**3GPP TSG-SA3 Meeting #123 S3-252971**

**Goteborg, Sweden, 25 – 29 August 2025** **(revision of S3-252971)**

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

**Title: New WID on 5G Security Assurance Specification (SCAS) for NR Femto Security Gateway (SeGW)**

**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 5G Security Assurance Specification (SCAS) for NR Femto Security Gateway (SeGW)

Acronym: SCAS\_Femto\_SeGW

Unique identifier: XXXXX

Potential target Release: Rel-20

# 1 Impacts

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

# 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

The security aspects of network products in 5G system is a major concern. To address the concerns, The 3GPP has established the SCAS specification for various components of a 5G network, including gNB, AMF, SMF, UDM, AUSF, NRF, NEF, SEPP and UPF, as well as newer components such as N3IWF, NWDAF, IPUPS, SCP.

Security Gateway (SeGW) is a security-related network function of 5G network responsible for separating the NR Femto security domain from the operator's security domain. It is located at the edge of the 5GC, and plays a key role in securing 5GC against the potential attacks from the NR Femto. As specified in TS 33.545 [1] and TS 38.300[2], the SeGW tunnells the NR Femto node and the 5G core network, optionally via the NR Femto GW depending on its deployment. The SeGW interacts with the NR Femto node, AMF and UPF etc. in 5GC, it may interact with NR Femto GW, HeMS and AAA server via various interfaces based on various protocols. Security concerns can be there for SeGW interacting with all these functions and entities. Also, due to the responsibility of authenticating the Hosting Party, topogy hiding of 5GC NFs, the security of the data stored at SeGW like the authentication data and the IP address of NFs in 5GC, and their access aspects need due consideration.

As SeGW interacts with a number of network functions/entities and uses different types of interfaces for communication, it is important to have a separate SCAS to address all possible security concerns for SMSF. This work item proposes to identify and define security requirements to ensure security of SeGW in different deployment scenarios. This SCAS for SeGW 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 38.300: "NR; NR and NG-RAN Overall Description", Release 19

# 4 Objective

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

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

- WT2: Develop and/or adapt SeGW-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 | No |  |
| 2. | 0 | 0.5 TU | No |  |

Total TU estimates for the normative phase: 1 TUs

Total TU estimates: 1

# 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 for NR Femto security gateway( SeGW) | 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 |
| CableLabs |
|  |