|  |  |
| --- | --- |
| 3GPP TR 33.xxx V0.1.0 (2025-08) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on Security Aspects for NR Femto Phase 2  (Release 20) | |
|  | |
|  |  |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  https://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 members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 6

4 Security Architecture and Assumptions 6

5 Key issues 7

5.1 Key Issue #1: Detection of misconfigured/compromised 5G NR Femto devices 7

5.1.1 Key issue details 7

5.1.2 Security threats 7

5.1.3 Potential security requirements 7

5.2 Key Issue #2: Security and privacy aspect for local access 7

5.2.1 Key issue details 7

5.2.2 Security threats 7

5.2.3 Potential security requirements 8

5.X Key Issue #X: <Key Issue Name> 8

5.X.1 Key issue details 8

5.X.2 Security threats 8

5.X.3 Potential security requirements 8

6 Solutions 8

6.1 Mapping of solutions to key issues 8

6.Y Solution #Y: <Solution Name> 8

6.Y.1 Introduction 8

6.Y.2 Solution details 8

6.Y.3 Evaluation 8

7 Conclusions 8

Annex <X> : Change history 9

# 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

Editor’s Note: This clause contains scope for the study.

The present document …

# 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 (5GS)".

[3] 3GPP TS 33.545: "Security aspects of NR Femto".

# 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] 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].

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

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

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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].

<ABBREVIATION> <Expansion>

# 4 Security Architecture and Assumptions

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

- Annex V in TS 23.501[2] captures the architecture for NR Femto. The architecture option of NR Femto with a local UPF is reused as the basis for this study.

- The security architectural and requirements captured in TS 33.545 [3] is reused as basis for this study.

# 5 Key issues

Editor’s Note: This clause contains all the key issues identified during the study.

## 5.1 Key Issue #1: Detection of misconfigured/compromised 5G NR Femto devices

### 5.1.1 Key issue details

NR Femto devices are deployed outside operator domain and considered to be in un-trusted environments. Un-detected misconfigured or compromised NR Femto devices can lead to disruptions in services to UEs. A misconfigured or compromised NR Femto device with valid credentials and subscription to serve the victim UE can pose various threats including authentication replay attacks, broadcasting CAG IDs that it is not authorized to serve, denial of service attacks, etc.. Besides, misconfigured or compromised NR Femto devices may report false security baseline information to the SeGW and pose potential security threats to the NR Femto MS and the core network.

Potential security enhancements to NR Femto security architecture to detect such misconfigured or compromised NR Femto devices are needed to ensure that UEs, the NR Femto MS and the core network do not become victims of such devices.

### 5.1.2 Security threats

A misconfigured or compromised NR Femto device with valid credentials and subscription to serve the victim UE can pose various threats including authentication replay attacks, broadcasting CAG IDs that it is not authorized to serve, denial of service attacks, etc.to the connected UEs.

A misconfigured or compromised NR Femto device with valid credentials and subscription to connect to the SeGW can pose various threats including abnormal traffics, abnormal signalling messages, denial of service attacks to the NR Femto MS and the core network.

### 5.1.3 Potential security requirements

The 5G system shall be able to detect misconfigured or compromised femto devices and eliminate associated risks, e.g. preventing the abnormal traffics/signalling threats.

## 5.2 Key Issue #2: Security and privacy aspect for local access

### 5.2.1 Key issue details

As defined in TS 23.501 [2] for NR Femto, if a local UPF is deployed close to the location of NR Femto node, the edge computing functionality shall be applied and the deployment options of NR Femto with a locally deployed UPF is also given the annex V. The security and privacy aspect for NR Femto and locally deployed UPF supporting edge computing was not discussed R19.

### 5.2.2 Security threats

The locally deployed UPF is located outside the operator’s security domain, if the 5GS core network topology is not hided towards locally deployed UPF, the core network topology and address information may be exposed outside the operator’s security domain.

### 5.2.3 Potential security requirements

The 5GS should support a mechanism to provide secure local access services for NR Femto.

The 5GS should support a mechanism to hide the 5GS core network topology from the locally deployed UPF.

## 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.

## 6.1 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 <X> :  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Change history | | | | | | | |
| Date | Meeting | TDoc | CR | Rev | Cat | Subject/Comment | New version |
| 2025-08 | SA3#123 | S3-252616 |  |  |  | TR skeleton. | 0.0.0 |
| 2025-08 | SA3#123 | S3-253007 |  |  |  | Incorporated changes from S3-253008, S3-253009 and S3-253010. | 0.1.0 |