**3GPP TSG-SA3 Meeting #123 S3-252882r1**

**Goteborg, Sweden, 25 – 29 August 2025** **(revision of xx-yyxxxx)**

**Source: China Mobile, CAICT, ZTE, CATT**

**Title: New WID on Security Assurance Specification (SCAS) for NR Femto**

**Document for: Approval**

**Agenda Item: 6.2**

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

Title: New WID on Security Assurance Specification (SCAS) for NR Femto

Acronym: SCAS\_NR\_Femto

Unique identifier: XXXXX

Potential target Release: Rel-20

# 1 Impacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes | X |  | X |  |  |
| No |  | X |  | X |  |
| Don't know |  |  |  |  | X |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
|  | Study  |
|  | Normative – Stage 1 |
|  | Normative – Stage 2 |
|  | Normative – Stage 3 |
| X | Normative – Other\* |

**\* Other = e.g. testing**

## 2.2 Parent Work Item

For a brand-new topic, use “N/A” in the table below. Otherwise indicate the parent Work Item.

|  |
| --- |
| Parent Work / Study Items  |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
| N/A | N/A | N/A | N/A |

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
| 950016 | Security Assurance Specification (SCAS) for 5G Rel-17 Features (SCAS\_5G\_ph2) | Baseline of Rel 18 |
| 870020  | Security Assurance Specification for 5G (eSCAS\_5G) | Baseline of Rel 17 |
| 790015 | Security Assurance Specification for 5G | Baseline of Rel 16 |

# 3 Justification

NR Femto are small, low-power base stations designed for homes, enterprises and dedicated networks to improve indoor mobile coverage. Unlike the regular macro base stations, the smaller size and user-proximate deployment of femtocells make them more vulnerable to physical access, which increases its security risks. So TS 33.545[1] defines several additional security mechanisms to enhance the protection. For example, the NR Femto includes an independent Hosting Party Module for supporting the host party to authenticate with the core network, the access control through the CAG to limit the threats posed by compromised femtocells to users, location verification mechanisms etc.

3GPP does have SCAS specifications for regular base stations including TS 33.216 [2] for 4G eNodeB and TS 33.511 [3] for 5G gNodeB. However, 3GPP does not have SCAS for NR Femto yet. There has already been some attacks to HeNB being reported by researchers due to various implementation and/or configuration issues by vendors. For example, based on a paper titled “*Small Cell, Big Risk: A Security Assessment of 4G LTE Femtocells in the Wild”* shared privately*, some HeNBs do not comply with some security requirements in TS 33.320, including, but are not limited to, do not use CAG, do not support UICC or trusted environment, do not use certificate for device authentication.* And the security specification of 5G NR Femto mostly inherits TS 33.320[4] for 4G HeNB. The lack of SCAS specification and no test cases specifically defined for NR Femto may caused that the specification is not complied to. For instance, TS 33.545 requires the use of a secure element(i.e.UICC) for storing femto node’s credentials that are used to authenticate itself to the network, the IPSec tunnell establishment between NR Femto and SeGW and the profiles for IKEv2 have additional and exceptional specifications, NR Femto shall not reveal the ID(SUPI/IMSI) of UEs to the Hosting Party of the NR Femto etc.

It is important to have a separate SCAS to address all possible security concerns for NR Femto. This work item proposes to identify and define security requirements to ensure the security of NR Femto. This SCAS for NR Femto shall also include functional and baseline security hardening (e.g.,vulnerability) requirements for security assurance.

[1] TS 33.545, “Security aspects of NR Femto”, Release 19

[2] TS 33.216, “Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class”, Release 19

[3] TS 33.511, “Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class”, Release 19

[4] TS 33.320, “Security of Home Node B (HNB) / Home evolved Node B (HeNB)”, Release 18

# 4 Objective

The objective is to develop the SCAS for the NR Femto network product class, with the aims to:

- WT1: Identify critical assets and threats of the NR Femto not already covered in TS 33.216 and TS 33.511

- WT2: Develop and/or adapt NR Femto specific security functional, hardening and basic vulnerability testing requirements and related test cases

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Work Task ID | TU Estimate(Study) | TU Estimate(Normative) | RAN Dependency(Yes/No/Maybe)  | Inter Work Tasks Dependency  |
| 1. | 0 | 0.5 TU | Yes |  |
| 2. | 0 | 1 TU | Yes |  |
|  |  |  |  |  |

Total TU estimates for the normative phase: 1.5 TUs

Total TU estimates: 1.5

# 5 Expected Output and Time scale

|  |
| --- |
| New specifications  |
| Type  | TS/TR number | Title | For info at TSG#  | For approval at TSG# | Rapporteur |
| TS | 33.xxx | Security Assurance Specification (SCAS) for NR Femto | TSG#111(Mar 2026) | TSG#112(Jun 2026) | NA |

|  |
| --- |
| Impacted existing TS/TR  |
| TS/TR No. | Description of change  | Target completion plenary# | Remarks |
| TR 33.926 | Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes | TSG#112(Jun 2026) |  |

# 6 Work item Rapporteur(s)

TBD

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

None

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| China Mobile |
| ZTE |
| CAICT |
| CATT |
|  |
|  |