects the AAnF according to TS 33.535 clause 6.7[5] using the A-KID associated with the expired KAF. Then it sends a notification to the AAnF with the [UE ID] (if available), the A-KID associated with the expiry KAF, the AF identity (AF\_ID), and an indication of “application key lifetime is about to expire”.

NOTE2: If the AF is located outside the HPLMN of the UE, it shall discover the HPLMN of the UE based on the A-KID and sends the notification towards the AAnF via NEF service API. The NEF selects the AAnF according to TS 33.535 clause 6.7[5], then forwards the notification to the AAnF.

1. Upon receiving the application key expiry notification, the AAnF determines whether to request UDM to trigger primary (re)-authentication procedures or not according to the following process.

If the UE ID (e.g., SUPI/GPSI) is present in the received notification message:

the AAnF checks if there is a newly stored A-KID for the UE which is different from the received A-KID, if yes, the AAnF skips to step 9;

if the AAnF checks that the locally stored A-KID for the UE is the same as the received A-KID, it shall check whether to request the HN triggered primary authentication for the UE based on the operator policy (the operator policy may include the details of the "waiting period before initiating new reauthentication"); if the check is passed, the AAnF shall continue with step 4~10;

If the UE ID is not present in the received notification message, which corresponds to the case that anonymous user access to the AF as specified in TS 33.535 clause 6.2.2[5], the AAnF retrieves in all of the stored A-KIDs to check if the received A-KID is present in the AAnF:

if the received A-KID is present in the AAnF, the AAnF shall check whether to request the HN triggered primary authentication for the UE based on the operator policy (the operator policy may include the details of the "waiting period before initiating new reauthentication"); if the check is passed, the AAnF shall recover the UE’s SUPI according to the A-KID, then continue with step 4~10;

if the received A-KID is not present in the AAnF, the AAnF shall skip to step 10 with an error response.

NOTE3: When the UE ID is not present in the received notification message of the AAnF, not finding the received A-KID in the AAnF implies that the A-KID for the UE has been refreshed. However, the AAnF cannot be aware of what UE the AF is serving since the UE is using anonymous access. Therefore, the AAnF cannot derive the new KAF for the AF because the AAnF cannot identify the latest A-KID and KAKMA for the UE just by the received A-KID.

1. The AAnF request UDM to trigger a primary (re)-authentication for that UE with the UE’s SUPI.

Editor’s Note: whether the AAnF can directly invoke the primary authentication service from UDM is FFS.

1. UDM checks whether the primary re-authentication for the UE to be initiated or the request to be rejected, based on the operator policy.
2. If the UDM agrees to the request from the AAnF, the UDM selects an AMF that the UE is registered to and notifies the AMF including the SUPI to trigger an authentication for that UE.
3. The AMF starts the primary authentication procedure as per TS 33.501 clause 6.1.3.
4. The UE, AUSF, and AAnF derive AKMA key after primary authentication as per TS 33.535 clause 6.1 step3~5.
5. The AAnF derives new KAF from the new KAKMA as specified in TS 33.535 Annex A.4.
6. The AAnF sends a notification response message to the AF with the new A-KID, the new KAF and the KAF expiration time, or sends an error response to the AF if UE ID is not present in the received notification message and the received A-KID is not found in the AAnF in step 3.

NOTE4: If the information in step 10 indicates an error response, the AF may choose to reject UE’s access to the AF when the KAF of a UE is expiry based on local policy. Afterward, UE may trigger a new Application Session Establishment request with the latest A-KID to the AKMA AF. Using this latest A-KID, the UE and the AF can establish a new application session using existing procedures defined in TS 33.535 clause 6.2.

NOTE5: If the AF is located outside the HPLMN of the UE, the AAnF shall send the notification response message to the AF via NEF service API.

5.10.3 Solution Evaluation

## 5.11 Solution #11: Home network triggered primary authentication controlled by the UDM

### 5.11.1 Introduction

The solution proposes the UDM to be the central point of control for a potential Home Network triggered authentication (HONTRA). This solution describes potential directions for all the three use cases.

### 5.11.2 Solution details

#### 5.11.2.1 General

The three use cases investigated in this study (Interworking, SoR/UPU counter wrap-around, KAKMA refresh) are different with respect to whether the UE is being registered or whether the UE has already registered to 5GC. Therefore, there are two main architectural patterns which could be used for the application of HONTRA or equivalent procedure to solve a potential need for the 3 use cases. In the first pattern the UDM uses existing procedures to trigger primary authentication under UE registration while in the second pattern the UDM triggers a new procedure after the UE is already registered to the 5GC.

#### 5.11.2.2 UDM triggered primary authentication during UE Registration

The procedure for UDM triggered primary authentication during UE Registration proposed in this solution is based on existing procedures already defined in TS 33.501 [3], TS 23.502 [2] and TS 29.503 [6].

Figure 5.11.2.2-1: UDM triggered primary authentication during UE Registration

0. The Registration procedure as in TS 23.502 [2], clause 4.2.2.2.2, steps 1-13.

1. During UE registration in AMF, the AMF triggers Nudm\_UECM\_Registration service operation to register the UE in the UDM.

2. The UDM checks the authentication status and decides based on a HN primary authentication configuration to request a new primary authentication for the UE. Refer to TS 33.501 [3] clause 6.1.4.2 for more details regarding when UDM potentially takes this decision. The UDM marks the UE as requiring primary authentication.

NOTE: A HN primary authentication configuration is a group of configuration options for authentication decisions. These may be per-UE or PLMN-wide, the design is left to implementation and could indicate for example when a UE should be authenticated, the use case for re-authentication, etc.

Editor's Note: The details of HN primary authentication configuration is FFS.

Editor's Note. How HN primary authentication configuration is utilized in different scenarios and use cases explained in Clause 5.Y.2.2 and 5.Y.2.3 is FFS.

3. Based on the HN primary authentication configuration the UDM decides to reject the Nudm\_UECM\_Registration service operation with a REAUTHENTICATION\_REQUIRED error as defined in TS 29.503 [6].

4. The AMF then initiates the primary authentication procedure as defined in TS 33.501 [3], clause 6.1.2. The primary authentication is executed according to TS 33.501 [3], clauses 6.1.3 and 6.1.4. The primary authentication is successful.

5. Upon successful primary authentication, the UDM clears the mark that the UE requires authentication.

6. The AMF repeats the Nudm\_UECM\_Registration service operation to register the UE in the UDM.

7. The UDM checks the authentication status and now decides that the AMF registration can be accepted.

8. The UDM accepts the AMF Registration.

9. The Registration procedure as in TS 23.502 [2], clause 4.2.2.2.2, steps 14b-25.

See clause 5.11.2.4.1 for more details on how this procedure can be applied to cover the interworking use case.

#### 5.11.2.3 UDM triggered primary authentication after UE Registration

The procedure for UDM triggered primary authentication after UE Registration proposed in this solution is depicted in the following figure.

Figure 5.11.2.3-1: UDM Triggered primary authentication after UE Registration

1. The UE is registered in the 5GC via an AMF. The AMF has registered the UE in UDM. The AMF potentially has authenticated the UE or has reused an authentication context from another AMF (or MME). The UDM keeps a time stamp of the latest UE authentication in 5GC (refer to TS 33.501 [3] clause 6.1.4).

2. The UDM decides that the UE needs to be authenticated according to the HN primary authentication configuration. It marks that the UE needs to be authenticated and takes the action to request a new primary authentication procedure for the UE towards the AMF. The reasons for the UDM deciding that the UE needs to be authenticated can be different:

a) The UDM is required to initiate a SoR/UPU procedure for the UE, but it detects that the corresponding Counters have wrapped-up or are about to wrap-up. See clause 5.11.2.4.2 for more details on how this procedure can be applied to cover the SoR/UPU wrap-up use case.

b) The UDM enforces a Home Network primary authentication configuration to refresh primary authentication after a selected period of time and that time (based on the time stamp of latest authentication kept in UDM) has expired for the UE. See clause 5.11.2.4.3 for more details on how this procedure can be applied to cover the KAF refresh use case.

3. Unless the UE is already engaged in a primary authentication procedure already, UDM requests the AMF to trigger a primary authentication procedure for the UE by sending a re-authentication notification to the AMF.

If multiple AMFs are registered in UDM, the UDM selects and notifies one AMF first and if primary authentication fails, UDM potentially also notifies the other AMF based on local policies.

This solution proposes that the new service operation is modelled as a notification operation within the set of services offered by UDM; i.e. a Nudm service operation.

NOTE: Which is the most appropriate alternative to model the re-authentication notification can be agreed with CT4 during normative phase.

4. . Before acknowledging the ReAuthentication notification, the AMF first checks if the UE can be contacted to execute the requested primary authentication procedure. After receiving the notification from the UDM in Step 3 the AMF decides based on its own policy and potentially the received Home Network authentication configuration when to initiate primary authentication and when to contact the UE or wait for the UE to contact the AMF.

Editor's Note: Whether the AMF pages the UE or waits for a UE to contact the AMF, is FFS.

5. The AMF replies to the ReAuthentication Notification either with a successful response including the status information (if the UE is reachable or not).

6. If the UE is reachable, the AMF then initiates the primary authentication procedure as defined in TS 33.501 [3], clause 6.1.2. The primary authentication is executed according to TS 33.501 [3], clause 6.1.3 and 6.1.4. The primary authentication is successful.

Otherwise, if the UE cannot be reached, the AMF marks the UE as requiring authentication, stores this information in the UE security context and:

- Upon next UE contact in the same AMF, the AMF then triggers the primary authentication procedure after consulting the information stored in the UE security context if the UE requires re-authentication.

- Upon UE registration in UDM via a different AMF, if the new AMF does not authenticate the UE prior to the AMF registration, the UDM then rejects the AMF registration with a Re-Authentication Required error as described in clause 5.11.2.2. If the new AMF is able to retrieve the UE security context from the old AMF, the security context includes an indication that the UE needs to be authenticated (this indication was based on the old AMF actions), or a specific event information. The new AMF acts on this information and initiates primary authentication. Otherwise, the new AMF registration to the UDM will trigger the UDM to act and initiate authentication as described in clause 5.11.2.2.

7. After the primary authentication is successfully completed, the UDM clears the mark that UE requires primary authentication in the HN primary authentication configuration.

8. The UDM executes other procedures (e.g. SoR/UPU) depending on the reason that motivated the UDM triggered reauthentication procedure in step 2.

#### 5.11.2.4 Applicability of the UDM triggered primary authentication procedures to the Use Cases.

##### 5.11.2.4.1 Interworking use case

The UDM triggered primary authentication procedure during registration as described in clause 5.11.2.2 can be used by the Home Network to initiate primary authentication during the interworking use case.

It can be observed that interworking mobility from EPS to 5GS could result from a handover. However, a registration procedure is executed as the last steps of a handover procedure so the procedure in 5.11.2.2 is applicable for the handover case.

This solution makes use of existing proposed procedures in TS 33.501[3], clause 6.1.4.2, and potentially no normative work is required to support this use case.

Editor's Note: Whether the existing proposed procedure is sufficient and no normative work is required are FFS.

NOTE: Solution #1 (clause 5.1.2.2) and Solution #3 proposes same solution for the interworking use case as proposed here too.

##### 5.11.2.4.2 SoR/UPU wrap around use case

The UDM triggered primary authentication procedure after registration as described in clause 5.11.2.3 can be used by the Home Network to initiate primary authentication during the SoR/UPU wrap around use case.

The UDM can detect that the SoR/UPU Counters has wrapped-up or are about to wrap-up during the execution of the corresponding services in AUSF. The UDM receives the value of the Counters from AUSF so UDM can detect when the Counter are about to wrap up. Ultimately, the AUSF provides a Counter wrap up error to UDM when the counters wrap up. Based on the HN primary authentication configuration, the UDM can then request the AMF to trigger a primary authentication procedure for the UE.

After the primary authentication is successfully completed, the UDM can trigger the SoR/UPU procedure if needed.

If the primary authentication cannot be initiated by the AMF after being requested by the UDM (e.g. in case the UE is not reachable at that time), the UDM is informed by the AMF in the result of the reauthentication notification. In this case, the UDM marks the UE as requiring re-authentication in the HN primary authentication configuration and suspends the SoR/UPU service for the UE until the UE is authenticated again.

##### 5.11.2.4.3 Home Network triggered primary authentication for KAF refresh

If there is a need to address the KAF refresh use case, the UDM triggered primary authentication procedure after registration as described in clause 5.11.2.3 can be used to ensure that there is fresh KAUSF/ KAKMA key available in the Home Network for the KAF refresh use case. This could be achieved in several ways for example the UDM decides based on the HN primary authentication configuration whether to perform a primary authentication for KAF refresh or the UDM providing the HN primary authentication configuration to the AAnF; the AAnF can then decide to set the KAF expiration time based on the HN primary authentication configuration so that a primary authentication happens before KAF expiration.

NOTE: The need to for KAF refresh based on HONTRA is dependent on the outcome of the AKMA study.

### 5.11.3 Evaluation

## 5.12 Solution #12: Delegated Home Network controlled primary authentication

### 5.12.1 Introduction

The solution proposes that the Home Network delegates the enforcement of its Home Network (HN) primary authentication policy to the Serving Network (SN). The SN initiates primary authentication upon time intervals and/or events described in the HN primary authentication policy such as timer events or receptions of specific messages.

Editor' Note: Whether the HN primary authentication policy is static or run-time policy is FFS.

A HN primary authentication policy is a group of configuration options for authentication decisions. These may be per-UE or PLMN-wide, and could indicate for example when a UE should be authenticated, the use case for re-authentication, etc. The exact design of the HN primary authentication policy is left to normative work.

### 5.12.2 Solution details

The basic concept of this solution is that the HN delegates the enforcement of its HN primary authentication policy to the SN.

The SN can be made aware of the HN primary authentication policy as part of the SLA agreements with each roaming partner. Such a sharing of HN primary authentication policies is in the scope of GSMA. However, when HPLMN provides the HN policy to the service network, then how the serving network will take into account such a HN policy is within the remits of 3GPP.

This document outlines the needed functionality on the home and serving network to support such a delegated primary authentication.

Alternatively, this solution proposes that the HN provides the HN primary authentication policy to the SN via an online method using SBA interactions. Some examples of how the HN authentication policy could be then provided to the SN include:

a) In the response to the authentication request to the AMF (Nausf\_UEAU\_Authenticate Response).

b) In the response to the AMF registration in UDM (Nudm\_UECM\_Registration Response).

c) As Subscription Data provided to the AMF during registration (Nudm\_SDM\_Get Response).

Depending on the method used, the HN primary authentication policy potentially applies either at HPLMN level or on a per UE basis (i.e. different UEs of the HPLMN potentially use different HN authentication policies).

The AMF potentially takes into account the local authentication policy and the provided HN primary authentication policy and decides when to initiate primary authentication and when to potentially contact the UE.

Editor's Note: How a (timer) policy interworks with other scenarios that cause UE reauthenticated.

### 5.12.3 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 |  |  |  |  | S3-221524, S3-221633, S3-221663, S3-221664, S3-221675, S3-221653, S3-221697, S3-221606, S3-221589, S3-221601, S3-221602, S3-221646 | 0.2.0 |
| 2022-10 | SA3#108Adhoc-3 |  |  |  |  | S3-222694-r1,S3-222920-r6, S3-222922-r4,S3-222511-r1,S3-222704-r1,S3-222717-r4,S3-222737-r3,S3-222738-r2,S3-2322760,S3-222841-r1,S3-222842-r1,S3-222880,S3-222881 | 0.3.0 |