|  |
| --- |
| 3GPP TR 33.741 V0.1.0 (2022-05) |
| 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 address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2021, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 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. Morever, solutions for potential normative work is 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 Use Cases

Editor's note: This clause includes the use case that needs the Home network initiates the primary authentication.

## 4.1 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.

## 4.2 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.

## 4.3 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.

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

# 5 Key issues

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

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

### 5.1.1 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 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. On the other hand, as described in clause x, there are several use cases that would benefit from such possibility, i.e. a home network initiated authentication procedure.

### 5.1.2 Security threats

Not applicable

### 5.1.3 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.

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

### 5.2.1 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 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 reauthentiations 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.

### 5.2.2 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

### 5.2.3 Potential security requirements

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

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

### 5.X.1 Key issue details

### 5.X.2 Security threats

### 5.X.3 Potential security requirements

# 6 Solutions

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

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

### 6.Y.1 Introduction

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

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

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

# 7 Conclusions

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

Annex A (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-05 | SA3#107-e |  |  |  |  |  S3-220831,S3-220832,S3-2201045-r2, S3-220892-r4, S3-220835-r1, S3-220834-r3, S3-220903-r5 | 0.0.0 |