|  |
| --- |
| 3GPP TR 33.745 V0.1.0 (2024-04) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security aspects of 5G 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.© 2024, 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 5

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 8

3.3 Abbreviations 8

4 Security Architecture and Assumptions 8

5 Key issues 8

5.1 Key Issue #1: Security of 5G NR Femto Ownership 8

5.1.1 Key issue details 8

5.1.2 Security threats 9

5.1.3 Potential security requirements 9

5.2 Key issue #2: Authentication aspect of 5G NR Femto connecting to the operator network. 9

5.2.1 Key issue details 9

5.2.2 Threats 9

5.2.3 Potential security requirements 9

5.3 Key Issue #3: Support of 5G Femto location security 9

5.3.1 Key issue details 9

5.3.2 Security threats 10

5.3.3 Potential security requirements 10

5.4 Key Issue #4: UE access control 10

5.4.1 Key issue details 10

5.4.2 Security threats 10

5.4.3 Potential security requirements 10

5.5 Key Issue #5: Protection of backhaul link between 5G NR Femto and 5GC 10

5.5.1 Key issue details 10

5.5.2 Security threats 11

5.5.3 Potential security requirements 11

5.6 Key Issue #6: Hosting Party authentication 11

5.6.1 Key issue details 11

5.6.2 Security threats 11

5.6.3 Potential security requirements 11

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

5.X.1 Key issue details 11

5.X.2 Security threats 11

5.X.3 Potential security requirements 11

6 Solutions 11

6.0 Mapping of solutions to key issues 11

6.Y Solution #Y: <Solution Name> 12

6.Y.1 Introduction 12

6.Y.2 Solution details 12

6.Y.3 Evaluation 12

7 Conclusions 12

Annex <A> (informative): Gap Analysis w.r.t. TS 33.320 13

Annex <X> (informative): Change history 15

# 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 will investigate 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)".

# 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], 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 3GPP TR 21.905 [1].

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

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

## 3.2 Symbols

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

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

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]

# 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 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.

Editor’s Note: Based on SA2 outcome, the access control mechanism to support UE moving between CAG cell of 5G NR Femto and CSG cell is FFS.

### 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.

NOTE 1: This key issue is a placeholder and will not start until RAN3 defines the architecture.

### 5.5.2 Security threats

TBD.

### 5.5.3 Potential security requirements

TBD

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

### 5.X.1 Key issue details

### 5.X.2 Security threats

### 5.X.3 Potential security requirements

# 6 Solutions

Editor’s Note: This clause contains the proposed solutions addressing the identified key issues.

## 6.0 Mapping of solutions to key issues

Editor's Note: This clause contains a table mapping between key issues and solutions.

Table 6.0-1: Mapping of solutions to key issues

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions | KI#X | KI#Y | KI#Z |
|  |  |  |  |

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

### 6.Y.1 Introduction

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

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

# 7 Conclusions

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

Annex <A> (informative):
Gap Analysis w.r.t. TS 33.320

**Table A-1: Gap analysis table w.r.t TS 33.320 [2]**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Clause number in TS 33.320** | **Can be re-used with update of 5G terms** | **Can be re-used partially** | **Needs to be completely revised** | **Rationale and relevant KI** |
| 4.1 |   |   |   |   |
| 4.2 |   |   |   |   |
| 4.3 |   |   |   |   |
| 4.4 |   |   |   |   |
| 5.1 |   |   |   |   |
| 5.2 |   |   |   |   |
| 5.3 |   |   |   |   |
| 5.4 |   |   |   |   |
| 6.1 |   |   |   |   |
| 6.3 |   |   |   |   |
| 7.1 |   |   |   |   |
| 7.2 |   |   |   |   |
| 7.3 |   |   |   |   |
| 7.4 |   |   |   |   |
| 7.5 |   |   |   |   |
| 8.1 |   |   |   |   |
| 8.2 |   |   |   |   |
| 8.3 |   |   |   |   |
| 8.4 |   |   |   |   |
| 8.5 |   |   |   |   |
| 9 |   |   |   |   |
| 10.1 |   |   |   |   |
| 10.2 |   |   |   |   |
| 11.1 |   |   |   |   |
| 11.2 |   |   |   |   |
| Annex A |   |   |   |   |
| Annex B |   |   |   |   |

Editor’s Note: This annex contains a table and potential descriptions for gap analysis between security aspects of 5G NR Femto and TS 33.320, studying to what extent the clauses in TS 33.320 can be reused.

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-04 | SA3#115-adhoc-e | S3-241188 |  |  |  | Skeleton of TR 33.745 | 0.0.0 |
| 2024-04 | SA3#115-adhoc-e | S3-241599 |  |  |  | Included changes from S3-241235, S3-241242, S3-241576, S3-241626, S3-241643, S3-241644, S3-241645, S3-241646, S3-241647 and S3-241111\_r6. | 0.1.0 |