|  |
| --- |
| 3GPP TR 33.864 V0.2.0 (2020-11) |
|  |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on the security of Access and Mobility Management Function (AMF) re-allocation;(Release 17) |
|   |
|  |  |
|  |
| 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.© 2020, 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 4

Introduction 5

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 7

3.3 Abbreviations 7

4 Architecture and security assumptions of AMF re-allocation 7

4.1 General 7

4.2 Procedure of Registration with AMF re-allocation 7

4.3 Architecture and security assumptions 9

5 Key issues 10

5.1 Key Issue #1: Security of AMF re-allocation procedures 10

5.1.1 Key issue details 10

5.1.2 Security threats 10

5.1.3 Potential security requirements 11

5.X Key Issue #X: <Key Issue Name> 11

5.X.1 Key issue details 11

5.X.2 Security threats 11

5.X.3 Potential security requirements 11

6 Solutions 11

6.1 Solution #1: AMF re-allocation via RAN using existing security states 11

6.1.1 Introduction 11

6.1.2 Solution details 11

6.1.3 Evaluation 12

6.2 Solution #2: Security of AMF re-allocation when 5G NAS security context is rerouted via RAN 12

6.2.1 Introduction 12

6.2.2 Solution details 12

6.2.3 Evaluation 15

6.3 Solution #3: Solving registration failure with AMF re-allocation via RAN 15

6.3.1 Solution Overview 15

6.3.2 Solution Details 15

6.3.3 Security Evaluation 17

6.4 Solution #4: Solution to enable NAS Security for AMF reallocation and reroute via RAN Scenario 18

6.4.1 Introduction 18

6.4.2 Solution details 18

6.4.3 Evaluation 21

6.Y Solution #Y: <Solution Name> 21

6.Y.1 Introduction 21

6.Y.2 Solution details 21

6.Y.3 Evaluation 21

7 Conclusions 21

Annex A (informative) 23

A.1 Registration failure issue with AMF re-allocation via RAN 23

A.1.1 General 23

A.1.2 Description of Registration Failure Issue 23

Annex X (informative): Change history 27

# Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

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

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

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

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

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

**should** indicates a recommendation to do something

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

**may** indicates permission to do something

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

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

**can** indicates that something is possible

**cannot** indicates that something is impossible

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

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

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

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

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

In addition:

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

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

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

# Introduction

The 5G System supports a registration procedure with AMF re-allocation. As described in TS 23.502 [2], this procedure is used when the initial AMF is unable to serve the UE. In which case, the NAS message received from the UE is rerouted to another target AMF either directly over the AMF-to-AMF interface i.e. N14, or via RAN. In this document only the indirect reroute via RAN is considered.

# 1 Scope

This document aims at addressing the case for the indirect reroute procedure for UE registration. The intention is to enable deployment scenarios with stricter slice isolation requirements on the core network, for example where the AMFs are unable to communicate with each other.

The aim of this work is to:

- Collect the potential requirements related to the AMF re-allocation procedure

- Study the potential enhancements to the security mechanisms in order to fulfil the requirements for the AMF re-allocation

# 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".

…

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

[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 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); 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 Architecture and security assumptions of AMF re-allocation

Editor’s Note: This clause contains some introductory text on the problem of AMF re-allocation, i.e. what is already specified in SA2 and SA3 specifications.

## 4.1 General

Editor's Note: The assumptions and analysis in this document may need to be checked with SA1 and SA2.

The present document focuses on the problem of the security of the registration procedure with AMF re-allocation. More specifically TS 23.502 [2], clause 4.2.2.2.3, states that there are two cases for the AMF re-allocation procedure, the direct case 7(A) and the indirect case 7(B) via RAN. Currently only the direct AMF re-allocation case is considered complete from a security point of view and supported in Rel-15 and Rel-16 in TS 33.501 [3]. This study addresses the security handling of the indirect AMF re-allocation case. It is important to note that the indirect case in TS 23.502 [2], covers only the transfer of the NAS Registration Request message via a RAN node.

## 4.2 Procedure of Registration with AMF re-allocation

When an AMF receives a registration request from a UE, the AMF may need to reroute the request to another AMF because the AMF may not be able serve the UE. Figure 4.2-1 describes the registration procedure with AMF re-allocation specified in TS 23.502 [2].

（B）

（A）

Initial AMF

1. Registration Request

4. Security Mode Command

Target AMF

5. Security Mode Complete

2. Namf\_communication\_UEContextTrasnfer

Old AMF

(R)AN

UE

3. Primary Authentication

6. Decides NAS reroute is needed

7. Namf\_communication\_RegistrationStatusUpdate

8. Namf\_Communication\_N1MessageNotify

9a. Rereoute NAS message (RR)

9b. Initial UE message (RR)

10. Namf\_communication\_UEContextTrasnfer

11. NAS message

Figure 4.2-1: Registration with AMF re-allocation

1. The UE sends a Registration Request (RR). Either a 5G-GUTI or a SUCI is included.
2. If a SUCI is received in the RR, this step is skipped. If a 5G-GUTI is received and if there is connectivity between the initial AMF and the old AMF assigning the 5G-GUTI, the AMF retrieves the UE context from the old AMF that assigned the 5G-GUTI. The old AMF may perform horizontal key derivation and send to the initial AMF the derived security context.
3. The initial AMF initiates a round of primary authentication if a SUCI is received in step 1 or if the context retrieval in step 2 fails or if local policy at the initial AMF requires primary authentication.
4. The initial AMF may send a Security Mode Command to UE to activate the new security context established in step 3 or the derived security context in step 2.
5. The UE responds with a Security Mode Complete.
6. The UDM decides NAS reroute and obtains network slice information including Allowed NSSAIs, instances to serve UE, target AMF set, and etc.
7. If step 2 is not performed, this step is skipped. Otherwise, the initial AMF notifies the old AMF that the registration is not successful. The old AMF continues as if the Namf\_Communication\_UEContextTransfer in step 2 had never been received.
8. **Direct NAS Reroute**
9. If the initial AMF based on local configuration and subscription information decides to forward the NAS message the target AMF directly, then initial AMF sends, among others, UE’s security context and the RR to the target AMF.
10. **Reroute via RAN**
11. If the initial AMF based on local configuration and subscription information decides to forward the NAS message the target AMF via (R)AN, the initial AMF sends a Reroute NAS message to the (R)AN (step 9a). The reroute NAS message includes the RR message and the target AMF information. The (R)AN sends an Initial UE Message to the target AMF, including the RR and the slice information obtained in step 6 indicating reroute due to slicing.
12. This step is skipped if SUCI is included in the RR. If the RR message contains the 5G-GUTI and if there is connectivity between the target AMF and the old AMF assigning the 5G-GUTI, the target AMF retrieves the UE context from the old AMF.
13. The target AMF continues with the registration procedure.

## 4.3 Architecture and security assumptions

The UE may have been registered in the past to an old AMF (oAMF). For the current study it is assumed that the UE initiates a new registration request and this request is currently handled by the initial AMF (iAMF). In this request the UE provides protected slice selection information (NSSAI) either in a protected registration request message if it shares a security context with the network (oAMF) or after security is established with the iAMF in case of initial registration. As a result, for the iAMF to determine whether it can handle the UE registration, the initial AMF may need to retrieve any existing security context from the oAMF or establish new security with the UE. It is assumed that the (iAMF) does not have a communication interface (e.g. N14) to the tAMF. iAMF may or may not have a communication interface to the oAMF. The tAMF may or not have a communication interface to the oAMF. The different cases of connectivity among iAMF, tAMF, oAMF are captured in Figure 4.Y-1 and described below. The absence of communication interfaces is assumed to be due to isolation requirements on the AMFs or deployment restrictions.

The study aims at capturing such isolation requirements and solutions involving re-route of the registration request the related security handling.

The problem of AMF re-allocation via RAN includes two cases. In both cases the iAMF and the tAMF do not have any communication interface such as N14 between them as specified in TS 23.502 [2], clause 4.2.2.2.3. The two cases are the following:

1. Initial registration: The UE performs an initial registration providing a SUCI. The UE potentially interacts only with the iAMF and the tAMF. In order for the iAMF to determine if there is an AMF re-allocation, the iAMF needs to establish security with the UE and the UE needs to send the complete Registration Request including the protected IEs (such as the NSSAI) to the iAMF. After security is established between the UE and the network the UE does not accept any unprotected NAS messages according to TS 24.501 [4] clause, 4.4.4.2.

2. Mobility Registration Update: The UE has established security with the oAMF in the last registration. In this case the AMF re-allocation procedure may involves the iAMF, the oAMF and the tAMF. There are the following four subcases in this case:

a. The oAMF does not share any direct communication interface with the tAMF

i. The iAMF and the oAMF can communicate directly.

ii. The iAMF and the oAMF do not have any direct communication interface between them.

b. The oAMF shares a direct communication interface with the tAMF.

i. The iAMF and the oAMF can communicate directly.

ii. The iAMF and the oAMF do not have any direct communication interface between them.

The different cases are summarized in the figure 4.3-1 below. A line between two AMFs means that there exists a N14 interface between the two AMFs and security context can be transferred between them. If there is no line between the two AMFs, security context cannot be transferred directly between them.

 Figure 4.3-1. Different cases of communicating AMFs (solid line means that there is a N14 interface)

Editor's Note: It is FFS, if any new NF or an instance of the existing NF is required to assist the secure re-allocation procedure.”

# 5 Key issues

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

## 5.1 Key Issue #1: Security of AMF re-allocation procedures

### 5.1.1 Key issue details

This key issue addresses the security handling of the AMF re-allocation procedure upon UE registration with slicing requirements. The AMF re-allocation procedure due to slicing may involve more than one AMFs which may be isolated with each other due to deployment requirements. TS 23.502 [2] includes two cases of the re-allocation procedure, the direct case and the indirect case. The security handling of the direct case is specified in TS 33.501 [3] and the security handling of the indirect case is the objective of this key issue.

According to the specified AMF re-allocation procedure, when an Initial AMF receives a registration request, the Initial AMF may need to reroute the registration request to another Target AMF, e.g. when the Initial AMF is not the appropriate AMF to serve UE. The Initial AMF may not be connected to the Target AMF. One option for the AMF re-allocation is to reroute the AMF registration request through RAN, i.e., the Initial AMF (that is, the AMF receiving the registration request message) will send the registration request to the RAN, and the RAN then will forward the registration request to the Target AMF.

### 5.1.2 Security threats

In the indirect case of AMF re-allocation, the UE Registration Request is transferred from Initial AMF to Target AMF through RAN, due to the lack of connectivity between Initial AMF and Target AMF.

However, the existing security handling for this case may lead to consistent registration failure which threatens the availability of the system. More specifically, if Initial AMF and UE have securely exchanged NAS messages, the UE will reject the NAS message from Target AMF, due to the potential lack of access to the UE security context by the Target AMF or due to inconsistent security context used by the Target AMF. Inconsistent security context usage by the Target AMF happens when the Target AMF retrieves a security context from the old AMF, and it does not match the new security context used by the UE, as UE has established new security context with Initial AMF. This impact the UE service availability (i.e., leading to registration failure and service failure).

### 5.1.3 Potential security requirements

The AMF re-allocation via RAN shall not compromise system availability.

NOTE: The current isolation requirements considered in this study include only connectivity requirements between the involved AMFs in the AMF-reallocation procedure i.e. the Initial AMF, the Target AMF and potentially the Old AMF.

## 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.

## 6.1 Solution #1: AMF re-allocation via RAN using existing security states

### 6.1.1 Introduction

This solution addresses key issue #1.

### 6.1.2 Solution details

Editor’s Note: It is FFS to update the solution with a message flow to portray the scenarios addressed and assumptions.

For AMF re-allocation via the RAN, provided the initial AMF does not send a protected NAS message to the UE then there is no issue in establishing security between the UE and target AMF. This is because the UE will still accept the allowed unprotected messages and the UE and target AMF can agree on security context.

If the initial AMF (the one that received the Registration Request sent by the UE) sends a security protected message to the UE, this protected message causes the UE to drop all subsequent messages that do not pass integrity protection during the current connection. So, if the target AMF does not have the security context currently in use by the UE or a new security context derived from the current security context (e.g., due to KAMF change) then the target AMF will not be able to send a protected message to the UE. Hence the Target AMF cannot complete the registration procedure.

There is a second issue as follows. If the initial AMF changes the current security context at the UE from the one that was used to protect the registration (e.g. by running an Authentication followed by a NAS SMC procedure), then the target AMF will receive a registration message that is protected with a security context different to one the current one in the UE. This may lead, for example, to integrity check failure of a Registration Accept at the UE if the target AMF protects a Registration Accept with the security context (received from the old AMF) that the UE does not consider the current one.

The first issue is solved by having some secured signalling from the initial AMF to allow the UE to accept only the limited set of NAS messages that can be processed when received without security before the secure exchange of NAS message has been established (see clause 4.4.4.2 of TS 24.501 [4]). This is not introducing a new state in the UE but utilising an existing state, i.e. the one the UE is in when leaving idle with a security context.

Editor’s Note: Security risk of accepting the unprotected message defined in 4.4.4.2 of TS 24.501 after security activation is FFS

Editor’s Note: It is FFS, how the solution works when a Target AMF cannot communicate with the old AMF

The second issue is resolved by the initial AMF changing the ngKSI in the Registration Request before forwarding the Registration Request to the target AMF. For the case that the target AMF can communicate with the old AMF, this has the effect of the integrity check failure of the Registration Request at the old AMF as the old AMF does not have a security context indicated by ngKSI and consequently an authentication is triggered by the target AMF as it will not have a security context for the UE.

Editor’s Note: The impact of changing ngKSI is FFS

In the case that the target AMF can not communicate with the old AMF, then target AMF initiates an authentication with the UE as it does not have a security context for the UE.

### 6.1.3 Evaluation

TBD

## 6.2 Solution #2: Security of AMF re-allocation when 5G NAS security context is rerouted via RAN

### 6.2.1 Introduction

This solution address Key Issue #1: "Security of AMF re-allocation procedures ".

In this solution the 5G NAS security context is re-routed via RAN together with the Registration Request (RR) message.

### 6.2.2 Solution details

Before the Initial AMF re-routes the Registration Request (RR) message and the 5G NAS security context, the Initial AMF performs horizontal Kamf derivation of the current Kamf-0 and generates a new Kamf-1 key which is then routed via RAN to the Target AMF together with an indication of horizontal KAMF derivation (i.e., keyAmfHDerivationInd). The current Kamf-0 is not rerouted via RAN to the Target AMF. This would ensure that the Target AMF has no access to the Kamf-0 key used in the Initial AMF/old AMF.

The Initial AMF forwards the RR message, the 5G NAS security context including the Kamf-1 and the keyAmfHDerivationInd indicator unprotected to the Target AMF via RAN.

The new generated Kamf-1 key could be seen as a one-time key for the purpose of the AMF re-allocation. It is worth noting that Kamf-1 is practically useless to a legitimate RAN node since it is a NAS key that has not been put into use by any AMF in the network. The Target AMF would then be mandated to establish a new further key Kamf-2 with the UE, which is not available to the Initial AMF and the RAN.

Because the Target AMF has received the keyAmfHDerivationInd indicator, the Target AMF runs a NAS SMC procedure with the UE, to take the new Kamf-1 key into use with the UE. The Target AMF is also mandated to initiate a new primary authentication with the UE to derive a new Kamf-2 when it has received the RR message from the RAN. The new primary authentication procedure is protected by the Kamf-1. This step would ensure that the Initial AMF has no access to the new Kamf-2 key (i.e. the Kamf key used in the Target AMF and the UE).

The Target AMF runs a new NAS SMC procedure with the UE to take the new Kamf-2 into use with the UE.



Figure 6.2.2-1: AMF re-allocation with NAS message and 5G NAS security context re-route via RAN

Figure 6.2.2-1 shows the solution steps:

Step 1: The UE prepares a Registration Request message including 5G-GUTI and slicing information which could potentially cause an AMF re-allocation and its 5G-GUTI. The UE has a 5G NAS security context and protects therefore the Registration Request message.

Step 2: The RAN forwards the RR message to an Initial AMF.

Step 3/4: These steps may only take place if UE has indicated its 5G-GUTI in the Registration Request message. The Initial AMF contacts the old AMF and requests the 5G NAS security context from the old AMF. The old AMF may perform horizontal Kamf derivation of the Kamf key.

Step 5: The Initial AMF may initiate a new primary authentication. This step is optional. This step is mandatory if the UE has indicated its SUCI in the Registration Request message

Step 6: The Initial AMF initiates a NAS SMC. This step takes place if a prior primary authentication has taken place or if the old AMF has performed horizontal Kamf derivation of the Kamf key. The Initial AMF may include the request to the UE to include the complete Registration Request message by setting the flag "request initial NAS flag" if the old AMF has performed horizontal Kamf derivation of the Kamf key.

Step 7: The UE includes the complete RR message sent in step 1 in the NAS Security Mode Complete message. The RR message is both integrity protected and encrypted.

Step 8: If the Initial AMF needs UE's subscription information to decide whether to reroute the Registration Request and UE's slice selection subscription information was not provided by old AMF, the AMF selects a UDM as described in TS 23.501 [2], clause 6.3.8. the Initial AMF sends Nudm\_SDM\_Get to UDM.

Step 9: The UDM responds to Initial AMF with a Nudm\_SDM\_GetResponse. The AMF gets the Slice Selection Subscription data including Subscribed S-NSSAIs. The UDM responds with slice selection data to Initial AMF.

Step 10: If there is a need for slice selection, (see clause 5.15.5.2.1 of TS 23.501 [2]), e.g. the Initial AMF cannot serve all the S-NSSAI(s) from the Requested NSSAI permitted by the subscription information, the Initial AMF invokes the Nnssf\_NSSelection\_Get service operation from the NSSF by including Requested NSSAI.

Step 11: The NSSF performs the steps specified in point (B) in clause 5.15.5.2.1 of TS 23.501 [2]. The NSSF responds to Nnssf\_NSSelection\_Get to the Initial AMF.

Step 12: The Initial AMF decides to reroute the RR message to a Target AMF via RAN. The Initial AMF optionally performs horizontal Kamf derivation of Kamf-0 to generate a new Kamf-1. This step would ensure that target AMF has no access to the Kamf-0 key used in Initial AMF;

Step 13: The Initial AMF forwards the complete Registration Request message, the 5G NAS security context including the new Kamf-1 and the keyAmfHDerivationInd indicator to the RAN.

Step 14: The RAN confirms the reception of the RR message etc. to the Initial AMF.

Step 15: The RAN forwards the complete Registration Request message, the 5G NAS security context and keyAmfHDerivationInd indicator to the target AMF.

Step 16: If the target AMF has received the keyAmfHDerivationInd indicator, then the target AMF runs a NAS SMC procedure with the UE, to take the new Kamf-1 key into use with the UE.

Step 17: The target AMF initiates a new primary authentication with the UE to generate a new Kamf-2. The new primary authentication procedure is protected by the Kamf-1. This step would ensure that the Initial AMF has no access to the new Kamf-2 key generated between target AMF and the UE.

Step 18: The target AMF runs a new NAS SMC procedure with the UE to take the new Kamf-2 into use with the UE.

Editor's Note: The security impact of exposing Kamf to RAN is FFS.

Editor's Note: The requirement and processing of Reroute NAS response at step 14 is FFS.

### 6.2.3 Evaluation

TBD

## 6.3 Solution #3: Solving registration failure with AMF re-allocation via RAN

### 6.3.1 Solution Overview

The cause of registration failure issue lies in the fact that after NAS reroute via RAN to the target AMF, the UE and the target AMF may have inconsistent security contexts:

* If the UE registers with a SUCI, then the UE and the initial AMF will establish and activate new security context before RR rerouting. After RR rerouting via RAN, the target AMF cannot obtain the new security context. Target AMF will send unprotected authentication request to the UE. UE with security activated will discard it.

To solve this, the solution requires the UE to process the unprotected authentication request.

* If the UE registers with a 5G-GUTI and protects the RR with the old security context, the UE and the initial AMF may also establish and activate new security context before RR rerouting. After RR is rerouted via RAN to the target AMF, the target AMF cannot obtain the new security context. The target AMF may or may not be able to obtain the old security context. If the target AMF cannot obtain the old security context, the target will send unprotected authentication request and the UE will discard. If the target AMF can obtain the old security context, it may send a NAS protected using the old security context. The UE with the new security context, cannot process the NAS message.

To solve this, the solution also requires the UE to resume the old security context. The idea of requiring UE to resume the old security context is inspired by how UE handles handover failure specified in TS 33.501 [3], i.e. when handover fails, the UE discards the new NAS security context established in the handover and continue to use the existing security context.

### 6.3.2 Solution Details

Figure 6.3.2-1 shows the security handling with AMF reallocation via RAN.

UE

RAN

Initial AMF

Old AMF

1. Registration Request

6. Security Mode Complete

10a. Reroute NAS message

10b. Initial UE message

Target AMF

8.Namf\_communication\_RegistrationStatusUpdate(“NOT\_TRANSFERRED”)

2. Namf\_communication\_UEContextTrasnfer/Response

3. Primary authentication

4. Security Mode Command

5. Save the old NAS security context

9. NAS Message (Indication)

7. Decides to NAS reroute is needed and finds the Target AMF

11. Namf\_communication\_UEContextTrasnfer/Response

12. NAS message

13. Process the NAS message

Figure 6.3.2-1: Security handling in registration procedure with AMF re-allocation via RAN

1. The UE sends a RR with a SUCI or a 5G-GUTI.

If the UE has the capability to process unprotected authenticate request and resume the old security context in the case of AMF reallocation, the UE also includes an indicator indicating the capability in the RR.

NOTE: A Rel-17 UE is required to include the indicator in the RR.

1. If a 5G-GUTI is included in the RR and if there is connectivity between the initial AMF and the old AMF which assigned the 5G-GUTI, the initial AMF obtains the old security context from the old AMF. The old AMF may perform horizontal key derivation and send the initial AMF with the derived old security context.
2. The initial AMF may perform a round of primary authentication with the UE to establish new security context.
3. The initial AMF sends a security mode command (SMC) message if decides to take into use the new security context resulted from step 3 or the derived security context from step 2.
4. When the UE receives the SMC, the UE which includes the indicator in RR saves the old security context that has been established with the old AMF.
5. Then UE processes the SMC and returns a security mode complete (SMP) message.
6. The initial AMF decides to NAS rerouting is needed based on local policy and subscription information.
7. If step 2 occurs, the initial AMF notifies the old AMF that the registration at the initial AMF is not successful and the old AMF acts as step 2 did not occur.
8. If the UE and the initial AMF have activated security (i.e. SMC in step 4 and 6 have occurred),
	* if no indictor is received in the RR (i.e. meaning the UE is Rel-15 or Rel-16), the initial AMF performs direct NAS reroute according to local policy, as specified in Clause 4.2.2.2.3 of TS 23.502 [2] (Rel-15, Rel-16).
	* if the indictor is included in the RR,
		+ - if the initial AMF decides direct NAS reroute is needed according to local policy, then the initial AMF performs direct NAS reroute as specified in option (A) in Clause 4.2.2.2.3 TS 23.502 [2];
			- if the initial AMF decides NAS reroute via RAN is needed according to local policy, then the initial AMF sends an indication in a NAS message to the UE. The indication is to request the UE to perform the following: if an unprotected authentication request is received, the UE shall process it; if a protected NAS message is received, the UE shall resume the saved security context to process the NAS message.

The indicator is included in the RR and the description on the indicator is in step 1. Based on the indicator, the initial AMF is aware of UE’s capability to process unprotected authenticate request and resume the old security context in the case of AMF reallocation.

Editor's note: It is FFS, if the SA3 solution should change the way of determining the AMF reallocation and reroute type (direct/indirect) specified in TS 23.502.

1. The initial AMF reroute RR to the target AMF, if it decides RR reroute via RAN is needed.

11-12. After receiving the RR, if SUCI is included, the target AMF sends an unprotected authenticate request to the UE. If a 5G-GUTI is included in the RR,

* + - * If there is no connectivity between the target and old AMF, the target AMF sends an unprotected authenticate request to the UE.
			* If there is connectivity between the target and the old AMF, the target AMF may fetch the old security context from the old AMF and may send a NAS message protected using the old security context.
1. When a NAS message is received at the UE, if the indication is received in step 7,

- if the received NAS message is an unprotected authentication request, the UE, based on the indication received in step 7, will process the unprotected authentication request; or

- if the received NAS message is a protected NAS message, the UE, based on the indication received in step 7, will resume the saved old security context (in step 5) to process it.

Note: In step 13, having UE accept unprotected authentication request does not increase security risk.

Editor's note: It is FFS how the solution works when the target AMF sends a NAS SMC in step 13 before initiating a primary authentication.

### 6.3.3 Security Evaluation

TBC.

## 6.4 Solution #4: Solution to enable NAS Security for AMF reallocation and reroute via RAN Scenario

### 6.4.1 Introduction

The solution addresses key issue #1related to NAS security context handling in AMF reallocation and reroute (via RAN) scenario, where N14 interface may not be supported between the AMFs (example. for the target AMF due to strict slice isolation requirements).

The solution considers the following scenarios to address the registration failure(s) related to the AMF reallocation and reroute via RAN Scenario :

- During an initial registration procedure, N14 interface may not be supported between the initial AMF and target AMF.

- During a registration due to mobility, N14 interface may not be supported between the initial AMF and target AMF and there is also a possibility that N14 interface may not be supported between the reallocated AMF (i.e., target AMF) and the Source AMF (i.e., during Mobility registration update procedure).

### 6.4.2 Solution details

The solution enables NAS security availability in the Target AMF during an AMF re-allocation and reroute (via RAN) as shown in Figure 6.4.2-1. The solution involves a new NF (i.e., an instance of existing NF that is well-connected) that can store a security key in the network after a successful UE primary authentication and can provide an AMF key when required to the Target AMF which cannot communicate with an initial AMF and/or source AMF directly.



Figure 6.4.2-1: Enabling NAS Security for AMF re-allocation with NAS re-route via RAN using a new well-connected NF

**Case 1- Initial Registration:**

The steps involved in the solution shown in Figure 6.4.2-1 is described as follows.

Step 1-3. The UE sends the Registration Request to the initial AMF and the procedure shall follow similar to TS 23.502 [2] Clause 4.2.2.2.2. Where at this step, the UE and network authentication would have been successfully completed and following a successful primary authentication, the NAS security between the UE and the initial AMF would also have been successfully setup. The UE will contain the NAS security context. The initial AMF will contain the NAS security context for the UE.

Step 4. The initial AMF determines to reroute the NAS message to the Target AMF via NG-RAN (as the initial AMF is not the appropriate AMF to serve the UE based on TS 23.502 [2] Clause 4.2.2.2.3), but the main issue here is that the Target AMF cannot fetch the UE’s NAS security context (i.e., Kamf) from the initial AMF either directly (as there is no N14 interface) nor via NGRAN (as NAS security context cannot be exposed to the NGRAN performing the routing of initial NAS message). To facilitate NAS security context provisioning to the Target AMF for the corresponding UE’s ongoing registration procedure, a new NF is introduced which is slice agnostic, well-connected and located in the serving network. In the absence of N14 interface between the AMFs (i.e., Initial/Source AMF and Target AMF), the new NF acts as the UE security context storage and control function managing the security context at the serving network which is provided by the home network after a successful authentication. New NF governs slice security requirements and facilitates NAS security context sharing among AMFs when required during Initial Registration procedure and Registration mobility update procedures related to AMF reallocation with Reroute (via RAN). If the Initial AMF has the complete initial NAS message received from the UE in NAS SMC complete, the initial AMF can send the complete initial NAS message to the Target AMF via NG-RAN by requesting a Reroute NAS security context from the new NF to facilitate security context provisioning to the target AMF. The initial AMF sends an AMFRealloc\_Security Context Request message (over a new service-based interface) to the new NF which includes Target AMF information, AMF\_Reroute\_Security Required indication, and SUCI.

Step 5. On receiving AMFRealloc\_SecurityContext Request message, the new NF based on the SUCI finds the SUCI-SUPI pair from its local memory and then based on the retrieved SUPI identifies the locally stored security context. Further the new NF generates the reroute security context (NAS\_Sec\_ID) from the locally stored anchor key (i.e., a slice agnostic key). The new NF locally stores the derived reroute security context along with the Target AMF authentication. NAS\_Sec\_ID is the hash code of security anchor key SUPI and Target AMF information, which enables to authenticate the Target AMF for fetching any security context at a later point of time.

Editor’s Note: Whether RR and related information rerouted via RAN need to be protected against RAN is FFS.

Editor’s Note: How does the new NF obtain the anchor key and SUCI-SUPI is FFS.

Step 6. The new NF sends reroute security context (NAS\_Sec\_ID) to the initial AMF in the AMFRealloc\_Security Context Response message.

Step 7a. The initial AMF sends the reroute NAS message along with NAS\_Sec\_ID to the target AMF via RAN. The additional information also contains the Target AMF information as specified in step 7(B) TS 23.502 [2] clause 4.2.2.2.3.

Step 7b. The NG-RAN forwards the received reroute NAS message to the appropriate Target AMF as specified in step 7(B) TS 23.502 [2] clause 4.2.2.2.3.

Step 8. After receiving the reroute NAS message with NAS\_Sec\_ID, the Target AMF determines that, it should fetch the corresponding security context from the new NF to handle the received rerouted NAS message. The Target AMF if required locally stores the received rerouted NAS message along with SUCI and NAS\_Sec\_ID (as part of Re-route security information).

Step 9. The Target AMF on receiving NAS\_Sec\_ID sends the NASKey\_Request message to the new NF containing the SUCI, NAS\_Sec\_ID, and Target AMF information (such as AMF ID or NSI ID etc).

Step 10. The new NF on receiving the NAS\_Sec\_ID, SUCI and AMF information, it verifies the NAS\_Sec\_ID to authenticate the Target AMF to provide the security information. If the NAS\_Sec\_ID validation is successful, the new NF generates the new NAS security context (Kamf) to be provided for the Target AMF.

Step 11. The new NF sends to Target AMF the NASKey\_Response message containing SUPI, NAS\_Sec\_ID, Kamf, N-NSCI (to indicate the Target AMF that the Kamf is derived from the anchor key). and a special ABBA parameter (to indicate Slice specific security feature defined for 5G)

Step 12. The Target AMF initiates a NAS security mode command with the UE to align the new NAS security context with the UE. The Target AMF locally stores the received SUPI, Reroute Security context (NAS\_Sec\_ID), N-NSCI, Kamf, and the special ABBA parameter along with the ngKSI.

Step 13. The Target AMF selects the NAS security algorithms (integrity and ciphering algorithms) based on the UE security capabilities and sends a NAS security mode command message with the UE which contains the New NAS Security Context Indicator (N-NSCI), and the special ABBA parameter value.

Step 14. The UE on receiving the N-NSCI in the NAS Security mode command message, uses an anchor key locally stored or newly derived one to derive a Kamf similar to the new NF and the one available in the Target AMF. The UE uses the special ABBA value and N-NSCI received in the Kamf generation.

Step 15. The UE after a successful validation of the NAS Security mode command message, sends a NAS security mode complete message to the Target AMF.

After a successful NAS Security mode command procedure between the target AMF and UE, the target AMF sends an initial Context setup message to the NG-RAN to initiate AS SMC between the UE and NG-RAN to set up AS Security based on the new NAS security context available in the Target AMF. Rest of the procedure executes similar to the existing 5G System.

Editor’s Note: The need for the anchor key, the need for its further uses and its provisioning is FFS.

**Case 2- Registration Mobility Update Procedure:**

Editor’s Note: This section will capture the adaptations required for steps shown in Figure 6.4.2-1 to address AMF-reallocation related to registration mobility update procedure.

Editors’ Note: How to solve idle mobility registration with 5G-GUTI is FFS.

### 6.4.3 Evaluation

TBD

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

### 6.Y.1 Introduction

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

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

# 7 Conclusions

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

# Annex A (informative)

## A.1 Registration failure issue with AMF re-allocation via RAN

### A.1.1 General

This clause analyses the registration failure issue with AMF re-allocation via RAN.

### A.1.2 Description of Registration Failure Issue

The registration failure case in the***initial***registration where no usable security context at UE at the time of registration is depicted in Figure A.1.2-1.

UE

(R)AN

Initial AMF

Target AMF

AUSF

1. RR (SUCI)

2. Primary Authentication

1. NAS Security Mode Command/Complete

5a. Reroute NAS message(RR)

5b. Initial NAS message(RR)

7. Authentication Request

UE discards unprotected Authentication Request

8. Registration Reject

6. Nausf\_UEAuthentication\_Authenticate/Response

4. Decides NAS reroute via RAN is needed

Figure A.1.2-1: Registration with SUCI

1-2. The initial AMF, upon the reception of the Registration Request with SUCI, initiates the primary authentication with the UE.

1. The initial AMF sends the NAS Security Mode Command (SMC) to the UE. The UE replies with NAS Security Mode Complete message containing a complete RR message.
2. The initial AMF decides to reroute the RR to the Target AMF.
3. The initial AMF reroutes the Registration Request to the target AMF, via (R)AN.
4. The Target AMF initiates the primary authentication. The Target AMF fetches RAND, AUTN and other parameters from the AUSF.
5. The Target AMF sends Authentication Request message to UE. As the Target AMF possesses no NAS security context of the UE, Authentication Request message is sent unprotected.

The UE, upon the reception of the unprotected Authentication Request message, will discard it. This is because UE has NAS security activated, and hence the UE will discard the Authentication Request message.

Eventually the registration will fails after timeout. Later even if the UE tries registering again, the above procedure still applies and registration will never be successful, hence the UE is denied service.

Figure A.1.2-2 depicts the registration failure in idle mobility registration.

The registration failure in theregistration with a GUTI is depicted in Figure A.1.2-2.

UE

(R)AN

Initial AMF

Old AMF

1. Registration Request(5G-GUTI)

4. Security Mode Command/Complete

5. Decides NAS reroute via (R)AN is needed

7a. Reroute NAS message (RR)

7b. Initial NAS message (RR)

Target AMF

8. Namf\_communication\_UEContextTrasnfer/Response

6.Namf\_communication\_RegistrationStatusUpdate(“NOT\_TRANSFERRED”)

2. Namf\_communication\_UEContextTrasnfer/Response

3. Primary authentication

9. NAS message

Figure A.1.2-2: Registration with GUTI.

1. The UE sends an integrity protected the Registration Request (RR) message with a 5G-GUTI.
2. This step is skipped if no connectivity between the initial and old AMF. Otherwise, the initial AMF based on the received 5G-GUTI, fetches the UE context from the old AMF.
3. The initial AMF chooses to perform a primary authentication run based on local policy or the retrieval of UE context is not successful.
4. The initial AMF may initiate the Security Mode Control procedure with the UE.
5. The initial AMF decides that NAS reroute via (R)AN is needed.
6. This step is skipped if there’s no step 2. Otherwise, the initial AMF notifies the old AMF that the registration of UE at the initial AMF fails. The old AMF then acts as if the UE context request has never been received in Step 2. The NAS security context including the NAS counts and keys change back to the values before Step 2.
7. The initial AMF reroutes the RR to the target AM via (R)AN.
8. If the target and old AMF have connectivity, the target AMF fetches the UE context from the old AMF. If the target and old AMF have no connectivity, this step is skipped.
9. Target AMF sends a NAS message to the UE.

There are 8 registration failure cases described below that can happen in the above procedure. In what follows, we use the following notations:

* Kamf : the AMF key that was established between the UE and the old AMF
* Kamf’: the key generated by performing the horizontal key derivation based on Kamf
* Kamf ” : the key generated by performing the horizontal key derivation based on Kamf’
* Kamf\_new: the AMF key generated from an authentication run.

In the registration failure Case 1, 2, and 3 below, the old AMF have derived and sent Kamf’ to the initial AMF in step 2; The initial AMF have decided to use Kamf’ and then have sent the Security Mode Command, with an indication requesting the complete registration request message, to the UE. After step 4, the UE and the initial AMF have established and activated the NAS security context containing Kamf’.

Case 1: In step 8, the target AMF receives Kamf from the old AMF, and the target AMF decides to use Kamf. The target AMF will protect the subsequent outgoing NAS message based on Kamf. When the UE receives the NAS message, the integrity check will fail, as UE uses Kamf’, while the target AMF uses Kamf. Hence, the registration will fail.

Case 2: In step 8, the target AMF receives Kamf’ and keyAMFHDerivation indicator from the old AMF, and the target AMF decides to use Kamf’. Then the target AMF sends a SMC, integrity protected based on Kamf’, to the UE. The SMC contains K\_AMF\_change\_flag. The UE, upon receiving the SMC with K\_AMF\_change\_flag, performs horizontal key derivation based on Kamf’ and obtains Kamf ”. Then the UE verifies the integrity of the SMC, based on Kamf ”. The verification will fail, as the SMC is integrity protected based on Kamf’. Hence the registration will fail.

Case 3: The target AMF decides not to use the keys received from the old AMF in Step 8, but performs an authentication run in step 9, and sends Authentication Request unprotected to the UE. The UE, however, will discard the Authentication Request.

In the registration failure Case 4, 5, and 6 below, the initial AMF performs an authentication run in Step 3. NAS Security Mode Control procedure has been initiated by the initial AMF to activate the new NAS security context. After step 4, the UE and the initial AMF have established and activated the new NAS security context containing Kamf\_new.

Case 4: In step 8, the target AMF receives Kamf from the old AMF, and the target AMF decides to use Kamf. The target AMF will protect the subsequent outgoing NAS message based on Kamf. When the UE receives the NAS message, the integrity check will fail, as UE uses Kamf\_new, while the Target AMF uses Kamf. Hence, the registration will fail.

Case 5: In step 8, the target AMF receives Kamf’ and keyAMFHDerivation indicator from the old AMF, and the target AMF decides to use Kamf’. Then the target AMF sends a SMC, integrity protected based on Kamf’, to the UE. The verification of SMC will fail at the UE, as the SMC is integrity protected based on Kamf’, but UE uses Kamf\_new.

Case 6: The target AMF performs an authentication run and sends Authentication Request unprotected to the UE in step 9. The UE, however, will discard the Authentication Request, because the UE already has NAS security activated and will discard unprotected NAS messages.

In the registration failure case 7 and 8 below, the old AMF returns Kamf to the initial AMF in step 2; the initial AMF decides to use Kamf, meanwhile the initial AMF selects different security algorithm than that selected by the old AMF. Then the initial AMF initiates Security Mode Control procedure (Step 4) with the UE to update the security algorithm to be used. After Step 4, the UE and The initial AMF has established and activated the NAS security context containing Kamf and the new selected security algorithm. The Security Mode Control procedure also updates the NAS counts.

Case 7: In Step 8 the target AMF receives Kamf from the old AMF. The target AMF decides to use Kamf and protect the subsequent outgoing NAS message based on Kamf. When receiving the NAS message, the UE discards the NAS message, because the DL NAS count in the NAS message is not acceptable by the UE. The UE considers this NAS message as a replay message.

Case 8: The target AMF performs an authentication run in step 9 and sends the Authentication Request unprotected to the UE. The UE will discard the Authentication message.

# Annex X (informative):Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2020-10 | SA3#100bis-e | S3-202310 |  |  |  | TR skeleton. | 0.0.0 |
| 2020-10 | SA3#100bis-e | S3-202734 |  |  |  | Version after incorporating changes in S3-202725, S3-202726. | 0.1.0 |
| 2020-11 | SA3#101-e | S3-203392 |  |  |  | Version after incorporating changes in S3-203395, S3-203419, S3-203420, S3-203421, S3-203445, S3-203446, S3-203465. | 0.2.0 |