|  |
| --- |
| 3GPP TS 33.545 V0.1.0 (2025-02) |
| Technical Specification |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Security aspects of 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 4

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 7

3.3 Abbreviations 7

4 Overview of Security Architecture and Requirements 8

4.1 Security Architecture of NR Femto 8

4.2 Reference points and functional entities 8

4.2.1 Functional entities 8

4.2.1.1 General 8

4.2.1.2 NR Femto 9

4.2.1.3 Security Gateway (SeGW) 9

4.2.1.4 NR Femto Management System 9

4.2.1.5 AAA Server/AUSF and UDM 9

4.2.2 Reference points 9

5 Security For NR Femto 9

5.1 General 9

5.1 Device Authentication 9

5.2 NR Femto Hosting Party Authentication 9

5.2.1 General 9

5.2.2 Combined device and hosting Party authentication procedure 10

5.3 Location Security 11

5.3.1 General 11

5.3.2 Location verification during the mutual authentication process by SeGW 12

5.3.3 Locations of UEs connected to the 5G NR Femto 13

5.4 Backhaul Link Protection 13

5.5 Access Control Mechanisms for Femto 13

5.6 Topology Hiding 13

Annex <X> (informative): Change history 14

# 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 specifies the security architecture for NR Femto subsystem. This includes security requirements on NR Femto, and other NR Femto associated network nodes (e.g. SeGW and NR Femto MS), as well as the procedures and features which are provided to meet those requirements.

# 2 References

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

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

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

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

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

[2] 3GPP TS 23.501: "System Architecture for the 5G System".

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

[4] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description".

[5] 3GPP TS 33.320: "Security of Home Node B (HNB) / Home evolved Node B (HeNB)".

[6] 3GPP TS 32.593: "Telecommunication management; Procedure flows for Type 1 interface H(e)NB to H(e)NB Management System (H(e)MS) ".

[7] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[8] 3GPP TS 33.210: "Network Domain Security (NDS); IP network layer security".

# 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].

**NR Femto:** A NR Femto is a Customer-premises equipment that connects a 3GPP UE over 5G NR wireless air interface to a mobile operator’s network using a broadband IP backhaul.

**NR Femto Gateway:** NR Femto Gateway is a mobile operator’s equipment (usually physically located on mobile operator premises) through which the NR Femto gets access to mobile operator’s core network.

**NR Femto subsystem**: A NR Femto subsystem consists of the NR Femto and NR Femto Gateway.

**Closed access mode:** NR Femto provides services only to its associated CAG members.

**CAG:** A Closed Access Group identifies a group of subscribers who are permitted to access one or more CAG cells associated to the CAG.

**CAG owner:** CAG owner is the individual who is authenticated and authorized by the 5GC to operate (add/delete/modify) on the allowed CAG list of the users for the associated NR Femto. For NR Femto, CAG owner is considered same as NR Femto Hosting Party.

**CSG**: Refer to TS 22.220 [3] for the definition of CSG.

**NR Femto hosting party**: Refer to TS 23.501 [2] clause 3.1 for definition of NR Femto hosting party.

**Security Gateway:** Element at the edge of an operator’s security domain terminating security association(s) for the backhaul link between NR Femto and network.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

CAG Closed Access Group

CSG Closed Subscriber Group

## 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 Overview of Security Architecture and Requirements

## 4.1 Security Architecture of NR Femto

In 5GS, an NR Femto node connects to 5GC directly via NG interface or optionally connects to 5GC via NR Femto Gateway (NR Femto GW) as specified in TS 38.300 [4] and in Annex V of TS 23.501 [2]. Additionally, other functions that will be used for security purpose are further depicted in Figure 4.1.1. Such security aspect enhancements to NR Femto are described in clause 5 of the present document.

UE

NR Femto

SeGW

Insecure link

Operator’s security domain(s)

NR Femto GW

NR Femto MS

NR Femto MS

AUSF / UDM

UPF

**Figure 4.1.1: System Architecture of NR Femto**

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

- The security requirements specified in TS 33.320 [5] shall be derived for NR Femto with the following modifications: H(e)NB replaced with NR Femto, H(e)MS replaced with NR Femto MS, optional L-GW replaced with the UPF, Iurh/X2 interface replaced with Xn interface. The extent to which TS 33.320 [5] shall be reused is captured as follows:

- Security architecture and assumption: Clause 4 in TS 33.320 [5] shall be reused. Text in TS 33.320 [5] clause 4.4, the security requirements are extended in clause 4 of this document.

- Security Features: Clause 5 in TS 33.320 [5] shall be reused. Text in TS 33.320 [5] clause 5.2, the device authentication is extended in clause 5.1 of this document. Text in TS 33.320 [5] clause 5.3, the Hosting Party authentication is extended in clause 5.2 of this document.

- Security Procedures in NR Femto: Clause 6 in TS 33.320 [5] shall be reused.

 - Security between NR Femto and SeGW: Clause 7 in TS 33.320 [5] shall be reused. Text in TS 33.320 [5] clause 7.2, the device authentication is extended in clause 5.1 of this document. Text in TS 33.320 [5] clause 7.3, the Hosting Party authentication is extended in clause 5.2 of this document. Text in TS 33.320 [5] clause 7.4, the IPSec tunnel establishment is extended in clause 5.4 of this document.

- Security aspects of NR Femto management: Clause 8 in TS 33.320 [5] shall be reused. Text in TS 33.320 [5] clause 8.1, the location verification mechanism is extended in clause 5.3 of this document. Text in TS 33.320 [5] clause 8.2, access control mechanism for NR Femto is extended in clause 5.5 of this document.

- Security aspects of emergency call handling: Clause 9 in TS 33.320 [5] shall be reused.

- Security aspects for mobility: Clause 10 in TS 33.320 [5] shall be reused.

- Security Procedures for direct interface between base stations: Clause 11 in TS 33.320 [5] shall be reused.

## 4.2 Reference points and functional entities

### 4.2.1 Functional entities

#### 4.2.1.1 General

This clause describes the functions that is used to perform security in Figure 4.1.1. Descriptions of the functions can further be found in TS 38.300 [4].

#### 4.2.1.2 NR Femto

An NR Femto is specified in TS 38.300 [4].

#### 4.2.1.3 Security Gateway (SeGW)

The SeGW is a network element at the border of a security domain of the operator. If a NR Femto GW is deployed, the SeGW is located in front of the NR Femto GW, else it is located at the edge of the 5GC. After successful mutual authentication between the NR Femto and the SeGW, the SeGW connects the NR Femto to the operator’s security domain. Any connection between the NR Femto and the NR Femto GW or core network is tunnelled through the SeGW.

#### 4.2.1.4 NR Femto Management System

The NR Femto Management System is a management server that configures the NR Femto according to the operator’s policy. NR Femto Management System is also capable of installing software updates on the NR Femto. The NR Femto Management System 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).

The NR Femto Management System is the same as HeMS or HMS that are captured in TS 32.593 [6].

#### 4.2.1.5 AUSF and UDM

UDM stores the subscription data and authentication information of the NR Femto. When hosting party authentication is required, AUSF authenticates the hosting party based on the authentication information retrieved from UDM.

### 4.2.2 Reference points

Interfaces or reference points in Figure 4.1.1 can be found in TS 38.300 [4].

# 5 Security For NR Femto

## 5.1 General

This clause describes the security procedures for NR Femto. The Architecture and requirement can be found in clause 4.

## 5.1 Device Authentication

The device authentication is mandatory for NR Femto.

Device mutual authentication between NR Femto and SeGW shall be performed using IKEv2 certificate-based authentication.

When IKEv2 certificate-based authentication is used for authentication between NR Femto and SeGW, the procedure in TS 33.320 [5] clause 7.2 shall be reused with the following modifications:

- Replace the H(e)NB with the NR Femto.

## 5.2 NR Femto Hosting Party Authentication

### 5.2.1 General

Device Authentication of the 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 [5] clause 5.3 and clause 7.3 can be derived with the following changes:

- Replace H(e)NB with NR Femto;

- Replace HSS with UDM;

- EAP-AKA'-based method can be used for NR Femto hosting party authentication exchange.

5FMTF can act as the proxy for NR Femto authentication. 5FMTF can be co-located with SeGW or an independent function deployed in the 5GC.

NR Femto hosting party can plays the role of CAG owner to operate (add/delete/modify) on the allowed CAG list of the users after authenticated and authorized by the 5GC. The security aspects of NEF specified in clause 12 of TS 33.501[7] can be reused when NR Femto hosting party operating on the allowed list in the UDM. Refer to clause 5.5 of the present document for relevant access control mechanisms.

### 5.2.2 Combined device and hosting Party authentication procedure

5FMTF can act as the proxy for NR Femto authentication. 5FMTF can be co-located with SeGW or an independent function deployed in the 5GC. The procedure between the NR Femto, SeGW and EAP authentication server is shown in Figure 5.2.2.1.



Figure 5.2.2.1: NR Femto hosting party authentication using EAP-AKA' authentication method

1. The NR Femto establishes connection between the NR Femto and the SeGW.

2. The SeGW sends an EAP Identity/Request to the NR Femto.

3. The 5G NR Femto sends an EAP Response/Identity message. The 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 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 NR Femto.

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

12. The 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.

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

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

## 5.3 Location Security

### 5.3.1 General

The NR Femto MS and/or NR Femto GW (referred to in this section as the “verifying node”) shall perform location verification. Optionally, the SeGW can act as the verifying node to perform the location verification for the NR Femto node. The location verification is performed during or after the device authentication process. If the location verification fails, the connection from the NR Femto node to 5GC should be blocked as early as possible.

One or more types of following location information of NR Femto may be optionally stored in the verifying node by operators for location verification and the location security aspects in TS 33.320 [5] clause 8.1 shall be reused:

- the public IP address of the broadband access device provided by the NR Femto;

- the IP address and/or access line location identifier provided by broadband access provider;

- information of the neighbouring cells surrounding the NR Femto;

- geo-coordinates provided by a GNSS receiver embedded into the NR Femto.

The following information may also be used to perform location verification of NR Femto:

- locations verification during the mutual authentication process by SeGW. Refer to clause 5.3.2 of the present document.

- locations of UEs connected to the NR Femto. Refer to clause 5.3.3 of the present document.

### 5.3.2 Location verification during the mutual authentication process by SeGW

When the SeGW acts as the verifying node, the mutual authentication between NR femto and SeGW may followed by location verification for the Femto node. If the mutual authentication is IKEv2 certificate-based, an example call flow of the location verification during the authentication process is performed as shown in Figure 5.3.2.1. As IKEv2 allows the inclusion of information data into Notify Payload, the location information of the NR Femto node may be carried in the Notify Payload (see Figure 5.3.2.1) during IKEv2 procedures from the NR Femto to the SeGW.



Figure 5.3.2.1: Location verification during the mutual authentication process by SeGW

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

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

1-3.The same as the steps 1-3 in TS 33.320 [5] clause A.1.

4. The same as the step 4 in TS 33.320 [5] clause A.1. Additionally, the NR Femto sends its location information in the Notify Payload with a Notification Type of LOCATION\_INFO in the IKE\_AUTH request. Notification Type of LOCATION\_INFO is defined and configured in both NR Femto and SeGW.

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

### 5.3.3 Locations of UEs connected to the 5G NR Femto

NR Femto cells are expected to provide coverage over a small geographical area. The location of UEs connected to the NR Femto cells can only be within small distances, and this can be used by the verifying nodes to verify the 5G NR Femto location.

## 5.4 Backhaul Link Protection

The backhaul link security aspects specified in TS 33.320 [5] clause 4.3.1, 4.4.5 and 7.4 shall be derived with the following change:

- Replace H(e)NB with NR Femto;

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

When NR Femto GW is needed, the protection of the interface between SeGW and NR Femto GW shall based on NDS/IP as specified in TS 33.210 [8]. The protection of the interface between NR Femto GW with other 5GC function shall reuses the protection for N2 or N3 as defined in TS 33.501 [7].

When NR Femto GW is not needed, the protection of the interface between SeGW and the function in 5GC shall be the same as N2 or N3 as defined in clause 9 in TS 33.501 [7].

## 5.5 Access Control Mechanisms for Femto

Clause 8.2.1 in TS 33.320 [5] shall be reused by replacing HNB with NR Femto.

The existing CAG concept defined for PNI-NPN in TS 23.501 [2] caluse 5.30.3 shall be re-used for Femto access control.

## 5.6 Topology Hiding

The core network topology shall not be directly exposed to the NR Femto.

The NR Femto GW may be deployed to allow the concentration of the NG-C and NG-U interface between the NR Femto and 5GC.

The SeGW shall hide the 5GC topology so that the core network identities (such as IP addresses of AMF, UPF etc.) are not inadvertently exposed to the NR Femto. If the NR Femto GW is not deployed, the SeGW shall allow the concentration of the NG interface.

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2025-02 | SA3#120 | S3-250540 |  |  |  | Skeleton of TS 33.545 | 0.0.0 |
| 2025-02 | SA3#120 | S3-250979 |  |  |  | Included changes from S3-250693, S3-250695, S3-250696, S3-250697, S3-250698, S3-250700, S3-250701, S3-250980, S3-250981, S3-250982, S3-250983, S3-250984, S3-250985, S3-250986, S3-250987, S3-250988 and S3-251135. | 0.1.0 |