|  |  |
| --- | --- |
| 3GPP TR 33.864 V0.4.0 (2021-03) | |
|  | |
| 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 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 5

Introduction 6

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 8

3.3 Abbreviations 8

4 Architecture and security assumptions of AMF re-allocation 8

4.1 General 8

4.2 Procedure of Registration with AMF re-allocation 8

4.3 Architecture and security assumptions 10

5 Key issues 11

5.1 Key Issue #1: Security of AMF re-allocation procedures 11

5.1.1 Key issue details 11

5.1.2 Security threats 12

5.1.3 Potential security requirements 12

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

5.X.1 Key issue details 12

5.X.2 Security threats 12

5.X.3 Potential security requirements 12

6 Solutions 12

6.1 Solution #1: AMF re-allocation via RAN using existing security states 12

6.1.1 Introduction 12

6.1.2 Solution details 12

6.1.2.1 Overview 12

6.1.2.2 Message flows 13

6.1.3 Evaluation 15

6.2 Solution #2: Security of AMF re-allocation when 5G NAS security context is rerouted via RAN 16

6.2.1 Introduction 16

6.2.2 Solution details 16

6.2.3 Evaluation 19

6.3 Solution #3: Solving registration failure with AMF re-allocation via RAN 20

6.3.1 Solution Overview 20

6.3.2 Solution Details 20

6.3.3 Security Evaluation 24

6.4 Solution #4: Solution to enable NAS Security for AMF reallocation and reroute via RAN Scenario 24

6.4.1 Introduction 24

6.4.2 Solution details 24

6.4.3 Evaluation 28

6.5 Solution #5: AMF re-allocation by re-directing UE to new AMF 29

6.5.1 Solution Overview 29

6.5.2 Solution Details 30

6.5.2.1 Handling Different cases of communicating AMFs (Figure 4.3-1) 31

6.5.3 Evaluation 32

6.6 Solution #6: Solution to provide Security context to AMF capable of serving the UE to ensure system availability 32

6.6.1 Introduction 32

6.6.2 Solution details 32

6.6.3 Evaluation 36

6.7 Solution #7: Solution to enable Reallocated AMF to serve the UE 37

6.7.1 Introduction 37

6.7.2 Solution details 37

6.7.3 Evaluation 41

6.8 Solution #8: Solution to enable UE connection directly to the slice AMF 42

6.8.1 Introduction 42

6.8.2 Solution details 42

6.8.2.1 Solution phase 1 42

6.8.2.2 Solution phase 2 43

6.8.3 Evaluation 44

6.9 Solution #9: Security of AMF re-allocation when 5G NAS security context is rerouted via RAN 44

6.9.1 Introduction 44

6.9.2 Solution details 44

6.9.3 Evaluation 48

7 Conclusions 49

Annex A (informative) 50

A.1 Registration failure issue with AMF re-allocation via RAN 50

A.1.1 General 50

A.1.2 Description of Registration Failure Issue 50

Annex X (informative): Change history 54

# 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".

[5] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP) "

# 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 initial AMF 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.

1. **Direct NAS Reroute**

8. 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.

1. **Reroute via RAN**

9. 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.

10. 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.

11. 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). 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 iAMF 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. The 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 4.3-1 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.

Editor's Note: Whether the cases can fulfills vertical requirement is FFS.

Editor's Note: Which existing NF in the registration procedure is used as common NF in the solutions is FFS.

Editor's Note: Whether UE contexts can be transferred between AMFs in separated slices indirectly via common NF is FFS.

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)

# 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.

# 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

#### 6.1.2.1 Overview

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

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.

In the case that the target AMF cannot 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.

#### 6.1.2.2 Message flows

Figure 6.1.2.2-1 provides the message flow for the solution. The flow assumes that an AMF re-allocation will be used and only shows the interactions between AMFs, between UE and AMF and AMF and NG-RAN, e.g. the parts of authentication involving the AUSF etc. in the home network are not shown.



Figure 6.1.2.2-1: AMF re-allocation via the RAN

Step 1: The UE sends the Registration Request message, that includes an indication that the UE supports the enhanced functionality to allow AMF re-allocation via the RAN as a non-cleartext IE in the case the Registration Request contains a GUTI, to the network which is routed by the NG-RAN node to Initial AMF.

Step 2: If the Registration Request contains a GUTI and there is a connection between the initial AMF and the old AMF, the initial AMF tries to fetch the UE context from the old AMF.

Step 3: If the integrity check of the Registration Request message is passed, then old AMF provides the UE context to the initial AMF. In addition, the old AMF may provide the decrypted Registration Request message to the initial AMF.

NOTE 1: Providing the decrypted Registration Request message to the initial AMF is an optimization that can save messages, i.e. it is not necessary for the procedure to work. Whether this is sufficiently useful to include is part of the evaluation of the solution.

If the Registration Request message contained a SUCI, then steps 5 and 6 are mandatory. If the initial AMF has received the decrypted Registration Request message from the old AMF or can decrypt a protected Registration Request, then the steps 4 to 6 are optional. Otherwise the initial AMF needs to identify the UE and steps 4 to 6 are mandatory.

Step 4: The initial AMF send and Identity Request to the UE and receives the UE’s SUCI in response.

Step 5: Initial AMF trigger and complete an authentication run with the UE.

Step 6: Initial AMF runs the NAS SMC procedure with the UE. [Option-1] As part of the NAS Security Mode Command messages, the AMF indicates to the UE to respond with a protected NAS Security Mode Complete message and then behave as though the secure exchange of NAS messages has not been established, e.g. accept the small set of NAS message given in clause 4.4.4.2 of TS 24.501 [4] as being acceptable to receive without integrity protection. The initial AMF obtains the complete Registration Request message, which contains the indication that the UE supports the enhanced functionality to allow AMF re-allocation via the RAN as a non-cleartext IE.

NOTE 2: If [Option-1] is used, then if the AMF can not rule out re-allocating the UE via RAN then it include the above indication in the NAS Security Mode Command message, which is ignored by a UE that does not understand the new behaviour. Regardless of whether a re-allocation occurs, then the legacy behaviour of a protected message from an AMF will establish the secure exchange of NAS messages at the UE.

NOTE 3: Only one of [Option-1] in above step or [Option-2] in step 8 needs to be standardised. The choice between these options is FFS.

Step 7: From the complete Registration Request message (obtained in step 3 or 6), the initial AMF determines that the UE needs to be re-allocated to the target AMF via the RAN.

Step 8: [Option-2] The initial AMF send the UE an integrity protected message to inform the UE to act as though the secure exchange of NAS messages has not been established, e.g. accept the small set of NAS message given in clause 4.4.4.2 of TS 24.501 [4] as being acceptable to receive without integrity protection.

NOTE 4: Which message this is and whether to use this approach or [Option-1] (see NOTE 3) is FFS.

Step 9: If the initial AMF changed the security context from the one that the UE used to protect the Registration Request message, the initial AMF shall change the ngKSI in the received Registration Request in step 1. The AMF forwards the (possibly with the changed ngKSI) Registration Request to the target AMF vis the RAN.

NOTE 5: Changing the ngKSI does not change the state of either the UE or any of the involved AMFs. The reason for doing it is to keep the UE and target/old AMF up to date on the security context being used by the UE to avoid possible errors, e.g. the target AMF thinking that the security context sent by the old AMF is the current one in the UE. The initial AMF can change the ngKSI to any value to enforce a context retrieval failure at the target AMF.

Step 10: The target AMF completes the registration procedure with the UE, e.g. if it cannot get the context from the old AMF it runs its own authentication.

NOTE 6: Any attempt to fetch the context from the old AMF using the Registration Request will fail if the initial AMF changed the ngKSI in the Registration Request before forwarding it to the target AMF (via the RAN). This causes no loss of MM context as these can be fetched from the old AMF using SUPI once the UE has been authenticated (see clause 4.2.2.2.2 of TS 23.502 [2]).

### 6.1.3 Evaluation

UE includes an indication of its support of the enhanced functionality to support AMF re-allocation via the RAN (see step 1 in clause 6.1.2.2).

Old AMF has the option to provide a decrypted Registration Request to the initial AMF (see step 3 in clause 6.1.2.2). This optional part of the solution requires the old AMF to support the capability to decrypt RR and send the decrypted RR in the context retrieval and is not used when UE sends RR with SUCI included.

Initial AMF either explicitly signals in the NAS Security Mode Command message that the UE is to not consider the secure exchange of NAS messages to be established when it has processed this NAS Security Mode Command (step 6) or sends an extra integrity message to get the UE to inform the UE to consider the secure exchange has not been established after receiving this message (step 8).

NOTE 1: This choice is left FFS.

The initial AMF changes the ngKSI in the Registration Request if it has established (or created) a new security context different from the one used to protect the Registration Request that the UE sent (step 9).

With the changed ngKSI, after the target AMF receives the RR with the changed ngKSI, the target AMF will retrieve UE context from the old AMF. The context retrieval will fail due to the changed ngKSI. Then target AMF is mandated to perform primary authentication. After primary authentication, the target AMF will need to retrieve UE context again from the old AMF.

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 needs to run 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).

As the target AMF can determine that a NAS re-route via RAN has taken place, the target AMF needs to restrict the use of the Kamf-1 only for the purpose of sending protected NAS Security Mode Command and Authentication Challenge/Request to the UE, and for receiving protected NAS Security Mode Complete and Authentication Response from the UE.

The Target AMF needs to run a new NAS SMC procedure with the UE to take the new Kamf-2 into use with the UE. The initial AMF needs to indicate to the UE to include the complete Registration Request message in the NAS Security Mode Complete message by setting the flag "request initial NAS flag" in the NAS Security Mode Command message. The UE includes the complete Registration Request message (sent in step 1) in the NAS Security Mode Complete message to the target AMF. This means that the target AMF can take the Registration Request message received in NAS Security Mode Complete message into use and drop the Registration Request message rerouted via RAN.



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 a SUCI or a 5G-GUTI and slicing information which could potentially cause an AMF re-allocation such as Requested NSSAI. If the UE has a 5G NAS security context (Registration with 5G-GUTI) it includes a protected NAS container in the Registration Request message.

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

Step 3a and 3b: These steps may only take place if UE has indicated its 5G-GUTI in the Registration Request message and there is connectivity between the initial AMF and the old AMF (cases 2.a.i and 2.b.i in clause 4.3). 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.

If there is no connectivity between the initial AMF and the old AMF (cases 2.a.ii and 2.b.ii in clause 4.3) and the UE has indicated its 5G-GUTI in the Registration Request message, then steps 3a and 3b are skipped and the initial AMF requests the UE identity SUCI from the UE in step 4 and then initiates primary authentication in step 5.

Step 4: The initial AMF may request UE identity SUCI from the UE.

Step 5: The Initial AMF may initiate a new primary authentication. This step is optional. This step is needed 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 or the Registration Request included the UE SUCI.

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. If the Initial AMF performs horizontal Kamf derivation then the initial AMF resets the corresponding uplink and downlink NAS COUNTs to 0.

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

Step 14: The RAN forwards the complete Registration Request message, the 5G NAS security context and keyAmfHDerivationInd indicator to the target AMF.

Step 15. After receiving the Registration Request,

If SUCI is included in the Registration Request, the target AMF skips step 15 (as no additional information about established PDU sessions etc. is stored in the old AMF).

If a 5G-GUTI is included in the Registration Request and the target AMF has received a 5G NAS security context and potentially a keyAmfHDerivationInd indicator, then:

- If there is no connectivity between the target AMF and old AMF (cases 2.a.ii and 2.b.ii in clause 4.3) , the target AMF skips step 15 (and any additional information about established PDU sessions etc. stored in the old AMF cannot be retrieved by the target AMF).

- If there is connectivity between the target AMF and the old AMF(cases 2.a.i and 2.b.i in clause 4.3), the target AMF can fetch any additional information about established PDU sessions etc. stored in the old AMF.

Editor's Note: How the solution works if the old AMF provides current 5G Security context to the target AMF is FFS.

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

Step 17: The target AMF needs to initiate 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.

Target AMF determines that a NAS re-route via RAN has taken place and the target AMF shall use the Kamf-1 only for the purpose of sending protected NAS Security Mode Command and Authentication Challenge/Request to the UE, and for receiving protected NAS Security Mode Complete and Authentication Response from the UE.

Step 18a-b: The target AMF needs to run a new NAS SMC procedure with the UE to take the new Kamf-2 into use with the UE. The target AMF needs to include the request to the UE to include the complete Registration Request message in the NAS Security Mode Complete message by setting the flag "request initial NAS flag" in the NAS Security Mode Command message. The UE includes the complete Registration Request message (sent in step 1) in the NAS Security Mode Complete message to the target AMF. This means that the target AMF can take the Registration Request message received in NAS Security Mode Complete message into use and drop the Registration Request message rerouted via RAN.

### 6.2.3 Evaluation

In this solution there is one more additional NAS SMC in the target AMF after the Registration Request message and the 5G NAS security context including the new Kamf-1 key has been re-routed via RAN, in order to take the new Kamf-1 key into use by the UE and target AMF (after the new horizontal Kamf derivation of Kamf-0 to generate a new Kamf-1 in Initial AMF).

Horizontal Kamf derivation in the initial AMF provides **backward security** so the target AMF has no access to the Kamf-0 and its corresponding NAS key used between the UE and the initial AMF. The initial AMF has access of the new Kamf-1 key re-routed via RAN to the target AMF, but after the target AMF has taken the new Kamf-1 key into use with the UE by running a NAS SMC, the target AMF can initiate a new protected Authentication procedure with the UE in order to generate a new Kamf-2 key shared with the UE, which the initial AMF has no access to. By running a new NAS SMC procedure between target AMF and UE to take the new Kamf-2 key into use, **forward security** is provided.

This solution has the following impact:

UE:

Editor's Note: UE impact is FFS

AMF:

This initial AMF needs to perform horizontal Kamf derivation of the Kamf before forwarding the 5G NAS security context together with the complete Registration Request message on the N2 interface to the RAN. The target AMF needs to process the new Reroute NAS message. The target AMF also needs to perform an authentication request in order to produce its own security context.

RAN:

- This solution has impact on RAN and N2 interface. The REROUTE NAS REQUEST message is defined in TS 38.413 [5] and the Initial AMF includes the INITIAL UE MESSAGE into the REROUTE NAS REQUEST message to RAN, but the REROUTE NAS REQUEST message needs to be updated to include the 5G NAS security context as well as it is currently not supported. Also the RAN needs to forward the 5G NAS security context to the Target AMF together with the INITIAL UE MESSAGE.

This solution proposes to route the 5G NAS security context via RAN and exposes the Kamf-1 key to the RAN which may impose a security threat so that an attacker in RAN can derive further NAS security keys and initiate attacks on the core network and the UE. Such exposure of NAS keys to RAN has not been done before and has risks. The risks were minimized by the following design:

A. The RAN is still a trusted network entity according to TS 33.501[2], clause 5.3.8.

B. The Kamf-0 key is never exposed to RAN. Due to performing horizontal Kamf derivation of the Kamf-0 key in the initial AMF and only providing the new horizontally derived Kamf-1 to the 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.

C. The target AMF needs to take the new generated Kamf-1 key received from RAN into use with the UE by running a NAS SMC procedure prior to initiating a primary authentication immediately thereafter in order to replace the Kamf-1 key received from the RAN with a new Kamf-2 key. The Kamf-1 key is invalidated as soon as the Kamf-2 key is activated after a new primary authentication. So, the Kamf-1 key becomes immediately useless.

D. Before the new primary authentication procedure is initiated in order to replace the Kamf-1 key with a new Kamf-2 key, there are risks as an attacker in RAN which has access to Kamf-1 key could misuse the key and perform attacks on the UE and the target AMF. As the target AMF can determine that a NAS re-route via RAN has taken place, the target AMF can restrictively use the Kamf-1 only for the purpose of sending protected NAS Security Mode Command and protected Authentication Challenge/Request to the UE, and for receiving protected NAS Security Mode Complete and protected Authentication Response from the UE.

## 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

3b. 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

3a. ID Request/Response

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 ID 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.

2. 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. If there is no connectivity between the initial and old AMF, step 2 is skipped and the initial AMF will request ID from the UE and then initiates primary authentication in step 3.

3. The initial AMF may initiate ID request to obtain SUCI and perform a round of primary authentication with the UE to establish new security context.

4. 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 obtained from Old AMF from step 2.

5. 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.

6. Then UE processes the SMC and returns a security mode complete (SMP) message.

7. The initial AMF decides that NAS rerouting is needed based on local policy and subscription information.

8. 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.

9. The initial AMF may decide NAS reroute via RAN is needed according to local policy. Then, if an indicator is received in step 1, 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 or ID 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 ID request and resume the old security context in the case of AMF reallocation.

NOTE 1: It is up to stage 3 spec to decide whether a UE needs to send back an ACK to the initial AMF.

10. 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.

13. When a NAS message is received at the UE, if the indication is received in step 9,

- if the received NAS message is an unprotected authentication request or ID request, the UE, based on the indication received in step 9, 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 9, will resume the saved old security context (in step 5) to process it.

NOTE 2: In step 13, having UE accept unprotected authentication request does not increase security risk.

The following analyses the solution for all the possible connectivity options among the initial AMF (iAMF), old AMF (oAMF) and target AMF (tAMF).

Case 1: no oAMF

The UE includes SUCI in RR in step 1. Later in step 10, the RR with SUCI is rerouted to the tAMF.

After the tAMF receives the rerouted RR message with SUCI in step 10, the tAMF initiates the primary authentication and sends UE with unprotected authentication response messge. The UE, based on the indication received in step 7, will process the authentication message.

Case 2.a.i: iAMF and oAMF can communicate; tAMF and oAMF cannot communicate.

The UE includes GUTI in RR in step 1.

After the tAMF receives the rerouted RR message with GUTI in step 10, the tAMF sends unprotected ID request to the UE. The UE, based on the indication received in step 7, will process the ID request messge and returns SUCI to the tAMF. The tAMF will obtains authentication token from the home network by providing SUCI. After that, the tAMF will send unprotected authentication reques to the UE. The UE, based on the indication received in step 7, will process the unprotected authentication request.

Case 2.a.ii: no communication allowed among iAMF, oAMF and tAMF

The UE includes GUTI in RR in step 1.

After the tAMF receives the rerouted RR message with GUTI in step 10, the tAMF performs the same as in Case 2.a.i., i.e. ID request and then primary authentication.

Case 2.b.i

The UE includes GUTI in RR in step 1.

The iAMF retrieves UE security context from the oAMF in step 2. The oAMF may perform horizontal key derivation.

After obtain the horizontal key derivation, the iAMF may perform one of the following:

1) Decide not to use the received security context, but perform authentication to create new security context. NAS SMC is performed to activate the new security context.

2) Decide to use the received security context from the oAMF

a) If the oAMF has performed horizontal Kamf derivation and sent the derived security context to the iAMF, then the iAMF will send NAS SMC protected by the derived security context. The NAS SMC also included an indicator to indicate the UE to perform horizontal Kamf derivation. The UE, based on the indication performs horizontal Kamf derivation.

b) If the oAMF has not performed horizontal Kamf derivation and sent the old security context to the iAMF, the iAMF is able to verify and decrypt the received RR message, and obtain requested S-NSSAIs. In this case, the iAMF is able to determine whether NAS reroute is needed without security activation, hence the regsitraton failure in the key issue does not exist.

After the tAMF receives the rerouted RR message with GUTI in step 10, the tAMF retrives UE context from the oAMF in step 11. The oAMF may perform horizontal Kamf derivation and returns the derived security context. After obtains the security context from the oAMF, the tAMF may perform one of the following:

1) Decide not to use the received security context from the oAMF, but perform authentication; therefore, the tAMF sends ID request to the UE to obtain SUCI and later sends authentication request to the UE. UE, based on the indication received in step 9, will process the ID request and authentication request.

2) Decide to use the received security context from the oAMF.

a) If oAMF has performed horizontal Kamf derivation based on the old security context and sent the derived security context to the tAMF, then the tAMF will send NAS SMC protected by the derived security context. The NAS SMC also included an indicator to indicate the UE to perform horizontal Kamf derivation. The UE, based on the indication received in step 9, resume the old security context, and then performs horizontal Kamf derivation and use the derived key to verify the NAS SMC.

b) If oAMF has not performed horizontal Kamf derivation and sent the old security context to the tAMF, the tAMF will use old security context to protect the NAS message to the UE. The UE based on the indication received in step 9, will resume the old security context and verify the received NAS message.

Case 2.b.i may need to be aligned with vertical requirement later if required.

Case 2.b.ii

The UE includes GUTI in RR in step 1.

The initial AMF performs primary authentication and NAS SMC. Then the intial AMF decides to reroute NAS via RAN. The RR is rerouted to the target AMF via RAN.

After the tAMF receives the rerouted RR message with GUTI in step 10, the tAMF retrives UE context from the oAMF in step 11. The oAMF may perform horizontal Kamf derivation and returns the derived security context. After obtains the security context from the oAMF, the tAMF performs the same as in Case 2.b.i.

### 6.3.3 Security Evaluation

The solution addresses Key Issue # 1. The solution impacts UE and the initial AMF.

**Impact on the UE:**

- In the solution, the UE includes an indictor for the capability in the RR. UE is required to support the capability to processes unprotected authentication request and ID request, as well as to resume the old security context.

**Impact on the initial AMF:**

- The initial AMF receives the indicator in the RR and sends to the UE an indication to instruct the UE to proccess the unprotected authentication request or ID requset and also resume old security context.

The solution does not require transfer of security context between two separated slices.

For case 2.b.i, where the iAMF and tAMF both can communicate with oAMF, iAMF and tAMF can obtain and use the security context from oAMF. Case 2.b.i need to be aligned with vertical requirement.

Editor's Note: Impacts on UE and other NFs are FFS.

## 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 #1 related 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 and takes into account the architecture and security assumptions specified in Clause 4.3 of this document to address the corresponding registration failure(s):

- 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/old AMF.

### 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 uses the AUSF involved in the authentication procedure of the UE to act as a common NF (i.e., an instance of existing NF that can be trusted and accessible to all AMFs in the serving network) to generate/store a security key in the network after a successful UE primary authentication and provide an AMF key when required for the Target AMF which cannot communicate with an initial AMF and/or source AMF directly. The AUSF in the home network is considered to be a trusted NF in the core network, as it will be involved during the primary authentication of the UE. Further the AUSF in the home network can provide AMF Re-allocation Security Service to the requester NF (i.e., initial AMF) by Nausf\_AMFRealloc\_SecurityContext service operation and can provide Key service to the requester NF (i.e., re-allocated Target AMF) by Nausf\_Key service operation accordingly. The new AUSF service operation related required and optional inputs and outputs with be described during the normative phase.

Using AUSF as a common NF in the home network:

The AUSF can assist to ensure NAS security context availability for the reallocated AMF. The primary authentication is run similar to TS 33.501 and the AUSF stores the Kseaf before sending the Nausf\_UEAuthentication\_Authenticate response message to the AMF/SEAF following a successful primary authentication (i.e., as in TS 33.501 Clause 6.1.3.2.0 where the AUSF at step 4 generates Kseaf, at step 5 removes Kseaf from 5G AV to send 5G SE AV and finally at step 12 if authentication is successful sends Kseaf to SEAF). The message flow for enabling NAS Security for AMF re-allocation with NAS re-route via RAN using AUSF is shown in Figure 6.4.2-1..



Figure 6.4.2-1: Enabling NAS Security for AMF re-allocation with NAS re-route via RAN using AUSF

**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 can follow similar to TS 23.502 [2] Clause 4.2.2.2.2 and Clause 4.2.2.2.3. 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.

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). To facilitate NAS security context provisioning to the Target AMF for the corresponding UE's ongoing registration procedure, the solution considers using AUSF that can connect with both AMFs to assist indirect AMF re-allocation procedure. If the Initial AMF determines to reroute via RAN, then to facilitate security context provisioning to the target AMF, . the initial AMF sends an AMFRealloc\_Security Context Request message (over a new service-operation message) to the AUSF which includes Target AMF information, AMF\_Reroute\_Security Required indication, SUPI and SUCI.

Editor’s Note: As target AMF information is sent to AUSF in step 4, it is FFS how to address revealing VPLMN network configuration to HPLMN (AUSF) while roaming.

Step 5. On receiving AMFRealloc\_SecurityContext Request message, the AUSF locally stores the SUCI along with SUPI. Based on the SUPI identifies the locally stored security context (i.e., Kseaf). Further the AUSF generates the reroute security context (NAS\_Sec\_ID). NAS\_Sec\_ID is the hash code of security anchor key, SUPI and Target AMF information, which enables AUSF to authenticate the Target AMF for fetching any specific security context at a later point of time.

NOTE 1: The rerouted RR and related information via RAN need not be protected unless any of the related information contains sensitive data (ex. SUPI or Security key etc.,). As this solution does not send any sensitive data along the rerouted information, the solution does not introduce any additional protection to the rerouted RR.

Step 6. The AUSF sends 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 and routing information (i.e., can contain for example address/FQDN/AUSF identification information) to the target AMF via RAN. The additional information includes 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 based on NAS\_Sec\_ID determines to fetch the corresponding security context from the AUSF to handle the received rerouted NAS message. The routing information in the SUCI and/or routing information can be used to select the right AUSF.

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

Step 10. The AUSF on receiving the NAS\_Sec\_ID, SUCI and AMF information, fetches the SUCI-SUPI pair and related information and further verifies the NAS\_Sec\_ID to authenticate the Target AMF to provide the security information. If the NAS\_Sec\_ID validation is successful, the AUSF generates the new NAS security context (Kamf) to be provided for the Target AMF.

NOTE 2: If required, alternatively the AUSF can provision security context (stored or new Kseaf) to the reallocated T-AMF/SEAF, where the related service operation can be defined as Key Request/Response message accordingly.

Step 11. The AUSF 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). For the alternative option, the SEAF derives the Kamf from the received Kseaf , assigns a slice specific ABBA based on received N-NSCI and provides ABBA and Kamf to AMF. The AUSF deletes the NAS\_Sec\_ID and SUCI after step 11..

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 such as 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 to the UE which contains the New NAS Security Context Indicator (N-NSCI), and the special ABBA parameter value (example. 0x0001 to indicate the slice specific feature supported in 5GS to meet slice isolation requirements)..

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 (as indicated with a special ABBA) to derive a Kamf similar to the one available in the Target AMF. The UE uses the received 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, 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 rest of the procedure executes similar to the existing 5G System.

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



**Figure 6.4.2-2: Enabling NAS Security during Registration Mobility Update Scenario for indirect AMF reroute**

This section describes the simple adaptations required for steps shown in Figure 6.4.2-2 to address indirect AMF-reallocation based security aspects handling during registration mobility update procedure.

Step 1. If the Registration Request contains 5G-GUTI, the initial AMF performs the following accordingly for various scenarios mentioned in Clause 4.3 'Architecture and security assumptions', of this TR,

Case 1-2.a.i) Initial AMF based on TS 33.501 Clause 6.9.3, fetches SUPI and security context from the old AMF by providing the 5G-GUTI and the registration request. Further the initial AMF decides whether to reroute the Registration Request according to TS 23.502 Clause 4.2.2.2.3 step 2 (TS 23.502 Clause 4.2.2.2.3 step 2-6b as applicable). If the initial AMF determines to perform RAN reroute due to indirect AMF reallocation (based on TS 23.502 Clause 4.2.2.2.3 step 7B), then the initial AMF decides to ignore the security context fetched from the old AMF after step 6 (initial AMF sends to old AMF Namf\_Communication\_RegistrationStatusUpdate (failure cause). Perform steps 4 to 15 as in Figure 6.4.2-2, with the following minimal changes related to 5G-GUTI storage and handling at theAUSF.

- In step 4, the initial AMF sends 5G-GUTI and SUPI (instead of SUCI)to the AUSF in AMFRealloc\_SecurityContext Request message.

- In step 5, on receiving AMFRealloc\_SecurityContext Request message, the AUSF based on the SUPI identifies the locally stored security context and stores the 5G-GUTI along with the SUPI.

- In step 6. The AUSF sends NAS\_Sec\_ID to the initial AMF in the AMFRealloc\_Security Context Response message.

- In step 8. the Target AMF based on the received NAS\_Sec\_ID, it determines to fetch the corresponding security context from the AUSF to handle the received rerouted NAS message. The routing information can be used to select the right AUSF instance which holds the UE security context.

- In step 9, the target AMF sends 5G-GUTI in the NASKey\_Request to the AUSF.

- In step 10, the AUSF based on the received 5G-GUTI, fetches the corresponding SUPI along with reroute security information to verify the NAS\_Sec\_ID.

Case 2-2.a.ii) As the initial AMF lack N14 with old AMF, the UE cannot be identified by means of a temporary identity (5G-GUTI) and so the AMF performs Subscription identification procedure with UE and continues with primary authentication. After a successful primary authentication, the initial AMF performs steps 4 to 15 same as in Figure 6.4.2-1.

Case 3-2.b.i) The initial AMF having N14 with old AMF will act similar to Case 1-2.a.i. As the scenario is related to indirect AMF reroute, the target AMF based on local policy and received NAS\_Sec\_ID determines to fetch and use security contextrelated to NAS\_Sec\_ID. If required, the target AMF can fetch UE context from the old AMF but may not use security context from old AMF. As the initial AMF already fetches and uses the UE context from old AMF, there is a possibility that old AMF can delete the security context (based on 33.501 Clause 6.9.3), and so the target AMF may not fetch any security context from the old AMF. Further the case 2.b.i may not be feasible according to the vertical slice isolation requirement, which may need to be aligned with the Clause 4.3 accordingly.

Case 4-2.b.ii) As the initial AMF lack N14 with old AMF, the UE cannot be identified by means of a temporary identity (5G-GUTI) and so the AMF performs Subscription identification procedure with UE and continues with primary authentication. After a successful primary authentication, the initial AMF performs steps 4 to 15 same as in Figure 6.4.2-1. On receiving the reroute NAS message with NAS\_Sec\_ID, the target AMF based on local policy determines to use the security context related to the received NAS\_Sec\_ID. As an alternative, the target AMF based on local policy determine either to use the security context related to NAS\_Sec\_ID fetched from AUSF or related to 5G-GUTI fetched from old AMF (where UE context will be fetched).

### 6.4.3 Evaluation

The solution uses AUSF to assist security handling for indirect AMF reallocation scenario to ensure the system availability.

1. The solution does not expose any sensitive information (UE identification information (i.e., SUPI) or security key) to the RAN.

2. The solution involves only one primary authentication run to ensure network availability for the UE during the AMF reroute via RAN scenario.

3. The solution is formulated to work using the existing SA2 defined procedures. Further the solution requires following new features to be supported in the UE and NFs (i.e., RAN and AMF in serving and AUSF in home network) as listed below.

UE Impacts: Process N-NSCI and slice specific feature indicated (i.e., specific ABBA) and derive new Kamf based on them.

RAN Impacts: Forward NAS\_Sec\_ID and Routing information along with Reroute NAS message.

AMF Impacts: Use new AUSF service operations to facilitate security context availability for Target AMF. Initial AMF need to send NAS\_Sec\_ID and Routing Information to RAN Node. Target AMF need to obtain security context from AUSF and send N-NSCI and specific ABBA to UE. For case 2.b.i, target AMF does not use UE security context from old AMF, but can use fetched UE context. For Case 2.b.ii, target AMF based on local policy may use either security context from AUSF or old AMF (where UE context will be available) as described in solution.

AUSF Impacts:

- Need to send slice specific ABBA and N-NSCI to AMF/SEAF. New AUSF service required.

NOTE 1: Slice specific ABBA (for example 0x0001) dedicated for Slice specific security feature in 5GS and it does not expose any information (i.e., versions of any NF) similar to the normal ABBA parameter in the current system (i.e, ABBA parameter value 0x0000 for Initial set of security features defined for 5GS.). As the solution allows one main option (i.e., sending ABBA from AUSF) and one alternative option (i.e., sending from SEAF as in existing system) to the AMF, any one of the options can be used for the normative work. The solution working does not essentially require slice specific ABBA but recommends slice specific ABBA to be used instead for using current ABBA parameter value (0x0000) as it will be more relevant because this feature is related to slicing support.

- Store the SUCI (temporarily) along with SUPI in the AUSF.

NOTE 2: The storage of SUCI and SUPI is not a new feature for the AUSF according to 33.501 Clause 6.1.3.2.0, where it states 'The AUSF shall store the XRES\* temporarily together with the received SUCI or SUPI.'.

- For the registration mobility update, temporary store 5G-GUTI along with SUPI.

NOTE 3: The essential functioning of solution can also work with out storage of 5G-GUTI and SUCI to request key from AUSF, where NAS\_Sec\_ID will act as single point of reference to fetch UE security. The usage of temporary ID complements security context retrieval per UE registration Request associated to a SUCI/5G-GUTI.

Impacts to Key hierarchy:

- No impact (i.e., as solution requires to derives new Kamf from Kseaf).

- Kamf derivation binds to inputs N-NSCI and specific ABBA.

## 6.5 Solution #5: AMF re-allocation by re-directing UE to new AMF

### 6.5.1 Solution Overview

The solution proposes that the Initial-AMF, upon determining that AMF re-allocation is needed and it cannot communicate with the new Target-AMF directly, sends Registration Accept message to the UE, containing a re-route assistance information. The re-route assistance information includes following information:

- A 5G-GUTI that is encoded for Target-AMF (set). It comprises of:

- AMF-Set ID in GUAMI set to that of Target-AMF, as returned from NSSF/NRF

- AMF Pointer set to 0xFFFFFF, or a reserved value

- 5G-TMSI set to random number

- An indication that UE needs to re-register to the network using 5G-GUTI provided in re-route assistance information.

A UE, receiving this information in Registration Accept Message re-initiates registration procedure by sending Registration Request with 5G-GUTI.

RAN, upon receiving the new routing information (derived from 5G-GUTI) along with new Registration Request, directly forwards the request to an AMF in target AMF set.

The new (target) AMF, upon receiving registration request containing a 5G-GUTI whose AMF Pointer is set to a reserved value (or 0xFFFFFF), understands that this is a re-routed registration request and proceeds with Primary Authentication procedure. Thus, it can now proceed with setting up fresh security context and registration procedure can succeed.

### 6.5.2 Solution Details

Figure 6.5.2-1 shows the detailed procedure.



Figure 6.5.2-1: Redirecting UE to Target-AMF

**Step #1:** UE initiates Registration procedure to connect to the network by sending registration request. RAN forwards the request to Initial-AMF. Initial-AMF may perform Primary authentication procedure.

**Step #2:** Initial-AMF may perofrm NAS SMC procedure with the UE. From this point onwards, UE only accepts ciphered/protected messages from the network. As part of “Security Mode Complete” message, UE also sends complete Registration Request to the UE, which includes Requested S-NSSAIs.

**Step #3:** Initial-AMF then initiates Nudm\_SDM\_Get procedure with UDM to download UE's subscription data. The subscription data includes information about UE's Subscribed S-NSSAIs.

**Step #4:** Based on UE's Requested S-NSSAIs, Subscribed S-NSSAIs and other (e.g. locally configured) information, Initial-AMF determines if it cannot serve all the S-NSSAI(s) from the Requested NSSAI permitted by the subscription information. Following sequence of events follows:

- Initial-AMF invokes the Nnssf\_NSSelection\_Get service operation towards NSSF to retrieve Allowed NSSAI. The request to NSSF includes UE's Requested S-NSSAIs, Subscribed S-NSSAIs, current tracking area (TAI) etc.

- NSSF responds to Initial-AMF with an AMF-Set-ID, or a list of AMF nf-Instance-IDs (e.g. of Target-AMF) which are better suited to serve the UE, along with allowed NSSAI.

**Step #5:** If Initial-AMF, based on local configuration, determines that it cannot forward the Registration Request to Target-AMF directly and/or may need to go via RAN, it sends a Registration Accept message to the UE. The message includes re-route assistance information containing:

- A 5G-GUTI that is encoded for Target-AMF (set). It comprises of:

- AMF-Set ID in GUAMI set to that of Target-AMF, as returned from NSSF/NRF

- AMF Pointer set to 0xFFFFFF, or a reserved value, or that of Target-AMF (if specific AMF IDs are returned by NRF/NSSF)

Editor's Note: How to solve GUTI collision is FFS.

- 5G-TMSI set to random number

- An indication that UE needs to re-register to the network using 5G-GUTI provided in re-route assistance information. This may be implicit due to presence of re-route assistance information. Exact details can be decided by Stage-3.

Following this, UE sends Registration Complete, and network releases ngAP/RRC connection.

UE also needs to indicate its support of receiving re-route assistance information in Step #1. Exact details will be decided by Stage-3.

For legacy UEs which do not support such capability, registration accept is sent with following information. Re-route assistance information is not sent in this case.

- 5G-GUTI set as indicated above

- Really short periodic registration timer (e.g. 4 seconds)

**Step #6:** UE re-initiates Registration procedure by sending Registration Request with 5G-GUTI as received above. via a new RRC Connection towards RAN. RAN forwards the request to Target-AMF.

**Step #7:** When Target-AMF receives the new Registration Request with new 5G-GUTI, it determines that it neither has UE's context locally, nor can reach the old AMF (e.g. due to presence of reserved value of AMF-Pointer in 5G-GUTI), and deduces that this is a re-routed Registration request. It accordingly proceeds with identity request/response followed by Primary authentication procedure. Since no Inter-AMF routing via RAN is involved now, the registration procedure is able to proceed.

For legacy UEs which may have initiated Registration Request of type "periodic", target AMF rejects registration request which forces it to send Registration Request of type "initial".

#### 6.5.2.1 Handling Different cases of communicating AMFs (Figure 4.3-1)

Case 1: This is handled with procedure defined in Clause 6.5.1

Case 2.a.i: This case cannot be handled with this solution, as source AMF does not transfer any data to target AMF.

Case 2.a.ii: This case cannot be handled by any procedure.

Case 2.b.i: It is proposed to handle this case as follows.

- UE does not discard 5G-GUTI pointing to old-AMF in Step #5, and sends it as an additional GUTI in the Registration Request in Step #6. Target-AMF, based on the presence of reserved value of AMF-Pointer in 5G-GUTI, determines that this is a re-routed Registration requests, and additional GUTI to be used to retrieve the UE's Context.

NOTE: The existing Registration Request procedure allows the inclusion of two 5G-GUTIs, if the UE has a valid EPS GUTI and a native 5G-GUTI and when the UE performs a mobility registration update from EPS to 5GS explicitly indicating the mobility from EPS in a plaintext IE. The inclusion of two native 5G-GUTIs in the Registration Request without the UE moving from EPS to 5GS is a new behaviour since the UE is not required to set the indication that is moving from EPS. However, this is not expected to cause any issues with the AMF handling the Registration Request.

- Target-AMF requests old-AMF to transfer UE's Context **after** UE has been successfully authenticated by Target-AMF. This is done by setting reason attribute to “MOBI\_REG\_UE\_VALIDATED” as specified in clause 5.2.2.2.1.2 of 3GPP TS 29.518

Legacy UEs (that do not support receiving/sending new IEs) cannot handle this case.

Case 2.b.ii: Same as above.

### 6.5.3 Evaluation

Pros:

- Since the solution does not involve routing security context via RAN, or introducing a new NF connecting isolated slices, there is no compromise with security.

Cons:

- Cannot handle Case 2.a.i.

- Legacy UEs cannot handle Case 2.b.i, 2.b.ii.

NOTE: This solution has impacts to SA2 procedures (e.g. as defined in 3GPP TS 23.502, Clause 4.2.2.2.3), and SA2 may need to be requested to review and update their specifications.

The initial AMF is mandated to assign a GUTI to the UE on behalf of the target AMF.

The target AMF is mandated to run identity request and perform primary authentication.

The target AMF is unable to retrieve UE context from the old AMF. Context loss is inevitable.

This solution removes the option of NAS reroute via RAN. How to solve the registration failure issue when RR is rerouted via RAN is still not solved.

This solution has impact on the UE.

The UE and the network are required to run two registration procedures.

## 6.6 Solution #6: Solution to provide Security context to AMF capable of serving the UE to ensure system availability

### 6.6.1 Introduction

The solution addresses Key issue #1 on Security of AMF re-allocation procedure. The solution enables provisioning of UE security context to the AMF capable of serving the UE to ensure system availability.

### 6.6.2 Solution details

The solution is based on the principle of verifying the initial AMF's capability and the UE's subscription information (i.e., slice subscription data), before the UE's security context can be provisioned to the initial AMF during the primary authentication to prevent system availability issues described in Key Issue#1. The Figure 6.6.2-1 describes the AMF capability and slice isolation requirement-based UE Security handling during primary authentication as follows. The essential adaptations required over initiation of primary authentication and authentication procedure is described here in Figure 6.6.2-1 and the rest follows similar to Clause 6.1.2 and clause 6.1.3 of TS 33.501.



Figure 6.6.2-1: AMF Serving Capability based Security handling during primary authentication

Step 1. The UE sends the Registration Request with SUCI or 5G-GUTI to the initial AMF.

Step 2a-b. The initial AMF forwards the received initial UE message containing Registration Request to the SEAF with SUCI by including the AMF Slice Capability set as unknown. The AMF can set the AMF serving capability as unknown based on SUCI and if there is no slice related information (example. slice selection information or reroute due to slicing information) available for the UE. The SEAF further sends a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF, which can contain SUCI, SNN and AMF Slice Serving Capability.

Step 3. The AUSF stores the received SNN and SUCI temporarily in its local memory. The AUSF sends to the UDM a Nudm\_UEAuthentication\_Get Request containing, SUCI, and SNN.

Step 4. The UDM/UDR performs SUCI deconcealment and authentication method selection as in TS 33.501 Clause 6.1.2. Further the UDM, determines, if there is any slice isolation required based on the available subscription information (ex., slice selection subscription data). If a slice isolation requirement information is available, then the UDM determines to provide the related information to the AUSF.

Step 5. The UDM sends a Nudm\_UEAuthentication\_Get Response to the AUSF, which contains an AV (i.e., EAP-AKA' AV/5G HE AV as in 33.501 based on authentication method), SUPI and Slice Isolation Required indication.

Step 6. The AUSF performs method specific message exchange with the UE to perform primary authentication as in 33.501 Clause 6.1.3 (steps 3-8 for EAP-AKA' or 3-11 for 5G AKA). The solution proposes no changes to the challenge request/response message exchanges involved in the primary authentication.

Step 7a. The AUSF if finds that the RES\* verification (if 5G AKA) or Authentication challenge verification (EAP-AKA') is successful, then the 5G network considers the primary authentication as successful.

Step 7b. Post successful authentication verification at the AUSF, if an AMF serving capability unknown was received from AMF/SEAF in step 2, then the AUSF determines to hold the UE security context until an acknowledgement is received from the initial AMF/SEAF that it is capable to serve the UE. As an alternative option 1, the AUSF can provide security context as in the existing system in addition to sending AMF serving capability check Required Indication and Slice Isolation Required Indication.

Step 8. The AUSF sends to AMF/SEAF, a Nausf\_UEAuthentication\_Authenticate Request message which includes authentication result as success, SUPI and an AMF serving capability Check Required indication and Slice Isolation Required Indication (if received from UDM). As an alternative option 1, the Anchor Key is also provided.

Step 9a-b. The AMF/SEAF on receiving an AMF serving capability Check Required indication and Slice Isolation Required Indication (if received), the AMF determines to check its serving capability and it performs steps 3a-6b (as applicable) of clause 4.2.2.2.3 Registration with AMF re-allocation as specified in TS 23.502. The initial AMF based on local policy and subscription information if decides to reroute via RAN (based on TS 23.502 clause 4.2.2.2.3 step 7B), then performs step 10a-15. Also, the AMF determines not to use the received security context (if received as in alternative option 1). Else if the AMF finds that it is capable to serve the UE (i.e., a reroute via RAN is not needed), and if no security context is received in addition to AMF serving capability check required indication, then the AMF/SEAF can perform step 10a'-10b' to fetch UE security context and then to continue with NAS SMC as in existing system. Else if, the AMF finds that it is capable to serve the UE (i.e., a reroute via RAN is not needed), and if a security context is received as in alternative option 1, then the AMF continue with NAS SMC as in existing system.

Step 10a. The AMF/SEAF, if determines to perform Reroute via RAN, then it sends SUPI, AMF Serving Capability Result set as '0', AMF reroute security required indication and target AMF information in an AUSF service operation message to the AUSF.

Step 10b. The AUSF on receiving an AMF Serving Capability Result set as '0' (as in step 10a) with AMF reroute security required indication, determines that it need to provide the security to new Target AMF. Further as a reroute security context is requested, the AUSF derives an AMF authentication token (AMF\_AUTN) using hash of AUSF key, SUPI and RAND. AUSF locally stores the AMF\_AUTN along with the SUPI, SUCI, Kausf, and Kseaf (if available). The AUSF further sends AMF\_AUTN in AUSF service operation message to the AMF/SEAF.

If No Reroute via RAN determined at AMF (then only steps 10a' and 10b' are applicable):

Step 10a'.The AMF if determines that it is capable to serve the UE (i.e., no reroute via RAN), sends SUPI and AMF Serving Capability Result set as '1' to the AUSF.

Step 10b'. The AUSF on receiving SUPI and AMF Serving Capability Result set as '1' determines to provide the UE Security context to AMF/SEAF and then AUSF can send SUPI, Authentication Result and Anchor Key to the AMF/SEAF as in the existing system.

Step 11a. The initial AMF based on local policy and subscription information if decides to reroute via RAN (based on TS 23.502 clause 4.2.2.2.3 step 7B) at step 9b, it further sends the Reroute NAS message to the NG-RAN, which contains the initial UE message, Routing Information (to select the AUSF instance holding the UE context), and AMF\_AUTN.

Step 11b. The NG-RAN forwards the received Reroute NAS message to the Target AMF with initial UE message, reroute due to slicing, AMF\_AUTN and Routing Information.

Step 12. The Target AMF on receiving the Reroute NAS message with AMF\_AUTN will attempt to contact the right AUSF (either directly or via co-located SEAF) based on the routing Information. The Target AMF sends to appropriate AUSF, the Nausf\_UEAuthentication\_Authenticate Request containing the SUCI, SNN, and the received AMF\_AUTN (to authenticate itself with AUSF to fetch the UE security context).

Step 13. The AUSF verifies the received AMF\_AUTN based on the UE authentication information locally stored. If the Target AMF provided AMF\_AUTN matches with the locally stored AMF\_AUTN for a SUCI, then the AUSF considers the AMF\_AUTN verification (i.e., Reallocated AMF authentication) as successful and determines to provide the anchor key.

Step 14. The AUSF sends to SEAF of the Target AMF, the Nausf\_UEAuthentication\_Authenticate Response containing authentication result, SUPI and Kseaf (the anchor key). Further the SEAF sends the ABBA parameters, authentication result as success, and Kamf key to the Target AMF as in the existing system.

Step 15. The Target AMF on receiving the Kamf and authentication result triggers the NAS Security mode command (NAS SMC) procedure with UE to set up the UE NAS security context as in TS 33.501.

**Adaptations for Registration Mobility Update:**

This section describes the simple adaptations required to address security handling in AMF-reallocation during registration mobility update procedure as shown in Figure 6.6.2-2.



**Figure 6.6.2-2: Security context handling during registration mobility update**

Step 1. If the Registration Request contains 5G-GUTI (pointing to an old AMF), the initial AMF performs the following accordingly for various scenarios mentioned in Clause 4.3 'Architecture and security assumptions', of this TR,

Case 1-2.a.i) N14 interface exists only between Initial AMF and Old AMF:

Step 2a-b.The Initial AMF based on TS 33.501 Clause 6.9.3, fetches SUPI and security context from the old AMF by providing the 5G-GUTI and the registration request. Further SUPI and subscription information (fetched from UDM as shown in 2b.3) can be used to decide whether to reroute the Registration Request according to TS 23.502 Clause 4.2.2.2.3 step 2. If a reroute is required, the initial AMF, if fetched the UE context (as in TS 23.502 Clause 5.2.2.2.2) from the old AMF, it can use the slice information to perform (2b.4) Nnssf\_NSSelection service operation based on 23.502 4.2.2.2.3 step 4a-b. Also, for the case, where the current 5G security context is fetched, the AMF may decipher the NAS container with the same security context, and get the initial NAS message and so if there is any Requested NSSAI provided by UE, it can also be used in Nnssf\_NSSelection service operation (even though it is an optional IE according to TS 23.502 Clause 5.2.16.2.1). If an indirect AMF allocation and reroute via RAN is required, the initial AMF does not send any NAS message to the UE (i.e., it does not use current/new 5G security context fetched from old AMF), in turn can perform reroute via RAN.

NOTE 1: According to TS 33.501 Clause 6.9.3 for the case where source/old AMF sends new 5G security context to Initial AMF, it states, 'The source AMF subsequently deletes the 5G security context which it holds.'

Step 2c.1 If another AMF is selected, the initial AMF sends a reject indication to the old AMF and the old AMF continues as if the Namf\_Communication\_UEContextTransfer had never been received.

Step 2c.2. Target AMF discovery can be based on 23.502 clause 4.2.2.2.3 steps 6a-b.

Step 3-4. The initial AMF performs reroute via RAN as in 23.502 Clause 4.2.2.2.3 step 7B.

Step 5a-b. The Target AMF on receiving the initial NAS message with 5G-GUTI finds that it is not able to identify the related old AMF and considers that it cannot identify the UE with 5G-GUTI and so initiates identity request procedure with UE and get SUCI.

Step 6. The target AMF initiates primary authentication by sending Registration Request with SUCI (without AMF slice serving capability IE, because the target AMF is aware that this is reroute due to slicing received in Reroute NAS message as in TS 23.502 Clause 4.2.2.2.3 step 7B).

The target AMF will not include any AMF slice serving capability IE as unknown, so, the AUSF soon after successful response verification will provide Anchor key to the AMF/SEAF as in existing system. If the UDM provides a Slice Isolation Required Indication during step 5 as in Figure 6.6.2-1, the AUSF also sends the received Slice Isolation Required Indication to the AMF/SEAF along with the authentication result, SUPI and anchor key. Alternatively, if the AUSF does not receive any AMF slice serving capability unknown indication from the AMF, the AUSF can skip sending Slice Isolation Required indication to the AMF (if received from the UDM). The Target AMF checks the SUPI and subscription information and then accordingly performs NAS SMC with the UE.

Case 2-2.a.ii) No N14 exists between Initial AMF and old AMF and also no N14 exists between target AMF and old AMF: As the initial AMF lack N14 with old AMF, the UE cannot be identified by means of a temporary identity (5G-GUTI) and so the initial AMF performs Subscription identification procedure (as shown in step 2.b-1) with UE and continues with primary authentication (as shown in step 2b.2) with the adaptations described in Figure 6.6.2-1 steps 2a-13.

Case 3-2.b.i) N14 exists between Initial AMF and old AMF and also between target AMF and old AMF: The initial AMF having N14 with old AMF will act similar to Case 2-2.a.i steps 1-4.

Step 5-6. The Target AMF on receiving the initial NAS message with 5G-GUTI finds it can contact the corresponding old AMF. Based on local policy and reroute due to slicing indication received in reroute NAS message, the target AMF may fetch security context from old AMF (or) determines not to fetch security context from old AMF and perform Identity request/response procedure and primary authentication accordingly (as in case 2.a.i).

If the target AMF fetches security context from old AMF, either based on local policy the target AMF may use current/new security context fetched from old AMF or the target may determine to perform primary authentication with SUPI (as in case 2.a.i, but SUPI is used instead of SUCI).

NOTE 2: Further the case 2.b.i may not be feasible according to the vertical slice isolation requirement and it may need to be aligned with the Clause 4.3.

Case 4-2.b.ii) N14 exists only between target AMF and old AMF: As the initial AMF lack N14 with old AMF, the UE cannot be identified by means of a temporary identity (5G-GUTI) and so the AMF performs Subscription identification procedure (as shown in 2b.1) with UE and continues with primary authentication (as shown in 2b.2) based on the adaptations described in Figure 6.6.2-1 steps 2a-13. The target AMF on receiving the reroute NAS message (i.e., Registration Request with 5G-GUTI), based on local policy, received authentication information (AMF\_AUTN) and reroute due to slicing indication, determine to fetch security context related to an authentication information received in the reroute NAS message from the AUSF.

### 6.6.3 Evaluation

The solution depends on AUSF to assist security handling for indirect AMF reallocation scenario to ensure the system availability. The solution has the following advantages:

1. The solution ensures security context provisioning only to AMF which can serve a UE and hence limiting the occurrence of system availability issues described in key issue#1.

2. The solution governs strict isolation requirements for the AMF without reusing the existing AMF Key belonging to a source AMF and/or old AMF for the Target AMF which has an isolation requirement.

3. The solution is formulated to work using the SA2 defined procedure specified in TS 23.502 Clause 4.2.2.2.3. The solution has impact on the primary authentication procedure (i.e., initiation of primary authentication and after the response verification at the AUSF). The solution does not impact challenge response message exchanges.

NOTE: As soon as SUPI is available for the initial AMF (Either after primary authentication or after fetching from old AMF), an amf reallocation and reroute via RAN requirement is determined and performed following 23.502 clause 4.2.2.2.3 steps 3a-3b (to fetch slice selection subscription data), step 4a-4b (network slice selection based on Nnssf\_NSSelection\_Get service operation, where essentially all conditions are applied as specified in Clause 5.2.16.2.1 Nnssf\_NSSelection\_Get service operation. The required inputs specified as 'Inputs, Conditional Required' will be included and 'Inputs, Optional'(i.e., Requested NSSAI) will be included only if it is available for the initial AMF (as used and described for case 3-2.b.i solution), where required step 5 (Namf\_communication\_RegistrationStatus update), steps 6a-b (NF Discovery with NRF) and finally step 7B(for reroute via RAN). If the initial AMF determines that an AMF reallocation and reroute is required, then the initial AMF skips NAS SMC to allow the reallocated AMF to perform primary authentication or NAS SMC with the UE. The Network slice selection alignment can be evaluated by SA2.

Impacts to NFs in serving network (i.e., RAN and AMF) and home network (i.e., AUSF and UDM) are listed below.

RAN Impact: Forward AMF\_AUTN and routing information to Target AMF along with reroute NAS message.

AMF Impact: Send AMF slice serving capability as Unknown while invoking authentication service (based on SUCI and if no slicing information is available) to AUSF. If a reroute via RAN is determined, AMF facilitates security context availability for the Target AMF during primary authentication. Target AMF need to process AMF\_AUTN and include AMF\_AUTN when invoking authentication service provided by AUSF.

AUSF Impact: If 'AMF slice serving capability' set to Unknown is received, the AUSF determines to hold the security context until an AMF serving capability with Result with '1' is received from AMF/SEAF. If an amf reroute is indicated along with AMF serving capability with Result '0', then AUSF generates and provides AMF\_AUTN to initial AMF to enable the new target AMF to fetch the corresponding security context. AUSF need to verify AMF\_AUTN.

Impact to Home network in roaming: The UDM/UDR require to store slice isolation requirements (if any) as part of subscription information and provide to AUSF.

UE Impact: No Impact.

## 6.7 Solution #7: Solution to enable Reallocated AMF to serve the UE

### 6.7.1 Introduction

The solution addresses Key issue #1 on Security of AMF re-allocation procedure.

The solution is based on the principle of allowing the initial AMF to decide when a SUPI is available, if a 'AMF reallocation with reroute via RAN' is required or not based on the critical factors (i.e., SUPI, subscription information, slice selection and AMF local policy etc.,), defined in TS 23.502 Clause 4.2.2.2.3.

### 6.7.2 Solution details

The solution is based on the principle of enabling the initial AMF to verify the UE's slice subscription data soon after response verification during the primary authentication to determine if an AMF is capable to serve a UE or not, before the UE's security context can be provisioned to the initial AMF to prevent system availability issues described in Key Issue#1 of this document. The Figure 6.7.2-1 describes the UE slice subscription data-based AMF serving capability verification and UE Security handling/provisioning to AMF/SEAF during primary authentication as follows. The essential adaptations required over initiation of primary authentication and authentication procedure is described here in Figure 6.7.2-1 and the rest follows similar to Clause 6.1.2 and clause 6.1.3 of TS 33.501.



Figure 6.7.2-1: AMF Serving Capability based Security Context handling during primary authentication

The solution uses the existing service operations for the adaptations required.

Step 1. The UE sends the Registration Request with SUCI or 5G-GUTI to the initial AMF.

Step 2a-b. The initial AMF forwards the received initial UE NAS message containing Registration Request to the SEAF by including the Slice Selection Information Not Available indication (if the AMF received a Registration Request with SUCI/ 5G-GUTI (i.e., during initial registration with SUCI /when the UE and old AMF could not be identified with 5G-GUTI). The SEAF further sends a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF. The Slice Selection Information Not Available can indicate that the initial AMF has no available information which can enable the network to select the appropriate slice.

Step 3. The AUSF on receiving the Slice Selection Information Not Available Indication determines that the network (ie., AMF) needs further information to verify the serving capability for the corresponding UE. The AUSF sends to the UDM a Nudm\_UEAuthentication\_Get Request containing, SUCI, and SNN.

Step 4. The UDM/UDR performs SUCI de-concealment and authentication method selection as in TS 33.501 Clause 6.1.2.

Step 5. The UDM sends a Nudm\_UEAuthentication\_Get Response to the AUSF, which contains an AV (i.e., EAP-AKA' AV/5G HE AV as in 33.501 based on authentication method), and SUPI.

Step 6. The AUSF performs method specific message exchange with the UE to perform primary authentication (i.e., as in TS 33.501 Clause 6.1.3 steps 3-8 for EAP-AKA' or 3-11 for 5G AKA). The solution proposes no changes to the challenge request/response message exchanges involved in the primary authentication.

Step 7. The AUSF if finds that the RES\* verification (if 5G AKA) or Authentication challenge verification (EAP-AKA') is successful, then the network considers the primary authentication as successful. If a Slice Selection Information Not Available was received in step 2a from AMF/SEAF, then the AUSF determines to hold the UE security context temporarily until the AMF/SEAF informs the AUSF about its serving capability.

Step 8. The AUSF can send to the AMF/SEAF, the authentication result as success, SUPI, and AMF serving Capability Check Required indication.

Step 9a-9b. The initial AMF on receiving the SUPI along with AMF serving Capability Check Required indication, determines to check if a reroute is required or not based on TS 23.502 as shown in step 9a-b.

Step 9c. If the AMF decides to perform an indirect AMF reroute, then it determines to facilitate the UE security context provisioning to the newly selected target AMF.

If the AMF determines to perform indirect AMF reroute via RAN, then sets the AMF service capability result as '0'.

Else, if the AMF determines to perform direct AMF reroute/ if it is capable to serve the UE based on the UE subscription information/slice subscription data, then sets the AMF service capability result as '1'.

Step 10. The AMF/SEAF sends to AUSF, the SUPI, AMF Reroute Security Required Indication, AMF service capability result, Target AMF Information, and optionally SUCI.

Alternatively, if No Reroute via RAN is determined, then AMF/SEAF sends to AUSF the SUPI, AMF service capability result set to '1'.

Step 11. The AUSF on receiving a AMF service capability result set as '0', and Reroute Security Required Indication, it determines to store the UE security context to facilitate the security provisioning to the Target AMF at a later point of time when required (i.e., after reallocation). The AUSF derives an authentication information AMF\_AUTN from the UE context available in the AUSF (for the Target AMF using the hash of AUSF, SUPI, RAND, SNN and the target AMF information).

Alternatively, for no Reroute via RAN case, the AUSF on receiving from AMF/SEAF, AMF service capability result with '1', provides the Anchor key, SUPI and authentication result to the initial AMF and the initial AMF can setup NAS Security similar to the existing system.

Step 12. The AUSF sends to the AMF/SEAF, the SUPI, AMF\_AUTN, AUSF locally stores the AMF\_AUTN along with the SUPI with SUCI, Kausf, Kseaf and corresponding SNN. The SEAF forwards the received SUPI, authentication result as success, SUPI, AMF\_AUTN, to the initial AMF.

Step 13a. The AMF sends a reroute NAS message to the NG-RAN with initial UE message, reroute due slicing, Routing Information (to indicate the AUSF holding the context) and AMF\_AUTN.

Step 13b. The NG-RAN forwards the received Reroute NAS message to the Target AMF with initial UE message, reroute due slicing, Routing Information and AMF\_AUTN.

Step 14. The Target AMF on receiving the Reroute NAS message with reroute due slicing, Routing Information and AMF\_AUTN will attempt to contact the right AUSF based on the Routing Information. The Target AMF sends to appropriate AUSF, the Nausf\_UEAuthentication\_Authenticate Request containing the SUCI, SNN, and the received AMF\_AUTN (to authenticate itself with AUSF to fetch the UE security context).

Step 15. The AUSF verifies the received AMF\_AUTN and SNN based on the UE authentication information locally stored. If the Target AMF provided AMF\_AUTN matches with the locally stored AMF\_AUTN for a SUCI and/or SUPI, then the AUSF considers the AMF\_AUTN verification as successful

Step 16. The AUSF sends to SEAF of the Target AMF, the authentication result, SUPI and Kseaf (the anchor key) as in the existing system and the rest follows similar to the existing procedures. Further the SEAF sends the ABBA parameters, authentication result as success, and Kamf key to the Target AMF.

Step 17. The Target AMF on receiving the Kamf and authentication result triggers the NAS Security mode command (NAS SMC) procedure with UE to set up the UE NAS security context as in TS 33.501.

**Adaptations for Registration Mobility Update:**

This section describes the simple adaptations required to address security handling in AMF-reallocation during registration mobility update procedure as shown in Figure 6.7.2-2.



Figure 6.7.2-2: Security context handling during registration mobility update

NOTE 1: According to TS 33.501 Clause 6.9.3 for the case where source/old AMF sends new 5G security context to Initial AMF, it states, 'The source AMF subsequently deletes the 5G security context which it holds.'

Step 1. If the Registration Request contains 5G-GUTI (pointing to an old AMF), the initial AMF performs the following accordingly for various scenarios mentioned in Clause 4.3 'Architecture and security assumptions', of this TR,

Case 1-2.a.i) N14 interface exists only between Initial AMF and Old AMF:

Step 2a-b. The Initial AMF based on TS 33.501 Clause 6.9.3, fetches SUPI and security context from the old AMF by providing the 5G-GUTI and the registration request. Further SUPI and subscription information (fetched from UDM as shown in 2b.3) can be used to decide whether to reroute the Registration Request according to TS 23.502 Clause 4.2.2.2.3 step 2. If a reroute is required, the initial AMF, if fetched the UE context (as in TS 23.502 Clause 5.2.2.2.2) from the old AMF, it can use the slice information to perform (2b.4) Nnssf\_NSSelection service operation based on 23.502 4.2.2.2.3 step 4a-b. Also, for the case, where the current 5G security context is fetched, the AMF may decipher the NAS container with the same security context, and get the initial NAS message and so if there is any Requested NSSAI provided by UE, it can also be used in Nnssf\_NSSelection service operation (even thought it is an optional IE according to TS 23.502 Clause 5.2.16.2.1). If an indirect AMF allocation and reroute via RAN is required, the initial AMF does not send any NAS message to the UE (i.e., it does not use current/new 5G security context fetched from old AMF), inturn can perform reroute via RAN.

Step 2c.1. If another AMF is selected, the initial AMF sends a reject indication to the old AMF and the old AMF continues as if the Namf\_Communication\_UEContextTransfer had never been received.

Step 2c.2. Target AMF discovery can be based on 23.502 clause 4.2.2.2.3 steps 6a-b.Step 3-4. The initial AMF perfoms reroute via RAN as in 23.502 Clause 4.2.2.2.3 step 7B.

Step 5a-b. The Target AMF on receiving the initial NAS message with 5G-GUTI finds that it is not able to identify the related old AMF and considers that it cannot identify the UE with 5G-GUTI and so initiates identity request procedure with UE and get SUCI.

Step 6. The target AMF initiates primary authentication by sending Registration Request with SUCI (without Slice Selection Information Not Available Indication, because the target AMF is aware that this is reroute due to slicing as received in Reroute NAS message as in TS 23.502 Clause 4.2.2.2.3 step 7B).

The target AMF will not include any Slice Selection Information Not Available Indication, so the AUSF soon after successful response verification will provide Anchor key to the AMF/SEAF as in existing system.

Case 2-2.a.ii) No N14 exists between Initial AMF and old AMF and also no N14 exists between target AMF and old AMF: As the initial AMF lack N14 with old AMF, the UE cannot be identified by means of a temporary identity (5G-GUTI) and so the initial AMF performs Subscription identification procedure (as shown in step 2b.1) with UE and continues with primary authentication (as shown in step 2b.2) with the adaptations described in Figure 6.6.2-1 steps 2a-17 as applicable.

Case 3-2.b.i) N14 exists between Initial AMF and old AMF and also between target AMF and old AMF: The initial AMF having N14 with old AMF will act similar to Case 2-2.a.i steps 1-4.

Step 5-6. The Target AMF on receiving the initial NAS message with 5G-GUTI finds it can contact the corresponding old AMF. Based on local policy and reroute due to slicing indication received in reroute NAS message, the target AMF may fetch security context from old AMF (or) determines not to fetch security context from old AMF and perform Identity request/response procedure and primary authentication accordingly (as in case 2.a.i).

If the target AMF fetches security context from old AMF, either based on local policy the target AMF may use current/new security context fetched from old AMF or the target may determine to perform primary authentication with SUPI (as in case 2.a.i, but SUPI is used instead of SUCI).

NOTE 2: Further the case 2.b.i may not be feasible according to the vertical slice isolation requirement and it may need to be aligned with the Clause 4.3.

Case 4-2.b.ii) N14 exists only between target AMF and old AMF: As the initial AMF lack N14 with old AMF, the UE cannot be identified by means of a temporary identity (5G-GUTI) and so the AMF performs Subscription identification procedure (as shown in 2b.1) with UE and continues with primary authentication (as shown in 2b.2) based on the adaptations described in Figure 6.6.2-1 steps 2a-13. The target AMF on receiving the reroute NAS message (i.e., Registration Request with 5G-GUTI), based on local policy, received authentication information (AMF\_AUTN) and reroute due to slicing indication, determine to fetch and use security context related to an authentication information received in the reroute NAS message from the AUSF and if required can fetch UE context from the old AMF.

### 6.7.3 Evaluation

The solution depends on AUSF to assist security handling for indirect AMF reallocation scenario to ensure the system availability. The solution has the following advantages:

1. The solution ensures security context provisioning only to AMF which can serve a UE and hence limiting the occurrence of system availability issues described in key issue#1.

2. The solution is formulated to work using the existing SA2 defined procedures. The solution has impact on the primary authentication procedure (i.e., initiation of primary authentication and after the response verification at the AUSF). The solution does not impact challenge response message exchanges.

NOTE: As soon as SUPI is available for the initial AMF (Either after primary authentication or after fetching from old AMF), an AMF reallocation and reroute via RAN requirement is determined and performed following 23.502 clause 4.2.2.2.3 steps 3a-3b (to fetch slice selection subscription data), step 4a-4b (network slice selection based on Nnssf\_NSSelection\_Get service operation, where essentially all conditions are applied as specified in Clause 5.2.16.2.1 Nnssf\_NSSelection\_Get service operation. The required inputs specified as 'Inputs, Conditional Required' will be included and 'Inputs, Optional'(i.e., Requested NSSAI) will be included only if it is available for the initial AMF (as used and described for case 3-2.b.i solution), where required step 5 (Namf\_communication\_RegistrationStatus update), steps 6a-b (NF Discovery with NRF) and finally step 7B(for reroute via RAN). If the initial AMF determines that an AMF reallocation and reroute is required, then the initial AMF skips NAS SMC to allow the reallocated AMF to perform primary authentication or NAS SMC with the UE. The Network slice selection alignment can be evaluated by SA2.

UE Impact:

- No impact

RAN Impact:

- Forward AMF\_AUTN and Routing Information in reroute NAS message.

AMF Impact:

- Send 'Slice Selection Information Not Available Indication' to AUSF based on SUCI and if no slice selection information is available. Further, provides serving capability information to AUSF if requested. If reroute via RAN is required, facilitates security context availability for the reallocated target AMF. Target AMF need to process AMF\_AUTN and include AMF\_AUTN when invoking authentication service provided by AUSF.

AUSF Impact:

- If 'Slice Selection Information Not Available Indication' is received from AMF/SEAF in authentication request, then request serving capability information from AMF to hold/provide UE security context accordingly.

- If notified that AMF is not capable to serve UE, then facilitates security context provision to Target AMF.

## 6.8 Solution #8: Solution to enable UE connection directly to the slice AMF

### 6.8.1 Introduction

A new solution is proposed here for connecting the UE directly to an isolated target AMF, and avoids UE connecting to any other AMF.

AMF re-allocation is required because the UE gets connected to an AMF which cannot serve the UE, AMF possibly belonging to an incorrect Network Slice. The base station routed the Registration Request from the UE to the incorrect AMF, because the S-NSSAI is not available in the RRC message, it is contained only in the NAS payload. So the base station is not able to select the correct AMF based on the S-NSSAI. If S-NSSAI is available in the RRC message, then base station can select the correct AMF corresponding the N-NSSAI and the Network Slice.

### 6.8.2 Solution details

Solution principles:

1) RRC Connection Request Complete (RRC Msg 5) carrying NAS REG-REQ is encrypted with network public key or certificate and will contain encrypted S-NSSAI in the RRC part of the message.

2) Base station will decrypt the encrypted RRC message and will route the NAS REG-REQ to the correct AMF according to the S-NSSAI.

3) Since the UE gets routed to the correct AMF, the AMF can be fully isolated, and no context transfer or context sharing is required between any other AMF.

The solution consists of two phases.

#### 6.8.2.1 Solution phase 1

Provisioning the network public key or certificate corresponding the network slice AMF.

This is only a one time procedure between the UE and the network.

On the network side it is expected that base stations support mechanisms to decrypt the encrypted RRC Msg5 to learn the S-NSSAI and route accordingly to the correct AMF.



Figure 6.8.2.1-1 Provisioning the UE with network public key or certificate

1. UE does initial attachment with the network and gets authenticated.

2. At the end of successful authentication, UDM triggers the AMF to send the network public key for encrypting RRC message. Once the UE gets provisioned with network public key or certificate, UE gets de-registered from the network.

NOTE: Provisioning of the network public key may be done by offline methods as well. Phase1 is required only if the UE is not already provisioned by the network public key or certificate. The UE stores the provisioned public key of the network in the USIM. It is expected that all base stations in the network support the same public key -private key pair.

Editor's Note: How to address the registration failure issue with NAS reroute via RAN is FFS.

#### 6.8.2.2 Solution phase 2

In subsequent connections to the network, UE uses the provisioned public key to encrypt the RRC message and the S-NSSI is included in the RRC message. The UE also includes an indication in the NAS message that it has the public key in possession from Phase1. The indication helps the network to learn that the UE has been already provisioned and further attempts to provision the public key is avoided.



1. In RRC message 5, UE includes the S-NSSAI in the RRC part of the message along with the NAS payload. The RRC message is encrypted with the provisioned public key.

2. gNB decodes the RRC message 5 with the network private key and learns the S-NSSAI and the Slice the UE wants to connect.

Editor's Note: It is FFS whether the gNB decodes the RRC message 5 or it takes the help of a trusted central node in possession of the network private key.

3. gNB forwards the NAS payload based on the S-NSSAI and the Slice the UE wants to connect to the corresponding AMF. The NAS message also contains an indication that UE is in possession of the public key from phase-1.

Editor's Note: It is FFS how gNB is able to route the NAS message to the correct serving AMF based on S-NSSAI.

4. UE and AMF establishes NAS context specific to the S-NSSAI and the slice.

Editor's Note: The details of public key provisioning to the UEs and corresponding private key provisioning to the gNBs are FFS.

Editor's Note: The security analysis of all the gNBs sharing the same private key is FFS.

Editor's Note: Whether public key cryptography impacts the radio protocols is FFS.

### 6.8.3 Evaluation

The solution avoids the necessity of UE AMF re-allocation altogether and hence security issues related to AMF re-allocation doesn't arise at all.

Solution requires provisioning of public key in the UE and private key in the network (gNB). Once the key provisioning is done, either offline means or online means one time, AMF re-allocation is not required.

Editor's Note: It is FFS whether solution is applicable for the NAS re-routing use case via RAN.

## 6.9 Solution #9: Security of AMF re-allocation when 5G NAS security context is rerouted via RAN

### 6.9.1 Introduction

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

In this solution the 5G NAS security context is protected before being re-routed via RAN together with the Registration Request (RR) message. The protection utilizes the NSSF as a trusted NF by both the initial and the target AMF. The NSSF belongs to the operator who deploys different slices and is assumed to serve all the slices offered by the operator.

### 6.9.2 Solution details

The initial AMF protects the security context or the potentially horizontally derived security context with an encryption key generated by the NSSF. Then the initial AMF sends both the Registration Request (RR) and a protected 5G NAS security context container (includes the security context along with the keyAmfHDerivationInd indicator if needed and potentially UL/DL NAS COUNTs) to the target AMF via RAN.



Figure 6.9.2-1: AMF re-allocation with NAS message and 5G NAS security context re-route via RAN

.Editor's Note: Aligning the figure with SA2 procedures is FFS.

Figure 6.9.2-1 shows the solution steps:

1. The UE prepares a Registration Request message including a SUCI or 5G-GUTI and slicing information which could potentially cause an AMF re-allocation such as Requested NSSAI. If the UE has a 5G NAS security context (Registration with 5G-GUTI) it includes a protected NAS container in the Registration Request message.

2. The RAN selects and forwards the RR message to an initial AMF.

3-4. These steps may only take place if UE has indicated its 5G-GUTI in the Registration Request message and if there is connectivity between the initial AMF and the old AMF (cases 2.a.i and 2.b.i in clause 4.3). 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.

If there is no connectivity between the initial AMF and the old AMF (cases 2.a.ii and 2.b.ii in clause 4.3) and the UE has indicated its 5G-GUTI in the Registration Request message, then steps 3 and 4 are skipped and the initial AMF requests the UE identity SUCI from the UE in step 5 and then initiates primary authentication in step 6.

Editor's Note: It is FFS if the Old AMF provides the current 5G security context.

5. The initial AMF may perform an Identity Request for a SUCI towards the UE.

6. The initial AMF may initiate a new primary authentication. This step is optional. This step is needed if the UE has indicated its SUCI in the Registration Request message

7. 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 or the Registration Request included the UE SUCI.

8. 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.

9. If the initial AMF needs UE's subscription information or the SUPI 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 the UDM.

10. 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 the initial AMF.

11. 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 the Requested NSSAI.

12. 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.

13. The initial AMF decides to reroute the RR message to a target AMF via RAN.The initial AMF requests a protection key from the NSSF for the purpose of AMF re-allocation and provides the RR and the target AMF set or target AMF address(es) as input.

Editor's Note: The details of key generation and key identifier generation on the NSSF is FFS.

14. The NSSF uses one or more of the provided inputs in Step 13 to generate a key Kamfreal and a key identifier/token Kamfreal ID. The NSSF stores the key, key identifier/token and the provided input (RR, target AMF address(es)).

15. The NSSF responds with the Kamfreal and a key identifier/token Kamfreal ID.

16. The initial AMF optionally performs horizontal Kamf derivation of Kamf-0 to generate a new Kamf-1. This step would ensure that the target AMF has no access to the Kamf-0 key used by the initial AMF. If the Initial AMF performs horizontal Kamf derivation then the initial AMF resets the corresponding uplink and downlink NAS COUNTs.

17. The initial AMF encrypts the security context (including Kamf-0 or Kamf-1), the keyAmfHDerivationInd indicator and potentially other parameters (e.g. UL/DL NAS COUNTs if horizontal key derivation was performed in Step 16) with the Kamfreal and creates a protected 5G NAS security context container. With respect to the protection algorithm(s) there are multiple alternatives. The protection algorithm(s) could be assumed to static and known to all the AMFs. Or the initial AMF could select one of the algorithms from a set and indicate the algorithm information in the Steps 18-19 in the protected 5G security context container. The NAS protection algorithms could be used for the protection of the 5G NAs security context container with parameters to be determined in the normative phase.

Editor's Note: It is FFS if and how the 5G NAS security context container is integrity protected.

18. The initial AMF forwards the complete Registration Request message, the protected 5G NAS security context container, the Kamfreal ID and potentially other parameters (e.g. AMF address(es)) to the RAN.

19. The RAN forwards the complete Registration Request message, the protected 5G NAS security context container, the Kamfreal ID to the target AMF.

20. The target AMF requests the protection key Kamfreal from the NSSF by providing the its own address, the RR, and the Kamfreal ID to the NSSF. The NSSF verifies that the target AMF is included in the target AMF set or its address matches one of the target AMF addresses provided by the initial AMF. If the verification is successful the NSSF returns the protection key Kamfreal to the target AMF and deletes the Kamfreal and Kamfreal ID.

21. The target AMF decrypts the protected 5G NAS security context container.

22. After decrypting the security context,

if SUCI is included in the Registration Request, the target AMF skips step 22 (as no additional information about established PDU sessions etc. is stored in the old AMF).

If a 5G-GUTI is included in the Registration Request and the target AMF has received a 5G NAS security context and potentially a keyAmfHDerivationInd indicator, then:

- If there is no connectivity between the target AMF and old AMF (cases 2.a.ii and 2.b.ii in clause 4.3), the target AMF skips step 22 (as any additional information about established PDU sessions etc. stored in the old AMF cannot be retrieved by the target AMF).

- If there is connectivity between the target AMF and the old AMF (cases 2.a.i and 2.b.i in clause 4.3), the target AMF can fetch any additional information about established PDU sessions etc. stored in the old AMF.

23. If the target AMF has received the keyAmfHDerivationInd indicator, then the target AMF shall run a NAS SMC procedure with the UE, to take the new Kamf-1 key into use with the UE.

24. The target AMF needs to initiate 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.

The target AMF determines that a NAS re-route via RAN has taken place and the target AMF shall use the Kamf-1 only for the purpose of sending protected NAS Security Mode Command and Authentication Challenge/Request to the UE, and for receiving protected NAS Security Mode Complete and Authentication Response from the UE.

25-26. The target AMF needs to run a new NAS SMC procedure with the UE to take the new Kamf-2 into use with the UE. The target AMF needs to include the request to the UE to include the complete Registration Request message in the NAS Security Mode Complete message by setting the flag "request initial NAS flag" in the NAS Security Mode Command message. The UE includes the complete Registration Request message (sent in step 1) in the NAS Security Mode Complete message to the target AMF. This means that the target AMF can take the Registration Request message received in NAS Security Mode Complete message into use and drop the Registration Request message rerouted via RAN.

### 6.9.3 Evaluation

In this solution the 5G NAS security context is protected before being re-routed via RAN together with the Registration Request (RR) message. The protection utilizes the NSSF as a trusted NF by both the initial and the target AMF. The NSSF belongs to the operator who deploys different slices and is assumed to serve all the slices offered by the operator.

The initial AMF sends the security context to the target AMF encrypted so that that the AMF key is not exposed to the RAN node. Although that RAN node has access to all the parameters to retrieve the decryption key of the protected 5G NAS security context container, the RAN node cannot directly request the decryption since it does not have a direct SBA interface to the NSSF. The RAN node is allowed to connect to the core network only via the NGAP protocol specified in TS 38.413 [5].

In this solution there is one more optional NAS SMC performed by the target AMF after the Registration Request message and the protected 5G NAS security context container including the AMF key (Kamf-0 or Kamf-1) has been re-routed via RAN. This optional NAS SMC is performed in order to take the new Kamf-1 key into use by the UE and target AMF (after the optional horizontal Kamf derivation of Kamf-0 to generate a new Kamf-1 in the initial AMF).

The optional horizontal Kamf derivation in the initial AMF provides **backward security** so the target AMF has no access to the Kamf-0 and its corresponding NAS key used between the UE and the initial AMF. The initial AMF has access of the new Kamf-1 key re-routed via RAN to the target AMF, but after the target AMF has taken the new Kamf-1 key into use with the UE by running a NAS SMC, the target AMF can initiate a new protected Authentication procedure with the UE in order to generate a new Kamf-2 key shared with the UE, which the initial AMF has no access to. By running a new NAS SMC procedure between target AMF and UE to take the new Kamf-2 key into use, **forward security** is provided.

This solution has the following impact:

UE:

Editor's Note: It is FFS if the solution impacts the UE

AMF:

This initial AMF may need to perform horizontal Kamf derivation of the Kamf before forwarding the protected 5G NAS security context container together with the complete Registration Request message on the N2 interface to the RAN.

- The initial AMF needs to request for a protection key from the NSSF and process the NSSF response.

- The initial AMF needs to encrypt the 5G NAS security context and potentially other parameters and produce the protected 5G NAS security context container.

- The target AMF needs to decrypt the protected 5G NAS security context container.

- The target AMF may need to perform a NAS SMC procedure to take any potentially horizontally derived Kamf key into use before initiating a primary authentication

- The target AMF also needs to perform an authentication request in order to produce its own security context.

NSSF:

- The NSSF is an optional NF and this solution would require NSSF to be deployed and trusted by the initial and target AMF.

- The NSSF needs a new service to generate keys and key identifiers for the protection of the 5G NAS securuty context container of the initial AMF and provide the keys and key identifiers to the target AMF.

RAN:

- This solution has impact on RAN and N2 interface. The REROUTE NAS REQUEST message is defined in TS 38.413 [4] and the initial AMF includes the INITIAL UE MESSAGE into the REROUTE NAS REQUEST message to RAN. The REROUTE NAS REQUEST message needs to be updated to include the protected 5G NAS security context container and potentially other parameters. Also the RAN needs to forward the protected 5G NAS security context container and potentially other parameters to the target AMF together with the INITIAL UE MESSAGE.

# 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.

3. 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.

4. The initial AMF decides to reroute the RR to the Target AMF.

5. The initial AMF reroutes the Registration Request to the target AMF, via (R)AN.

6. The target AMF initiates the primary authentication. The target AMF fetches RAND, AUTN and other parameters from the AUSF.

7. 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.

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 Registration Request (RR) message including 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 which assigned the 5G-GUTI.

3. The initial AMF chooses to perform a primary authentication run based on local policy or if the retrieval of UE context in step 2 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. The 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. Both UE and the initial AMF generates Kamf\_new. NAS Security Mode Control procedure has been initiated by the initial AMF to activate the new NAS security context in 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. 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 |
| 2021-01 | SA3#102-e | S3-210620 |  |  |  | Version after incorporating changes in S3-210374, S3-210576, S3-210631, S3-210646, S3-210683, S3-210684, S3-210685. | 0.3.0 |
| 2021-03 | SA3#102bis-e | S3-211288 |  |  |  | Version after incorporating changes in S3-210961, S3-211194, S3-211195, S3-211196, S3-211245, S3-211247, S3-211248, S3-211279, S3-211285, S3-211286, S3-211315, S3-211316, S3-211334, S3-211335. | 0.4.0 |