|  |
| --- |
| 3GPP TR 33.745 V19.1.0 (2025-03) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security aspects of 5G Next Radio (NR) Femto(Release 19) |
|   |
|  |  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2025, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 6

1 Scope 8

2 References 8

3 Definitions of terms, symbols and abbreviations 8

3.1 Terms 8

3.2 Symbols 9

3.3 Abbreviations 9

4 Security Architecture and Assumptions 9

5 Key issues 9

5.1 Key Issue #1: Security of 5G NR Femto Ownership 9

5.1.1 Key issue details 9

5.1.2 Security threats 10

5.1.3 Potential security requirements 10

5.2 Key issue #2: Authentication aspect of 5G NR Femto connecting to the operator network. 10

5.2.1 Key issue details 10

5.2.2 Security Threats 10

5.2.3 Potential security requirements 10

5.3 Key Issue #3: Support of 5G Femto location security 10

5.3.1 Key issue details 10

5.3.2 Security threats 11

5.3.3 Potential security requirements 11

5.4 Key Issue #4: UE access control 11

5.4.1 Key issue details 11

5.4.2 Security threats 11

5.4.3 Potential security requirements 11

5.5 Key Issue #5: Protection of backhaul link between 5G NR Femto and 5GC 11

5.5.1 Key issue details 11

5.5.2 Security threats 11

5.5.3 Potential security requirements 12

5.6 Key Issue #6: Hosting Party authentication 12

5.6.1 Key issue details 12

5.6.2 Security threats 12

5.6.3 Potential security requirements 12

5.7 Key Issue #7: Direct link between 5G NR Femtos 12

5.7.1 Key issue details 12

5.7.2 Security threats 12

5.7.3 Potential security requirements 12

5.8 Key Issue #8: 5G NR Femto management system accessible on the public internet 13

5.8.1 Key issue details 13

5.8.2 Security threats 13

5.8.3 Potential security requirements 13

5.9 Key issue #9: 5GS Core network topology hiding from 5G NR Femto deployments 13

5.9.1 Key issue details 13

5.9.2 Threats 13

5.9.3 Potential security requirements 13

6 Solutions 14

6.0 Mapping of solutions to key issues 14

6.1 Solution #1: Reusing existing mechanism for Ownership Security 14

6.1.1 Introduction 14

6.1.2 Solution details 14

6.1.3 Evaluation 14

6.2 Solution #2: IKEv2 EAP-AKA-based authentication 14

6.2.1 Introduction 14

6.2.2 Solution details 15

6.2.3 Evaluation 16

6.3 Solution #3: Solution to secure backhaul of 5G NR Femto 16

6.3.1 Introduction 16

6.3.2 Solution details 16

6.3.3 Evaluation 17

6.4 Solution #4: UE access control using CAG verification 17

6.4.1 Introduction 17

6.4.2 Solution details 17

6.4.3 Solution Evaluation 19

6.5 Solution #5: Security of 5G NR Femto Ownership 20

6.5.1 Solution details 20

6.5.2 Solution Evaluation 21

6.6 Solution #6: Multi-factor authentication based femto owner/manager authentication 21

6.6.1 Solution details 21

6.6.2 Solution Evaluation 23

6.7 Solution #7: Support of 5G NR Femto location security 23

6.7.1 Solution details 23

6.7.2 Solution Evaluation 25

6.8 Solution #8: Security solution for backhaul link between 5G NR Femto and 5GC 25

6.8.1 Introduction 25

6.8.2 Solution details 25

6.8.3 Evaluation 26

6.9 Solution #9: Hosting party authentication using EAP-AKA’ 26

6.9.1 Introduction 26

6.9.2 Solution details 26

6.9.3 Evaluation 27

6.10 Solution #10: Verify and authorise direct connections between 5G NR Femtos 27

6.10.1 Introduction 27

6.10.2 Solution details 28

6.10.3 Evaluation 29

6.11 Solution #11: Security solution for backhaul link between 5G NR Femto and 5G NRFemto MS 29

6.11.1 Introduction 29

6.11.2 Solution details 29

6.11.3 Evaluation 29

6.12 Solution #12: Reusing existing location verification security features 29

6.12.1 Introduction 29

6.12.2 Solution details 29

6.12.3 Evaluation 29

6.13 Solution #13: Security solution for UE CAG verification 30

6.13.1 Introduction 30

6.13.2 Solution details 30

6.13.3 Evaluation 30

6.14 Solution #14: security between 5G NR Femtos 30

6.14.1 Introduction 30

6.14.2 Solution details 30

6.14.3 Evaluation 30

6.15 Solution #15: Verify the 5G NR Femto location with Security Gateway 30

6.15.1 Introduction 30

6.15.2 Solution details 30

6.15.3 Evaluation 31

7 Conclusions 32

7.1 Conclusions to Key Issue #1: Security of 5G NR Femto Ownership 32

7.2 Conclusions to Key Issue #2: Authentication aspect of 5G NR Femto connecting to the operator network 32

7.3 Conclusions to Key Issue #3: Support of 5G Femto location security 32

7.4 Conclusions to Key Issue #4: UE access control 33

7.5 Conclusions to Key Issue #5: Protection of backhaul link between 5G NR Femto and 5GC 33

7.6 Conclusions to Key Issue #6: Hosting Party authentication 33

7.7 Conclusions to Key Issue #7: Direct link between 5G NR Femtos 33

7.8 Conclusions to Key Issue #8: 5G NR Femto management system accessible on the public internet 33

7.9 Conclusions to Key Issue #9: 5GS Core network topology hiding from 5G NR Femto deployments 34

Annex A : Change history 35

# 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.

# 1 Scope

The present document studies the potential security enhancements for supporting 5G NR Femto. More specifically, the study investigates potential security enhancements in the following areas:

- With the gap analysis, study the potential updates or enhancements needed for 5G NR Femto over TS 33.320[2].

- Study the security impacts for interworking between CAG and CSG cells.

- Study the security impacts of enabling provisioning of subscribers allowed to access 5G NR Femto cells and how to manage 5G NR Femto access control by the Closed Access Group (CAG) owner or an authorized administrator.

# 2 References

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

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

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

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

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

[2] 3GPP TS 33.320: "Security of Home Node B (HNB) / Home evolved Node B (HeNB)".

[3] 3GPP TR 23.700-45: "Study on system aspects of 5G NR Femto"

[4] 3GPP TS 23.501: "System Architecture for the 5G System".

[5] 3GPP TS 22.220: "Service requirements for Home Node B (HNB) and Home eNode B (HeNB)".

[6] 3GPP TS 38.799: "Study on Additional Topological Enhancements for NR"

[7] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS)"

[8] 3GPP TS 29.503: "5G System; Unified Data Management Services".

[9] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[10] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[11] 3GPP TS 23.502: "Procedures for the 5G System".

[12] 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 TR 21.905 [1], TR 23.700-45[3] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

**CAG:** as defined in TS 23.501 [4].

**CSG:** as defined in TS 22.220 [5].

**Hosting Party:** as defined in TS 22.220 [5].

**NR Femto Hosting Party:** "H(e)NB Hosting Party" defined in TS 22.220 [5].

**CAG Owner**: NR Femto Hosting Party.

NOTE: CAG owner is authenticated and authorized by the 5GC to operate (add/delete/modify) on the allowed CAG list of the users.

## 3.2 Symbols

Void

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

CAG Closed Access Group

CSG Closed Subscriber Group

# 4 Security Architecture and Assumptions

The following architecture and security assumptions are applied to the present document:

- The architectural assumptions and principles captured in TR 23.700-45 [3] are used as architecture assumptions in this study.

- The security architecture defined in clause 4.1 in TS 33.320[2] can be reused as basis for this study. Whether all components are all necessary and what are the function names in 5G will be studied in the present document.

UE

H(e)NB

SeGW

insecure link

Operator’s security domain(s)

H(e)NB-GW

H(e)MS

H(e)MS

AAA Server/HSS

L-GW

Figure 4.1: System Architecture of H(e)NB defined in TS 33.320[2]

- The security requirements captured in TS 33.501 [10] Annex I.4 are used as security assumptions in this study.

# 5 Key issues

## 5.1 Key Issue #1: Security of 5G NR Femto Ownership

### 5.1.1 Key issue details

According to TR 23.700-45 [3], the 5G NR Femto aims to re-use the existing CAG mechanism defined for PNI-NPN for access control. In order to add flexibility to the 5G NR Femto, the owner of 5G NR Femto (or CAG or both) is able to control which UE(s) can access to the 5G NR Femto.

The 5G NR Femto owner or administrator (or CAG or both) may or may not belong to the operator domain and is able to provide/update CAG information to the network that 5G NR Femto serves and the network that the UE has subscription.

From a security point of view, a fake owner of 5G NR Femto or an unauthorized administrator may provision false information of subscribers allowed to access 5G NR Femto cells. Thus, only the authenticated 5G NR Femto owner or an authorized administrator is able to manage the CAG information for 5G NR Femto. A mechanism for authentication and authorization for the owner or administrator is needed.

### 5.1.2 Security threats

Unauthorized parties or fake owner of 5G NR Femto can gain access to the CAG information and perform unauthorized operation (e.g. update, deletion) to the CAG information if the owner or the administrator is not properly authenticated or authorized.

### 5.1.3 Potential security requirements

The 5GS shall support means for authentication and authorization of the 5G NR Femto owner.

## 5.2 Key issue #2: Authentication aspect of 5G NR Femto connecting to the operator network.

### 5.2.1 Key issue details

When a 5G NR Femto connects to the operators’ core network, based on a deployment scenario the 5G NR Femto cell may not be in operators’ control. The 5G NR Femto may be using unsecure public and/or 3rd party network to connect with the operator core. If a fake 5G NR Femto connects to operator’s security domain, it may steal sensitive information from operator’s security domain and/or provision false information to operator’s security domain. Unless adequate security measures are in place, this may make both, the 5G NR Femto as well as operator’s network vulnerable to security threats and compromise its integrity and functionality.

### 5.2.2 Security Threats

Possible loss of confidentiality, integrity and threats on network availability are likely due to lack of security of the services offered by 5G NR Femtos deployed in non-trusted environments.

- Malicious attacker may claim to be genuine 5G NR Femto in order to request certain services (theft of service) or information (data leakage) and mount further attacks towards the core network.

- Man in the Middle attacks between the genuine 5G NR Femto and the operator’s core network.

### 5.2.3 Potential security requirements

The 5GS shall support a mechanism to establish mutual authentication between 5GS and 5G NR Femto.

## 5.3 Key Issue #3: Support of 5G Femto location security

### 5.3.1 Key issue details

The 5G NR Femto can be deployed in residential homes, the buildings of enterprises and small business etc., and are out of the direct operators’ control. Operators require assurance of the 5G Femto location to satisfy various security, regulatory and operational requirements.

TS 33.320 [2] lists some information which may be used to perform location verification and specifies H(e)MS and/or HNB-GW as the verifying node, based on the gap analysis, this key issue is supposed to investigate whether the location verification information list may need to be updated or complemented.

### 5.3.2 Security threats

If an attacker either changes the location information of an 5G NR Femto or is in position to mis-inform 5G NR Femto regarding its location. Thus a stolen 5G NR Femto could be used in unwanted place, the following problems may occur:

- Users: Users might have no service in primarily expected location. Emergency calls might be routed to the wrong location.

- Operator network: Provisioning of services meant for different location with potential impact on revenue.

If 5G Femto changes its location without reporting, customers may relocate Femto and make the provisioned location information invalid, the following problems may occur:

- Users: Emergency call from such Femto cannot be reliably located, or routed to correct emergency centre. This also violates governmental requirements in some counties.

- Operator: Lawful interception position reporting becomes impossible.

### 5.3.3 Potential security requirements

5G NR Femto location verification mechanism shall be supported to satisfy various security, regulatory and operational requirements of operators.

## 5.4 Key Issue #4: UE access control

### 5.4.1 Key issue details

SA2’s architecture assumes that the existing CAG concept defined for PNI-NPN is re-used for Femto access control. This key issue investigates UE access control mechanism to support the UE accessing to the cell of 5G NR Femto.

NOTE: As concluded in TR 23.700-45 [3] clause 8.2, this key issue does not cover the scenario where the UE moves between CAG cell of 5G Femto and CSG cell. This scenario is not to be addressed.

### 5.4.2 Security threats

If a rogue UE accesses to an 5G Femto gNB with a given CAG ID, to which it does not belong to, the following types of attacks could potentially occur:

- The wasting of resource of 5G NR Femto.

- The Femto owner might end-up paying the charges for the rogue user.

### 5.4.3 Potential security requirements

UE access control with CAG concept of 5G NR Femto shall be supported.

## 5.5 Key Issue #5: Protection of backhaul link between 5G NR Femto and 5GC

### 5.5.1 Key issue details

5G NR Femto will connect with operator’s core network. The backhaul will carry signaling messages of the UE and 5G NR Femto, and the User Plane messages of UE. This key issue investigates the protection mechanism for the traffic on the backhaul link between 5G NR Femto and 5GC.

### 5.5.2 Security threats

Not applicable.

### 5.5.3 Potential security requirements

The transport of control plane data over backhaul shall be integrity, confidentiality and replay-protected.

The transport of user data over backhaul shall be integrity, confidentiality and replay-protected

## 5.6 Key Issue #6: Hosting Party authentication

### 5.6.1 Key issue details

The optional EAP-AKA-based hosting party authentication following the device authentication of the H(e)NB is documented in TS 33.320 [2], it needs to investigate whether the IKEv2 EAP-AKA authentication mechanism is appropriate for 5G Femto.

This key issue proposes to investigate whether the IKEv2 EAP-AKA authentication mechanism is still appropriate for 5G Femto, whether any upgrade is needed, and the related procedure.

### 5.6.2 Security threats

Identity authentication is the basis of security, if the hosting party is required, lack of authentication for the hosting party may lead to spoofing or impersonation attacks.

### 5.6.3 Potential security requirements

When hosting party is required in 5G Femto, the related hosting party authentication mechanism shall be supported.

## 5.7 Key Issue #7: Direct link between 5G NR Femtos

### 5.7.1 Key issue details

A 5G NR Femto may establish a direct link to another 5G NR Femto. If the direct link is not protected, the traffic may be eavesdropped, or tampered etc. And if a fake or unauthorized 5G NR Femto connects to another 5G NR Femto, it may steal sensitive information from the 5G NR Femto and/or provision false information to the 5G NR Femto.

### 5.7.2 Security threats

If traffic on the direct link between 5G NR Femtos is not confidentiality protected, sensitive information may be leaked to unauthorized entities.

If the integrity of the traffic on the direct link between 5G NR Femtos is not protected, the data may be modified.

A fake or unauthorized 5G NR Femto may steal sensitive information from another 5G NR Femto and/or provision false information to another 5G NR Femto.

### 5.7.3 Potential security requirements

5GS shall support confidentiality, integrity, and replay protection for direct link between 5G NR Femtos.

5GS shall support authenticate and authorize the direct link between 5G NR Femtos.

## 5.8 Key Issue #8: 5G NR Femto management system accessible on the public internet

### 5.8.1 Key issue details

The 5G NR Femto management system(Femto MS) configures 5G NR Femto and installs software updates on the 5G NR Femto according to the operator’s policy. The Femto MS may be located inside the operator’s access or core network (accessible on the MNO Intranet) or outside of it (accessible on the public internet).

When the Femto MS is accessible on the public internet, a fake or unauthorized 5G NR Femto may connect to the Femto MS, or a 5G NR Femto may connect to a fake Femto MS. And if the connection between 5G NR Femto and Femto MS is not protected, the traffic may be eavesdropped, or tampered etc.

### 5.8.2 Security threats

If the connection between 5G NR Femto and Femto MS is not confidentiality protected, sensitive information may be leaked to unauthorized entities.

If the integrity of the traffic between 5G NR Femto and Femto MS is not protected, the data may be modified.

A fake or unauthorized 5G NR Femto may steal sensitive information from Femto MS.

A fake or unauthorized Femto MS may provision false information to 5G NR Femto.

### 5.8.3 Potential security requirements

5GS shall support confidentiality, integrity, and replay protection for the connection between 5G NR Femto and Femto MS.

5GS shall support mutual authentication and authorization between 5G NR Femto and Femto MS.

## 5.9 Key issue #9: 5GS Core network topology hiding from 5G NR Femto deployments

### 5.9.1 Key issue details

When a NR Femto cell connects to the operators’ core network, based on a deployment scenario the Femto may not be under direct control of the operator. The 5G NR Femto may be using unsecure public and/or 3rd party network to connect with the operator core. In such a deployment scenario, visibility of the operators’ core network topology to the5G NR Femto, this may make the operator’s network vulnerable to may threats.

### 5.9.2 Threats

Visibility of the operators’ core network topology to the 5G NR Femto connected over public unsecure networks, may make the operator’s network vulnerable to may threats by exposing it and providing insights about the network to potential rouge entities.

### 5.9.3 Potential security requirements

The 5GS should support a mechanism to establish connectivity with the 5G NR Femto, to enable the femto cells to offer services while hiding the 5GS core network topology from the 5G NR Femto.

# 6 Solutions

## 6.0 Mapping of solutions to key issues

Table 6.0-1: Mapping of solutions to key issues

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Solutions | KI#1 | KI#2 | KI#3 | KI#4 | KI#5 | KI#6 | KI#7 | KI#8 | KI#9 |
| **1** | **X** |  |  |  |  |  |  |  |  |
| **2** |  | **X** |  |  |  |  |  |  |  |
| **3** |  | **X** |  |  | **X** |  |  |  | **X** |
| **4** |  |  |  | **X** |  |  |  |  |  |
| **5** | **X** |  |  |  |  |  |  |  |  |
| **6** | **X** |  |  |  |  |  |  |  |  |
| **7** |  |  | **X** |  |  |  |  |  |  |
| **8** |  |  |  |  | **X** |  |  |  |  |
| **9** |  |  |  |  |  | **X** |  |  |  |
| **10** |  |  |  |  |  |  | **X** |  |  |
| **11** |  |  |  |  |  |  |  | **X** |  |
| **12** |  |  | **X** |  |  |  |  |  |  |
| **13** |  |  |  | **X** |  |  |  |  |  |
| **14** |  |  |  |  |  |  | **X** |  |  |
| **15** |  |  | **X** |  |  |  |  |  |  |

## 6.1 Solution #1: Reusing existing mechanism for Ownership Security

### 6.1.1 Introduction

This solution addresses KI#1 Security of 5G NR Femto Ownership.

### 6.1.2 Solution details

The definition of the 5G Femto owner is the same with the hosting party, who buying the Femtos from the operator. The 5G NR Femto owner or administrator is able to provide/update CAG information to the network. In this case, the owner or administrator can be assumed as an AF in the MNO domain or an AF external to MNO domain. To enhance the 5GS to support receiving and updating of CAG information, the authentication and authorization between AF and the UDM/UDR needs to be supported.

The 5G NR Femto owner interacts with the UDM/UDR using Service-based Interfaces. The existing 5G security mechanism can be reused for the transfer of CAG information over the SBA interface between the owner and the UDM/UDR. When the owner is located in the operator’s network, the UDM/UDR uses Service-Based Interface as depicted in clause 13 of TS 33.501 [10] to communicate with the owner directly. When the owner is located outside the operator’s network, the NEF is used to exchange the messages between the owner and the UDM/UDR. The security aspects of NEF is specified in clause 12 of TS 33.501[10].

### 6.1.3 Evaluation

This solution is align with the progress of system aspects in TR 23.700-45 [3], where the 5GC NF that managing the received CAG information is UDM/UDR. This solution realizes the authentication and authorization requirement between CAG owner or an authorized administrator and UDM/UDR using the existing SBI procedures, without great impact to the 5GC network functions and procedures.

## 6.2 Solution #2: IKEv2 EAP-AKA-based authentication

### 6.2.1 Introduction

This solution addresses KI#2.

This solution proposes to reuse IKEv2 certificate-based authentication as described in TS 33.320 [2] Clause 7.2. This solution also proposes to add IKEv2 EAP-AKA-based authentication as an option.

### 6.2.2 Solution details

When IKEv2 certificate-based authentication is used for authentication between 5G NR Femto and SeGW, the procedure in TS 33.320 [2] Clause 7.2 can be reused.

When IKEv2 EAP-AKA-based authentication is used for authentication between 5G NR Femto and SeGW, the procedure is shown in Figure 6.2-1. The 5G NR Femto is provided by means of a UICC. Subscription data and authentication vectors can be configured in the AAA server, or AAA server can fetch them from UDM.



Figure 6.2-1 IKEv2 EAP-AKA-based authentication

1. Following successful device integrity check, the 5G NR Femto sends an IKE\_SA\_INIT request to the SeGW.

2. The SeGW sends IKE\_SA\_INIT response to the 5G NR Femto.

3. The 5G NR Femto sends IKE\_AUTH request message with the 5G NR Femto’s identity in the IDi payload and the AUTH payload omitted to inform the SeGW that the 5G NR Femto wants to perform EAP authentication.

4. The SeGW sends the Authentication Request message with an empty EAP AVP to the AAA Server, containing the identity received in IKE\_AUTH request message received in step 3.

5. The AAA Server shall fetch the subscription data and authentication vectors from UDM if the subscription data and authentication vectors are not configured in the AAA Server. The AAA Server initiates the authentication challenge.

6. The SeGW sends IKE\_AUTH response to 5G NR Femto. The EAP message received from the AAA Server (EAP-Request/AKA-Challenge) is included in order to start the EAP procedure over IKEv2.

7. The 5G NR Femto processes the EAP challenge message and verifies the AUTN and generates the RES parameters.The 5G NR Femto sends the IKE\_AUTH request with the EAP-Response/AKA-Challenge to the SeGW.

8. The SeGW forwards the EAP-Response/AKA-Challenge message to the AAA Server.

9. When all checks are successful, the AAA Server sends the Authentication Answer including an EAP success and the key material to the SeGW. This key material should consist of the MSK generated during the authentication process.

10. The EAP Success message is forwarded to the 5G NR Femto over IKEv2 in IKE\_AUTH response..

11. The 5G NR Femto takes its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE\_SA\_INIT message. The IKE\_AUTH request with the AUTH parameter is sent to the SeGW.

12. The SeGW checks the correctness of the AUTH received from the 5G NR Femto. The MSK received in step 9 is used by the SeGW to generate the AUTH parameters in order to authenticate the IKE\_SA\_INIT phase messages. Then the IKE\_AUTH response with AUTH parameter is sent to the 5G NR Femto together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.

13. If the SeGW detects that an old IKE SA for that 5G NR Femto already exists, it will delete the IKE SA and send the 5G NR Femto an INFORMATIONAL exchange with a Delete payload in order to delete the old IKE SA in 5G NR Femto.

### 6.2.3 Evaluation

This solution addresses KI#2 by reusing IKEv2 certificate-based authentication and adding IKEv2 EAP-AKA-based authentication as an option.

When IKEv2 EAP-AKA-based authentication is used, the 5G NR Femto needs to be provided by means of a UICC, AAA server needs to be introduced to the 5GC, and the UDM needs to support AAA server, the interface between AAA, UDM needs to be further defined.

## 6.3 Solution #3: Solution to secure backhaul of 5G NR Femto

### 6.3.1 Introduction

The proposed solution addresses the security requirement of key issue#2, key issue#5 and key issue#9.

### 6.3.2 Solution details

The SeGW network element at the border of security domains can be deployed. Here, the 5G NR Femto is in customer premises in one security domain, and the 5GS is in MNO in another security domain. The SeGW in the 3GPP system architecture sits at the front of 5G NR Femto GW function, as depicted TR 38.799 [6] sec 5.2.1.2 (option-2 for NR Femto architecture) also shown below in fig 6.3.1. TR 38.799 [6] concludes that, “The NR Femto GW appears to the AMF as a gNB. The NR Femto GW appears to the NR Femto node as an AMF. The NG interface between the NR Femto node and the 5GC is the same regardless of whether the NR Femto node is connected to the 5GC via an NR Femto GW or not.”



Figure 6.3.1 5G NR Femto Architecture (option-2 in 38.799 sec 5.2.1.2)

The SeGW can provide the following security properties to address KI#2, KI#5 and KI#9: mutual authentication, topology hiding, confidentiality/integrity and anti-replay protection.

The NR Femto and SeGW can inherit principles from clauses 4.3.1, 4.4.2, 4.4.3, 4.4.9 and 7 of TS 33.320 [2].

The NR Femto may directly connect to the 5GC. The NG-RAN architecture may also deploy an NR Femto Gateway (NR Femto GW) to allow the concentration of the NG-C interface between the NR Femto and the 5GC. Based on implementation, the transport of NG-U between the NR Femto and the 5GC may be optionally concentrated in the NR Femto GW. Together with the security properties of SeGW, the core network topology is not directly exposed the 5G NR Femto, so that core network identities such as IP addresses (of AMF, UPF etc.) are not inadvertently exposed to the Femtos which may be beyond operator’s direct control.

### 6.3.3 Evaluation

The solution is leveraging the conclusions from system architecture options work in TR 38.799[6].

This solution can fulfil requirements for KI#9 i.e. 5GS Core network topology hiding from 5G NR Femto deployments.

## 6.4 Solution #4: UE access control using CAG verification

### 6.4.1 Introduction

This solution assumes that secure connection between 5G NR Femto and Serving Network is pre-established.

This solution proposes the following:

- Include Cell Access Mode, CAG ID and 5G NR Femto ID along with NAS Registration Request message from 5G NR Femto to AMF.

- If AMF receives the cell access mode as closed access mode, AMF requests UDM to provide allowed CAG list for the UE requesting for the NAS registration.

- If the CAG ID received from 5G NR Femto is in the allowed CAG list received from UDM, AMF proceeds with UE authentication procedure and subsequent security context establishments as per legacy procedures.

- If the CAG verification fails (CAG ID received from 5G NR Femto is NOT in the allowed CAG list received from UDM), NAS Registration Reject is sent from AMF with the cause for unauthorized CAG access (as per TS 24.501 [7] clause 9.11.3.2)

- This CAG verification can be done before proceeding for UE authentication procedure, or after completion of UE authentication procedure but before establishing NAS security context.

### 6.4.2 Solution details

Figure 6.4.2-1 shows the message sequence where CAG verification is done at AMF before UE authentication procedure.



Figure 6.4.2-1.: CAG verification before UE authentication

Figure 6.4.2-2 illustrates the message sequence where the CAG verification can be done after UE authentication procedure is successfully completed, but before NAS security context establishment.

In both scenarios, AMF requests UDM to provide allowed CAG list and checks if the CAG ID received from 5G NR Femto along with NAS registration request is in the received allowed CAG list. Implementations can re-use existing CAG verification which is performed at UDM, as per clause 5.4.2.2.2 (Step 2b) from TS 29.503 [8], in which case, 200 OK or 403 Forbidden responses can be sent by the UDM according to success or failure respectively.

If this succeeds, further steps are executed as per legacy. If it fails, NAS registration reject message is sent with cause as unauthorized CAG access (per TS 24.501 [7] clause 9.11.3.2).



Figure 6.4.2-2: CAG verification after UE authentication

This solution proposes re-use of the following:

- Clause 5.4.2.2.2 (Step 2b) from TS 29.503 [8] defines the CAG verification before UE authentication by the UDM.

- Solution proposes that reject to be done before or after UE authentication, if CAG verification fails.

- This can allow core networks to optimize the procedure based on number of times the CAG verification has failed, and reduce signaling for potentially malicious UEs and/or manual mode selection, i.e., based on the frequency of the registration attempt the network shall decide whether to reject the request before authentication to avoid signalling overhead (if there is re-try frequent) or after authentication (if updated Allowed CAG list to be provided to the UE), so that AMF send the CAG information in the protected NAS reject message.

- TS 24.501 [7] clause 9.11.3.2: Sending NAS registration reject message with existing cause as unauthorized CAG access if:

- CAG ID verification fails based on subscription data available at UDM.

- TS 23.501 [4] clause 5.30.3.4: AMF includes CAG information in the protected NAS reject message.

NOTE: Requiring CAG verification for each UE at core network can have additional load on the network.

### 6.4.3 Solution Evaluation

This solution has impacts on 5G NR Femtocell, AMF and UDM. This solution can help avoid significant amount of signaling if CAG verification fails.

This solution addresses key issue #4.

## 6.5 Solution #5: Security of 5G NR Femto Ownership

This solution assumes that an AF (web tool) is available to the femto owner to provide authenticated and authorized access to update the allowed CAG list. This is similar to LTE.

This solution proposes the following:

- Pre-provisioned femto owner credentials and/or operator CA signed certificate in UDM/UDR.

- Using AF (web tool), the femto owner presents the credentials and/or operator CA signed certificate for authentication and authorization.

- AF forwards these credentials and/or operator CA signed certificate to NEF.

- NEF further interacts with UDM/UDR to authenticate and authorize the femto owner. Only authenticated and authorized femto owners can update the allowed CAG list.

### 6.5.1 Solution details

Figure 1 shows the message sequence where femto manager authentication procedure using encrypted usrname and password.



Figure 1: Femto manager authentication using username & password

Step 1: AF sends Nnef\_ParameterProvision with encrypted username, password, and/or certificate and CagIdList to NEF (It is assumed that Femto owner-AF and 5GC(UDM/UDR) have negotiated and agreed the encryption algorithm and mechanism).

Step 2: In this step, NEF requests AUSF to verify the username and password using new Nudr\_FemtoOwnerAuthentication request API. During Stage 3 standardization API name may be decided.

Step 3: In this step, AUSF requests UDM/UDR for the credentials.

Step 4: In this step, UDM/UDR responds to AUSF with credentials.

Step 5: In this step, AUSF decrypts and verifies username and password with already stored username and password for that femto owner in UDM/UDR.

Step 6: UDM/UDR responds to NEF using new API Nausf\_FemtoOwnerAutentication Response.

Step 7: After the successful authentication NEF initiates allowed CAG list add/modify/delete operations as it has already received allowedCagList as it is received in step 1.

Step 8: IF the authentication in Step 6 succeeds, existing mechanism may be used to add/modify/delete allowedCagList for a UE.

Step 9: IF the authentication fails in Step 5, NEF sends Nnef\_ParameterProvision with new failure cause=un-authorized femto owner or CAG manager.

### 6.5.2 Solution Evaluation

TS 23.501 [4] has defined term “NR Femto hosting party” which is similar to “H(e)NB Hosting Party” defined in TS 22.220 [5]. Accordingly, for this solution, “5G NR Femto Owner” can be considered as “NR Femto hosting party”.

This solution addresses key issue#1.

Impacted entities: NEF, AUSF, UDM/UDR

## 6.6 Solution #6: Multi-factor authentication based femto owner/manager authentication

This solution proposes the following:

- This solution assumes following.

- DAC is pre-configured femto owner/manager’s biometric templates and other relevant information which may include government ID proof, etc., at the time of femto device procurement from the opetor’s store.

- UDM/UDR is pre-configured with username, password, serial number of Femto, Social Security number / GovtID of femto owner/manager of HgNB ID, encryption alorithms.

- Femto owner/manager reigsters with network as one time so that he can operate (add/delete/modify) on the allowed CAG list of the users.

- In this solution, “biometric templates” imply symmetric hashes derived from biometrics collected. This is similar to existing implementations in UEs supporting biometric based authentication where multiple biometrics are collected from the user and the templates are stored internally for future use.

- After successful registration, femto owner can be authenticated using biometric templates collected during runtime.

### 6.6.1 Solution details

Figure 1 shows the message sequence where femto manager authentication procedure using encrypted usrname and password.



Figure 1: Multi-factor authentication based femto owner/manager registration procedure.

DAC (Digital Asset Container) stores the biometric templates of the femto manager. DAC is managed by the operator and this enables operator to populate the DAC with femto manager details during the femto device procurement.

End user visits operator’s store to purchase/procure the Femto device by providing Name, Phone number and Govt ID proof (E.g., SSN – Social Security Number) and biometric templates.

Operator’s representative at store maps the end username, phone number with Femto serial number, HgNB ID, Installation location, CAG IDs supported by that Femto device in the operator’s database (it may be in UDM/UDR), permissions to operate on allowed CAG list for UE(s).

UDM/UDR (or any equivalent NF) creates and stores the mapping based on the information received in step 2 & also verifies femto manager’s biometric templates form the DAC (Digital Asset Container).

Femto owner establishes connectivity with operator using his USIM. (same as TS 23.502 [11] clause 4.2.2.2.2). This step is done so that Femto owner can send the username, password, and phone number and other details on a secured network.

Femto owner sings up using the AF (web-based tool) by providing the phone number, username, password, encryption algorithm and biometric templates.

UDM/UDR and DAC verifies the femto managers biometric details.

Femto owner receives OTP to his mobile.

Femto owner provides the OTP received from the operator.

UDM/UDR verifies the OTP received from the Femto owner. Now Femto owner is registered with the operator’s network.

Operator send the certificate(s) to the Femto owner (AF: web-based tool). This is the certificate(s) used by the femto owner to authenticate with core network while adding / modifying / deleting the allowed CAG list for UE(s).

Femto one-time registration is successful. From now onwards, Femto owner/manager can add/modify/delete the allowed CAG List based on the need.



Figure 2: Biometric enabled authentication of femto owner.

Figure 2 illustrates the use of registration information during runtime to authenticate the femto owner using biometrics.

### 6.6.2 Solution Evaluation

TS 23.501 [4] has defined term “NR Femto hosting party” which is similar to “H(e)NB Hosting Party” defined in TS 22.220 [5]. Accordingly, for this solution, “5G NR Femto Owner” can be considered as “NR Femto hosting party”.

This solution provides a 5G specific enhanced security for 5G NR Femto owner registration and authentication. This solution addresses key issue #1.

Impacted entities: DAC, AUSF, UDM/UDR, NEF

## 6.7 Solution #7: Support of 5G NR Femto location security

This solution proposes the following:

- This solution assumes that LMF is pre-configured with the 5G NR Femto location when a new Femto is deployed.

- Location verification of the femto device is done by the core network with assistance from the UEs connected to the Femto.

a) Solution does not rely on the Femto to get the location.

- With the knowledge of Femtocell’s coverage region and the location information provided by the UEs connected to the network via the femtocell, the exact location of the Femtocell can be verified.

- Also, this solution proposes to inform Operator or an automation function about any Femto location verification failures.

### 6.7.1 Solution details

Figure 6.7.1-1 shows the message sequence where Core network (AMF) initiated location verification.



Figure 6.7.1-1: Core network (AMF) initiated location verification.

NOTE 1: For the figure 1, TS 23.273 Figure 6.11.1-1 is used as a base.

1. 5G NR Femto sends NG Setup Request by including the 5G NR Femto ID as per TS 38.413 [12].
2. AMF responds with NG Setup Response indicating the NG connection is successful.
3. UE registers with network and is in the RRC connected state.
4. If 5G NR Femto ID is included in the NG Setup request, AMF decides to initiates location verification of 5G NR Femto.
5. AMF obtains UE location using NAS TRANSPORT messages for requesting the UE position, or, using MDT reports provided by the UE. For MDT reports, prior user-consent is verified before seeking the report from UEs connected with the Femto.

NOTE 2**:** If the payload container type is set to "Location services message container" and is included in the UL NAS TRANSPORT, DL NAS TRANSPORT or CONTROL PLANE SERVICE REQUEST message, the payload container contents include location services message payload. This is as per existing 3GPP specification TS 24.501 [7].

1. After obtaining UE location, AMF requests LMF to verify the location information by sending new message Nlmf\_DetermineFemtoLocation Request by including 5G NR Femto ID, Location information, optionally 5G NR Femto serial number may be sent to AMF (during Stage 3 standardization API name may be decided). Any of the existing equivalent message may also be used.

Considering that Femto device is not expected to move beyond a certain range, AMF sends this request only to the LMF of the same serving network. If LMF fails to find the Femto ID and/or its location, failure case is handled as explained below.

1. LMF verifies Location information received from AMF with operator configured location (optionally 5G NR Femto serial number may be considered). Here, LMF uses the 5G NR Femto location information and Femto range to verify whether the UE is within the configured range (coverage area) and checks the relative location to confirm that the 5G NR Femto is at the location where it is supposed to be.
2. LMF responds to AMF with location verification of 5G NR Femto is success.

If the verification is successful Femto services can be continued as normal.

1. If the received location information from AMF (in step 6) is not within the range (coverage area) of the configured/stored Femto location in the LMF then LMF sends Nlmf\_DetermineFemtoLocation Response message to AMF with failure cause = “Femto/5G NR Femto device location has been changed as compared to assigned location”.

This failure message is also sent if the femto device location is not found in that LMF. In such a scenario, a different failure cause indicating “Femto/5G NR Femto device location not found in LMF” can be sent to AMF.

1. AMF notifies operator to take corrective measures because the 5G NR Femto has moved from its location. Also, this can be an indication of a false/compromised 5G NR Femto. Operator can use this information to further apply analytics and derive patterns if any. In some implementations, this information can be sent to an automation function (like NWDAF/MDAF) which can take automated decisions based on analytics.
2. Operator/automation function disables the services to 5G NR Femto due to the change of 5G NR Femto location. In some implementations, the operator/automation function can download factory software with a range of 0 meters, or, disable the broadcast/pilot channel, or any other such methods to ensure that the compromised 5G NR Femto cannot be used.
3. Operator/automation function informs the Femto owner about the disabled services via SMS or other means. This can enable any genuine Femto owners to approach the operator and resolve the problem. Also, Operator/automation function may inform the LEA about this finding of false/compromised 5G NR Femto, if needed based on local regulations.

### 6.7.2 Solution Evaluation

In this solution, AMF contacts only the LMF which belongs to the serving network for verifying the NR femto’s location.

This solution provides an additional location security mechanism for NR Femto. This solution proposes to use UE location, which can be obtained transparently and securely by AMF, to verify the Femto’s actual location and ensure that it has not moved beyond a certain range (e.g., outside the home for residential femtos).

This solution addresses key issue #3.

## 6.8 Solution #8: Security solution for backhaul link between 5G NR Femto and 5GC

### 6.8.1 Introduction

This solution addresses requirement in KI#5, based on the option1 and option2 architectures captured in TR 38.799[6]

The backhaul link between 5G NR Femto and 5GC can be split to two different basic interfaces: the interface between 5G NR Femto and the SeGW, and the interface between the SeGW and the 5GC. The interface between the SeGW and the 5GC can be further split into two interfaces based on whether a new function is introduced into 5GC. This solution covers the security for all 3 potential interfaces.

### 6.8.2 Solution details

The protection of the interface between 5G NR Fetmo and the SeGW is based on IPsec, the keys used for IPsec is pre-configured and is based on certificate is addressed in other solution.

When a new NF is needed the protection of the interface between SeGW and NF is also based on NDS/IP as specified in TS 33.210 [9]. The protection of the interface between 5FTMF with other 5GC function reuses the protection for N2 or N3 as defined in TS 33.501[10].

When a new 5GC function is not needed, the protection of the interface between SeGW and the function in 5GC is the same as N2 or N3 as defined in clause 9 in TS 33.501[10].

### 6.8.3 Evaluation

This solution can fulfil the requirement in KI#5.

This solution reuses existing mechanisms so that does not have system impact.

## 6.9 Solution #9: Hosting party authentication using EAP-AKA’

### 6.9.1 Introduction

This solution addresses requirement in KI#6.

In this solution, EAP-AKA’ authentication between 5G NR Femto and 5GC is introduced. The solution is trying to reuse NSWO authentication defined in clause S.3.2 of TS 33.501[10].

### 6.9.2 Solution details

Similar as NSWO authentication, a new function is introduced as proxy for 5G NR Femto authentication naming as 5FMTF, short for 5G NR Femto Function. This function can be co-located with SeGW or an independent function deployed in the 5GC or co-located with NSWOF. The SeGW is a security gateway that is the same as described in TS 33.320[2].



Figure 6.9.3-1: 5G NR Femto authentication using EAP-AKA’ authentication method

1. The 5G NR Femto establishes connection between the 5G NR FEMTO and the SeGW.

2. The SeGW sends an EAP Identity/Request to the 5G NR FEMTO.

3. The 5G NR Femto sends an EAP Response/Identity message. The 5G NR Femto uses the SUCI in NAI format as its identity.

4. The EAP Response/Identity message is routed over SeGW towards the 5FMTF based on the realm part of the SUCI.

5. The 5FMTF sends the message Nausf\_UEAuthentication\_Authenticate Request with SUCI, Access Network Identity and 5FMT indicator towards the AUSF. 5FMT\_indicator is used to indicate to the AUSF that the authentication request is for 5G NR Femto purposes. The 5FMTF sets the Access Network Identity to "5G: 5FMT".

6. Based on the 5FMT\_indicator, the AUSF (acting as the EAP authentication server) sends a Nudm\_UEAuthentication\_Get Request to the UDM, including SUCI and the Access Network Identity and 5FMT indicator.

7. Upon reception of the Nudm\_UEAuthentication\_Get Request, the UDM invokes SIDF. SIDF de-conceal SUCI to gain SUPI before UDM can process the request. Based on the 5FMT indicator and if 5FMT is allowed based on the subscription data, the UDM/ARPF selects the EAP-AKA´ authentication method and generate an authentication vector using the Access Network Identity as the KDF input parameter. The UDM includes the EAP-AKA’ authentication vector (RAND, AUTN, XRES, CK´ and IK´) and may include SUPI to AUSF in a Nudm\_UEAuthentication\_Get Response message.

8. The AUSF stores XRES for future verification. The AUSF sends the EAP-Request/AKA'-Challenge message to the 5FMTF in a Nausf\_UEAuthentication\_Authenticate Response message.

9. The 5FMTF sends the EAP-Request/AKA'-Challenge message to the SeGW.

10. The SeGW forwards the EAP-Request/AKA'-Challenge message to the 5G NR Femto.

11. At receipt of the RAND and AUTN in the EAP-Request/AKA'-Challenge message, the 5G NR Femto derives CK' and IK' using the Access Network Identity as the KDF input parameter. The 5G NR Femto may derive MSK from CK’ and IK’. When the 5G NR Femto is performing 5FMT authentication, the KAUSF does not be generated by the 5G NR Femto.

12. The 5G NR Femto sends the EAP-Response/AKA'-Challenge message to the SeGW.

13. The SeGW forwards the EAP-Response/AKA'-Challenge message to the 5FMTF.

14. The 5FMTF send the Nausf\_UEAuthentication\_Authenticate Request with EAP-Response/AKA'-Challenge message to AUSF.

15. The AUSF verifies if the received response RES matches the stored and expected response XRES. If the AUSF has successfully verified, it continues as follows to step 16, otherwise it returns an error to the 5FMTF. The AUSF derives the required MSK key from CK’ and IK’, based on the 5FMT indicator received in step 5. The AUSF does not generate the KAUSF.

16. The AUSF sends Nausf\_UEAuthentication\_Authenticate Response message with EAP-Success and MSK key to 5FMTF. The AUSF may optionally provide the SUPI to 5FMTF. The AUSF/UDM does not perform the linking increased home control to subsequent procedures (as stated in present document clause 6.1.4).

17. The 5FMTF sends the EAP-success and MSK to SeGW. The EAP-Success message is forwarded from SeGW to the 5G NR Femto.

18. Upon receiving the EAP-Success message, the 5G NR Femto derives the MSK, if it has not derived the MSK earlier. The 5G NR FEMTO uses the first 256-bit of MSK as PMK to establish a secure connection with the SeGW.

### 6.9.3 Evaluation

This solution can fulfil the requirement in KI#6.

This solution reuses existing NSWO authentication mechanisms so it has the least impact to the 5GS.

## 6.10 Solution #10: Verify and authorise direct connections between 5G NR Femtos

### 6.10.1 Introduction

The proposed solution addresses the security requirements of KI#7.

### 6.10.2 Solution details

The requirements for direct links between 5G NR Femtos should follow the requirements for backhaul links in clause 4.4.5 of TS33.320 [2].

NOTE: The 5G NR Femto can only establish direct links with other base stations after the backhaul link has been established. If the backhaul link is terminated, all direct links to other base stations need to be terminated.

The use of IKEv2/IPsec security procedures on the direct link is optional, and both 5G NR femtoes need to be authorised to establish the direct link. The IKEv2/IPsec security protocol supports the operation of IKEv2 and enables mutual authentication through the use of certificates. The flow of certificate-based mutual authentication between 5G NR Femtos is shown in the figure below.



Figure 6.10.2-1: 5G Femtos certificate authentication process

5G Femto should be equipped with a device certificate, which should be provided by a CA trusted by the operator (such as the operator's CA, the 5G Femto manufacturer or supplier), or by another party trusted by the operator.

1) 5G Femto A sends an IKE\_SA\_INIT request to Femto B.

2) Femto B responds with an IKE\_SA\_INIT response, requesting the certificate of Femto A.

3) Femto A sends an IKE\_AUTH request to Femto B, this request carries the AUTH payload, Femto A’s certificate, and its identity in the IDi payload, with the request for Femto B’s certificate.

4) Note: Remote (i.e., internal) IP address assignment during IKEv2 is independent from establishing a direct connection.

5) Femto B verifies the correctness of the AUTH payload received from Femto A and calculates the AUTH parameter to validate the second IKE\_SA\_INIT message. Femto B also validates the certificate received from Femto A.

6) Femto B sends an IKE\_AUTH response to Femto A, containing its identity, the AUTH parameter, and its own certificate in the IDr payload.

7) Femto A validates Femto B's certificate.

8) If Femto B detects that an old IKE SA of this Femto A already exists, it deletes the old IKE SA and sends an INFORMATIONAL message with a Delete payload to inform Femto A to delete related data.

NOTE: Authorisation steps can also be performed based on a allow/reject list configured by the 5G NR Femto. If the IKEv2/IPsec security mechanism is unavailable, authorisation can also be achieved by using management measures such as virtual LAN configuration. .

### 6.10.3 Evaluation

None.

NOTE: The evaluation of the solution is not addressed in the present document.

## 6.11 Solution #11: Security solution for backhaul link between 5G NR Femto and 5G NRFemto MS

### 6.11.1 Introduction

This solution addresses requirement in KI#8.

### 6.11.2 Solution details

Clause 8.3.2.1 in TR 33.320[2] can be reused with the following modifications:

- Replace H(e)MS with 5G NRFemto MS.

- Replace H(e)NB with 5G NR Femto.

### 6.11.3 Evaluation

This solution can fulfil the requirement in KI#8.

This solution reuses existing mechanisms so that does not have system impact.

## 6.12 Solution #12: Reusing existing location verification security features

### 6.12.1 Introduction

This solution addresses requirements in KI#3: Support of 5G Femto location security.

### 6.12.2 Solution details

The 5G NR Femto MS can be deployed according to the operator’s policy. The 5G NR Femto MS server may be located inside the operator’s access or core network (accessible on the MNO Intranet) or outside of it (accessible on the public Internet). Clause 8.1 in TR 33.320[2] can be inherited with the following modifications:

- Replace H(e)NB with 5G NR Femto.

- Replace H(e)MS with 5G NR Femto MS.

### 6.12.3 Evaluation

This solution reuses the existing security mechanism for 5G NR Femto location verification. This solution complies with the conclusion of the system architecture in TR 38.799 [6]. No system impact to 5GC.

## 6.13 Solution #13: Security solution for UE CAG verification

### 6.13.1 Introduction

This solution addresses Key Issue #4: UE access control.

### 6.13.2 Solution details

CAG verification for UE access control defined in TS 23.502[11], TS 38.413[12] are reused.

### 6.13.3 Evaluation

No system impact to 5GC.

## 6.14 Solution #14: security between 5G NR Femtos

### 6.14.1 Introduction

This solution addresses Key Issue #7: Direct link between 5G NR Femtos.

### 6.14.2 Solution details

The security between 5G NR Femtos shall reuse clause 9.4 of TS 33.501[10].

### 6.14.3 Evaluation

The solution fulfils the requirement in KI#7.

No system impact to 5GC.

## 6.15 Solution #15: Verify the 5G NR Femto location with Security Gateway

### 6.15.1 Introduction

This solution addresses key issue #3.

To meet various security, regulatory and operational requirements, 5G NR Femto’s location needs to be verified as early as possible. The SeGW sitting at the front of 5GC between the two security domains would be the rational node to perform the security check including not only the identity authentication, but also the location verification for the NR Femto node that attempts to connect to 5GC. Depending on the operator’s policy, if the location check of the NR Femto node is unsuccessful, the connection to 5GC could be blocked by the SeGW, which can protect users and operators from the security threats caused by the unwanted location as early as possible. Therefore, as an option of the verifying node described in TS 33.320[2] Clause 8.1, this solution proposes the SeGW as the verifying node to perform the location verification for the NR Femto node.

### 6.15.2 Solution details

As the location verifying node, the SeGW supports the types of location information listed in TS 33.320[2] section 8.1.1,

The location information and the location verification policies can be pre-configured in the SeGW or be dynamically provided by NR Femto management system or 5GC NF.

The SeGW supports to perform location verification using the information provided by the NR Femto node. This information may be provided automatically and/or upon request.

Depending on the result of location verification, the SeGW supports to take one or more of the following actions: block the connection from the NR Femto node to 5GC, raise an alarm, permit the NR Femto node to radiate or prevent the NR Femto node from radiating.

The SeGW supports to block the connection from the NR Femto node to 5GC during or after the mutual authentication process between the NR Femto node and the SeGW. As an example, if the mutual authentication is IKEv2 certificate-based, the location verification during the authentication process can be performed as shown in Figure 1.



Figure 1: Location verification during the mutual authentication process by SeGW

0a.The location information and verification policy can be pre-configured in SeGW.

0b.Optionally the location information and verification policy can be dynamically provided by NR Femto management system or NF in 5GC.

1-3.The same as the steps 1-3 in TS 33.320[2] clause A.1.

4. The same as the step 4 in TS 33.320[2] clause A.1. Additionally, the NR Femto can send its location information in the Notify Payload with a Notification Type of LOCATION\_INFO in the IKE\_AUTH request. Notification Type of LOCATION\_INFO can be defined can configured in both NR Femto and SeGW.

5. The same as the step 5 in TS 33.320[2] clause A.1.

6. The SeGW processes the Notify payload of the IKE\_AUTH request and verify the location of the NR Femto based on the policy of the operator.

7. If the location verification is successful in step 6, the SeGW sends IKE\_AUTH response to continue the authentication.

NOTE 1: If the location verification fails, the following procedure may not be executed based on the operator policy.

8-9. The same as the steps 8-9 in TS 33.320[2] clause A.1.

### 6.15.3 Evaluation

This solution addresses key issue #3. The SeGW takes the role as the verifying node to perform the location verification for the NR Femto node. This solution can handle and block the security threats as early as possible.

The SeGW takes same role as a mandatory network entity which is specified in TS 33.320 [2] and can be used for additional way of femto location verification.

# 7 Conclusions

## 7.1 Conclusions to Key Issue #1: Security of 5G NR Femto Ownership

It is agreed to consider the following principles for the normative work:

- The security aspects of NEF specified in clause 12 of TS 33.501[10] can be reused.

- The CAG owner/administrator is authenticated and authorized by the 5GC to operate (add/delete/modify) on the allowed CAG list of the users.

- TS 23.501 [4] defined term “NR Femto hosting party” which is similar to “H(e)NB Hosting Party” defined in TS 22.220 [5] will be used during the normative phase. Also, as clarified by SA2, “NR Femto hosting party” plays the role of “CAG owner”.

NOTE: Considering above terminology, the concepts of “H(e)NB Hosting Party Authentication” defined in TS 33.320 [2] can be re-used for “NR Femto hosting party authentication”.

To be decided during normative phase, whether multi-factor authentication based solutions can be considered as optional implementation alternatives for “NR Femto hosting party authentication”.

## 7.2 Conclusions to Key Issue #2: Authentication aspect of 5G NR Femto connecting to the operator network

It is agreed to consider the following principles for the normative work:

- The SeGW network element can be deployed at the border of operator’s security domain and the security features for device mutual authentication specified in TS 33.320 [2] can be inherited with the following changes:

- Replace H(e)NB with 5G NR Femto.

- IKEv2 EAP-AKA-based authentication can be as an option for authentication between 5G NR Femto and SeGW.

## 7.3 Conclusions to Key Issue #3: Support of 5G Femto location security

It is agreed to consider the following principles for the normative work:

- The location verification security mechanisms specified in TS 33.320 [2] clause 8.1 can be inherited with the following changes:

- Replace H(e)NB with 5G NR Femto.

- Replace H(e)MS with 5G NR Femto MS.

- The 5G NR Femto MS can act as the verifying node.

- Furthermore, UE location-based verification, or SeGW assisted verification can be optionally considered as additional location verification for 5G NR Femto.

## 7.4 Conclusions to Key Issue #4: UE access control

It is agreed to consider the following principles for the normative work:

- The CAG based access control mechanism for a CAG capable UE accessing the 5G NR Femto is performed in the core network.

- CAG verification for UE access control defined in TS 23.502[11], TS 38.413[12] is reused.

- No solution is needed for normative work for interworking between CAG and CSG cells in this release.

## 7.5 Conclusions to Key Issue #5: Protection of backhaul link between 5G NR Femto and 5GC

It is agreed to consider the following principles for the normative work:

- The protection of the interface between 5G NR Fetmo and the SeGW is based on IPsec, the keys used for IPsec is pre-configured and is based on certificate.

- When NR Femto GW is needed, the protection of the interface between SeGW and NR Femto GW is also based on NDS/IP as specified in TS 33.210 [9]. The protection of the interface between NR Femto GW with other 5GC function reuses the protection for N2 or N3 as defined in TS 33.501[10].

- When NR Femto GW is not needed, the protection of the interface between SeGW and the function in 5GC is the same as N2 or N3 as defined in clause 9 in TS 33.501[10].

NOTE: The impact on the above links for the support of EAP-AKA’ will be decided in normative phase.

## 7.6 Conclusions to Key Issue #6: Hosting Party authentication

It is agreed to consider the following principles for the normative work:

- Device Authentication of the 5G NR Femto by the SeGW can be followed with a hosting party authentication. The security features for hosting party authentication specified in TS 33.320 [2] can be inherited with the following changes:

- Replace H(e)NB with 5G NR Femto.

- EAP-AKA’-based hosting party authentication can be as an option for hosting party authentication.

NOTE: the impact on the networkfunctions to support EAP-AKA’ will be decided in the normative phase.

## 7.7 Conclusions to Key Issue #7: Direct link between 5G NR Femtos

It is agreed to consider the following principles for the normative work:

- The security aspects for direct links between 5G NR Femtos specified in TS 33.320 [2] can be inherited with the following changes:

- Replace HNB/H(e)NB with 5G NR Femto.

- Replace Iurh/X2 interface with Xn interface.

## 7.8 Conclusions to Key Issue #8: 5G NR Femto management system accessible on the public internet

It is agreed to consider the following principles for the normative work:

- The security features for H(e)MS accessible on public Internet specified in TS 33.320 [2] can be inherited with the following changes:

- Replace H(e)NB with 5G NR Femto.

- Replace H(e)MS with 5G NR Femto MS.

## 7.9 Conclusions to Key Issue #9: 5GS Core network topology hiding from 5G NR Femto deployments

Aggregation function hides control plane and user plane.

Annex A :
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-12 | SA#106 | SP-241795 |  |  |  | Presented for information and approval | 1.0.0 |
| 2025-01 |  |  |  |  |  | Upgrade to change control version | 19.0.0 |
| 2025-03 | SA#107 | SP-250110 | 0001 | - | F | Clean up for TR 33.745 | 19.1.0 |