ETSI TS 133 545 V19.3.0 (2026-02)

TECHNICAL SPECIFICATION

5G;
Security aspects of NR Femto
(3GPP TS 33.545 version 19.3.0 Release 19)

Reference
RTS/TSGS-0333545vj30

Keywords
5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
ETSI Search & Browse Standards application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on ETSI deliver repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2026.
All rights reserved.

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found at 3GPP to ETSI numbering cross-referencing.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

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].

CAG: The CAG is defined in TS 23.501 [2].

CAG owner: The CAG owner is defined in TS 23.501 [2].

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

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

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

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

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

Void

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].

5GC	5G Core
5GS	5G System
AAA	Authentication, Authorization, and Accounting
AKA	Authentication and Key Agreement
AUSF	Authentication Server Function
CAG	Closed Access Group
CSG	Closed Subscriber Group
eNB	Evolved Node-B
EAP	Extensible Authentication Protocol
H(e)NB	Home NodeB or Home eNodeB
H(e)MS	Home NodeB Management or Home eNodeB Management System
HeMS	Home eNodeB Management System
HeNB	Home eNodeB
HMS	Home NodeB Management System
HNB	Home NodeB
HP	Hosting Party
HPM	HP Module
HSS	Home Subscriber Server
IKE	Internet Key Exchange
L-GW	Local Gateway
MSK	Master Session Key
NR	New Radio
NRFAP	NR Femto Authentication Proxy
SeGW	Security Gateway
UDM	Unified Data Management

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.

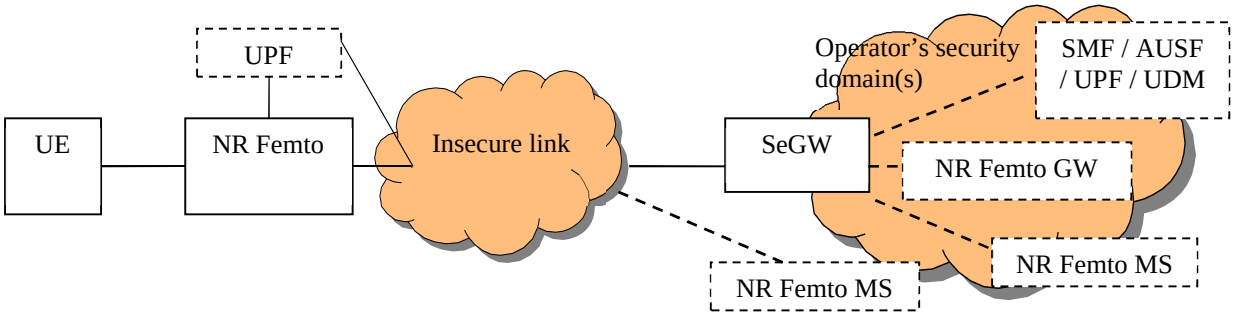

Figure 4.1.1: System Architecture of NR Femto

The architecture of clause 4.1 in TS 33.320 [5] shall be reused for NR Femto with the following modifications: H(e)NB is replaced with NR Femto, H(e)MS is replaced with NR Femto MS, H(e)NB GW is replaced with NR Femto GW and Iurh/X2 interface is replaced with Xn interface. Optional L-GW is not specified in the present document.

4.2 Reference points and functional entities

4.2.1 Functional entities

4.2.1.1 General

This clause describes the functions that are 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.

4.2.1.6 NR Femto Gateway

As mentioned in clause 5.50.2 of TS 23.501[2], NR Femto node can optionally connect to 5GC via NR Femto Gateway (NR Femto GW).

The NR Femto GW appears to the AMF as a gNB. The NR Femto GW appears to the gNB as an AMF. The NG interface between the NR Femto and the 5GC is the same, regardless whether the NR Femto is connected to the 5GC via a NR Femto GW or not.

4.2.1.7 Locally deployed UPF

Security between NR Femto and locally deployed UPF: Security requirements and procedures on N3, as specified in TS 33.501 [7] shall be followed to ensure security between NR Femto and locally deployed UPF.

- Locally deployed UPF shall securely communicate with SMF via SeGW in front of 5GC over N4 interface.
- Also, local UPF shall communicate with UPF in operator's 5GC via SeGW in front of 5GC using N9 interface.
- This locally deployed UPF is outside operator's network, and hence, as specified in clause 4.5 of TS 33.210[8], IPSec should be used to ensure the secure communications.

NOTE 1: Support for a co-located UPF similar to the L-GW described in TS 33.320 [5] is not covered in the present document.

4.2.2 Reference points

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

4.2.3 Security Requirements and Principles

The Security Requirements and Principles defined in clause 4.4 of TS 33.320[1] shall be reused with the following modifications: H(e)NB replaced with NR Femto, H(e)MS replaced with NR Femto MS, H(e)NB GW replaced with NR Femto GW, Iurh/X2 interface replaced with Xn interface. Optional L-GW is not specified in the present document.

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.

Clauses 5 to 11 from TS 33.320 [5] are reused in principle, by replacing H(e)NB with NR Femto, H(e)MS with NR Femto MS, H(e)NB GW with NR Femto GW, Iurh/X2 interface with Xn interface. The L-GW functionality is not specified in the present document. Moreover, some mechanisms need to be upgraded to acommodiate the 5G system which are captured in the following subclauses, i.e., from clause 5.1 to clause 5.8. Thus, the new mechanisms from clause 5.1 to clause 5.8 for NR Femto in the present document superseed the old ones captured in the TS 33.320 [5].

5.2 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.

5.3 NR Femto Hosting Party Authentication

5.3.1 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.

NR Femto Authentication Proxy (NRFAP) 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.

5.3.2 Combined device and hosting party authentication procedure

NRFAP can act as the proxy for NR Femto authentication. NRFAP 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.

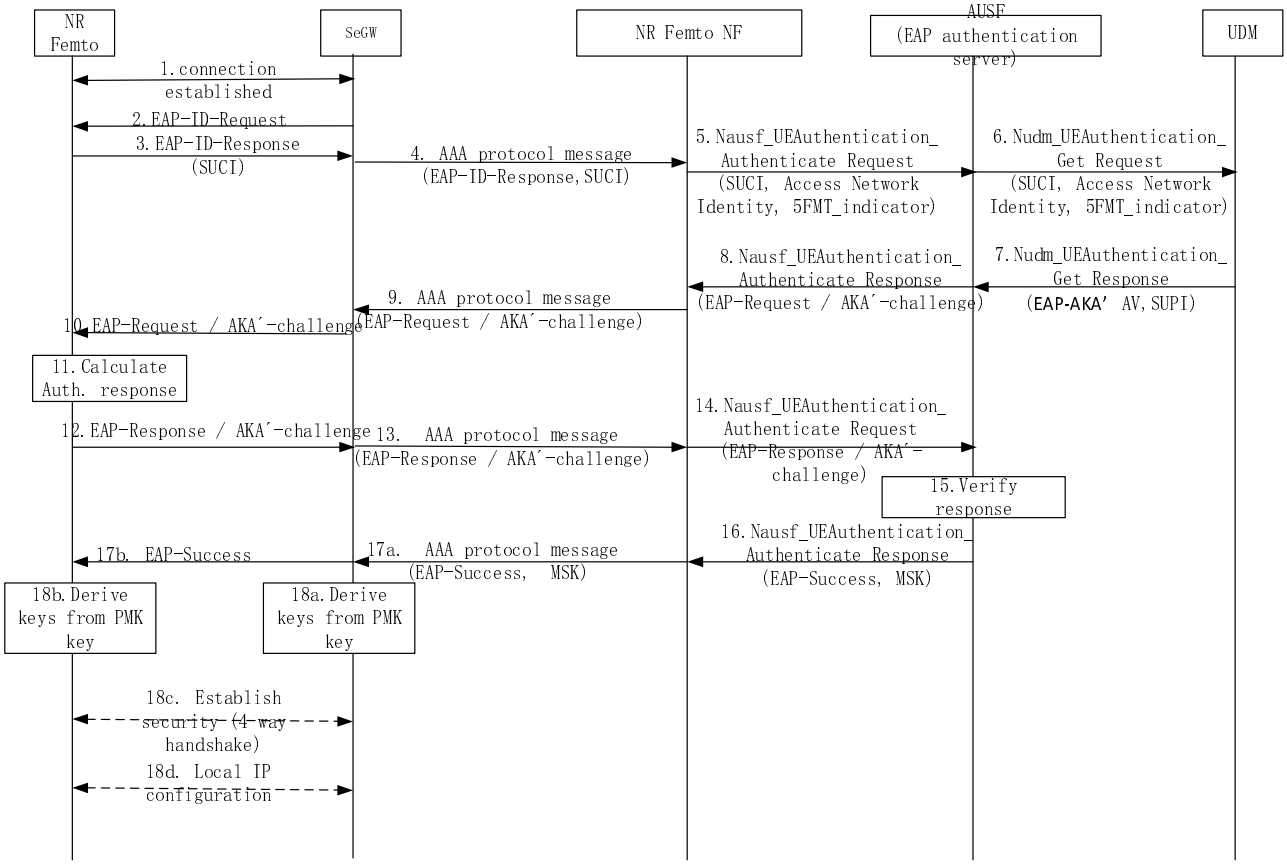

Figure 5.3.2.1: NR Femto hosting party authentication using EAP-AKA' authentication method

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 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 NRFAP based on the realm part of the SUCI.

5. The NRFAP sends the message Nausf_UEAuthentication_Authenticate Request with SUCI, Access Network Identity and NRFemto_indicator towards the AUSF. NRFemto_indicator is used to indicate to the AUSF that the authentication request is for NR Femto purposes. The NRFAP sets the Access Network Identity to "5G: NRFemto".

6. Based on the NRFemto_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 NRFemto_indicator.

7. Upon reception of the Nudm_UEAuthentication_Get Request, the UDM invokes SIDF. SIDF de-conceals SUCI to gain SUPI before UDM can process the request. Based on the NRFAP indicator and if NRFAP 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 NRFAP in a Nausf_UEAuthentication_Authenticate Response message.

9. The NRFAP 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 NR Femto authentication, the K_{AUSF} does not be generated by the 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 NRFAP sends 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 NRFAP. The AUSF derives the required MSK key from CK' and IK', based on the NRFAP_indicator received in step 5. The AUSF does not generate the K_{AUSF}.

16. The AUSF sends Nausf_UEAuthentication_Authenticate Response message with EAP-Success and MSK key to NRFAP. The AUSF may optionally provide the SUPI to NRFAP. The AUSF/UDM does not perform the linking increased home control to subsequent procedures.

17. The NRFAP 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.

5.4 Location Security

5.4.1 General

The NR Femto MS and/or NR Femto GW (referred to in this clause 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 5.4.2 of the present document.
- locations of UEs connected to the NR Femto. Refer to clause 5.4.3 of the present document.

5.4.2 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 5.4.2.1. 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 5.4.2.1) during IKEv2 procedures from the NR Femto to the SeGW.

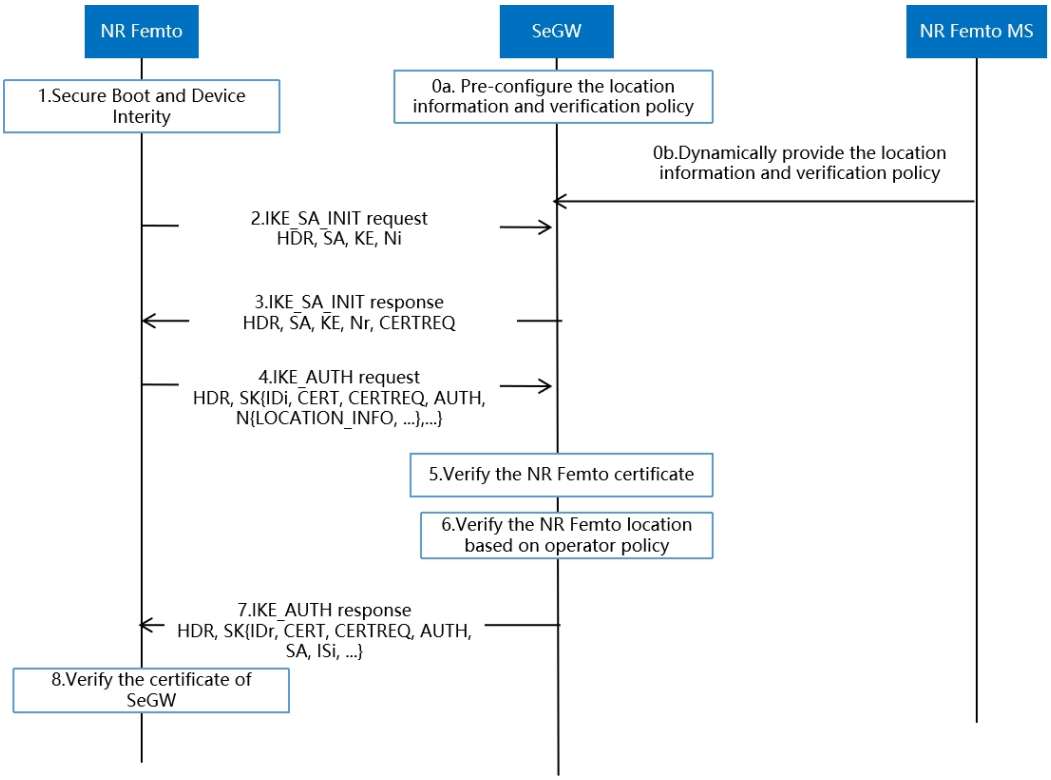

Figure 5.4.2.1: Location verification during the mutual authentication process by SeGW

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: 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.

5.4.3 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 NR Femto location.

5.5 Backhaul Link Protection

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

- 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].

5.6 Access Control Mechanisms for Femto

Clause 8.2.1 in TS 33.320 [5] shall be reused by replacing H(e)NB with NR Femto.

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

5.7 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 entity address information (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.

5.8 CAG ID verification

CAG ID is optional to be used as specified in TS 23.501[2], and when it is used, the NR Femto GW shall verify that all UE associated messages from a NR Femto cell can be mapped to a specific CAG ID and that this CAG ID is allowed for the identity of the originating NR Femto. In the absence of a NR Femto GW, the NR Femto shall include in NG-AP message an information that the message is originated from an NR Femto cell, and then the AMF shall perform this CAG ID verification whether the CAG ID is allowed to be used by the NR Femto cell.

One NR Femto can host multiple Femto cells. Cells may belong to PNI-NPN. Hence, the CAG ID verification shall be applied to all the CAG IDs mapping to individual Femto cells. The existing CAG concept defined for PNI-NPN in TS 23.501 [2] clause 5.30.3 shall be re-used for Femtocell access control.

NOTE 1: The CAG ID being verified may be explicitly present in the message as an information element or may be mapped by other means.

NOTE 2: The above requirement implies that the network has to ensure that all UE-associated messages from Femto cells are subject to the above verification, even if a (rogue) message from a compromised Femto would not indicate to originate from a NR Femto.

NOTE 3: It is left to implementation on how the AMF or Femto GW knows the CAG ID that the NR Femto cell can use.

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2025-02	SA#107	SP-250088				Presented for information and approval	1.0.0
2025-03	SA#107					Upgrade to change control version	19.0.0
2025-07	SA#108	SP-250665	0001	1	F	Update NR Femto Gateway Functionality	19.1.0
2025-07	SA#108	SP-250665	0002	1	F	Some terminology corrections in TS 33.545 clause 5.2.1 and 5.2.2	19.1.0
2025-07	SA#108	SP-250665	0003	1	F	Update local UPF related aspects of the specification to align with SA2	19.1.0
2025-07	SA#108	SP-250665	0006	1	F	New clauses on security requirement and principles	19.1.0
2025-07	SA#108	SP-250665	0008	-	F	Aligning terms in clause 3.1 to specifications	19.1.0
2025-07	SA#108	SP-250665	0011	-	F	Minor corrections to clause 5.2.2	19.1.0
2025-07	SA#108	SP-250665	0014	-	F	Topology hiding correction	19.1.0
2025-07	SA#108	SP-250665	0015	1	D	Editorial modification	19.1.0
2025-07	SA#108	SP-250665	0016	-	F	Term alignment	19.1.0
2025-07	SA#108	SP-250665	0017	1	F	Clarification to clause 4.1	19.1.0
2025-09	SA#109	SP-251006	0019	-	F	Update the description of the Femto architecture	19.2.0
2025-09	SA#109	SP-251006	0021	-	F	Figure 4.1.1 updates missing from CR S3-252011	19.2.0
2025-09	SA#109	SP-251006	0022	1	F	Changes based on RAN3 input	19.2.0
2025-09	SA#109	SP-251006	0023	-	F	Editorial change to clause 5.1	19.2.0
2026-01	SA#110	SP-251535	0024	1	F	Clarification on AMF knows the message from a NR Femto	19.3.0
2026-01	SA#110	SP-251535	0025	1	F	Clarification on CAG ID is option to use in NR Femto	19.3.0

History

Version	Date	Status
V19.2.0	January 2026	Publication
V19.3.0	February 2026	Publication