**3GPP TSG-SA3 Meeting #123 draft\_S3-252615-r1**

**Goteborg, Sweden, 25 – 29 August 2025**

**Source: ZTE, Nokia**

**Title: New SID on Security Aspect for NR Femto Phase 2**

**Document for: Approval**

**Agenda Item: 6.1.3**

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: Study on Security Aspect for NR Femto Phase 2

Acronym: FS\_NR\_Femto\_Sec\_Ph2

Unique identifier: TBD

Potential target Release: Rel-20

# 1 Impacts

{For Normative work, identify the anticipated impacts. For a Study, identify the scope of the study}

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

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
| X | Study |
|  | Normative – Stage 1 |
|  | Normative – Stage 2 |
|  | Normative – Stage 3 |
|  | 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) |
| 5G\_Femto-Sec | SA3 | 1060062 | Security aspects of 5G NR Femto |

### 2.3 Other related Work Items and dependencies

|  |  |  |
| --- | --- | --- |
| Other related Work /Study Items (if any) | | |
| Unique ID | Title | Nature of relationship |
| 1050125 | Additional topological enhancements for NR | Work Item on the overall RAN architecture and required functional and procedural impacts for supporting 5G Femto deployments |

**Dependency on non-3GPP (draft) specification:**

# 3 Justification

**Justification1:**

NR Femto devices are deployed outside operator domain and considered to be in un-trusted environments. As described in S3-243009, 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 core network.

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

**Justification2:**

As discussed in S3-244004 and S3-244098, according to RAN3 conclusions in TR 38.799, the NR Femto nodes reuse LADN and edge computing functionality to support access to local services. As per TS 23.548 clause 4.3 elaborates following connectivity models to enable Edge Computing:

- **Distributed Anchor Point**: For a PDU Session, the PSA UPF is in a local site, i.e. close to the UE location. The PSA UPF may be changed e.g. due to UE mobility and using SSC mode 2 or 3.

- **Session Breakout**: A PDU Session has a PSA UPF in a central site (C-PSA UPF) and one or more PSA UPF in the local site (L-PSA UPF). The C-PSA UPF provides the IP Anchor Point when UL Classifier is used. The Edge Computing application traffic is selectively diverted to the L-PSA UPF using UL Classifier or multi-homing Branching Point mechanisms. The L-PSA UPF may be changed due to e.g. UE mobility.

- **Multiple PDU Sessions**: Edge Computing applications use PDU Session(s) with a PSA UPF(s) in local site(s). The rest of applications use PDU Session(s) with PSA UPF(s) in the central site(s). Any PSA UPF may be changed due to e.g. UE mobility and using SSC mode 3 with multiple PDU Sessions.

For NR Femto scenario, the NR Femto nodes are deployed outside operator domain and considered to be in un-trusted environments. If the appropriate connectivity model(s) which ensure higher security and privacy is not selected for NR Femto, local access can lead to loss of confidentiality, integrity and/or availability. Thus, it is important for 5GS to secure the connection(s) for local access services for NR Femto, and ensure that the connectivity model(s) used for local access is(are) secure and do not leak privacy details.

Also, Local UPF tightly integrated with NR Femto, like L-GW for H(e)NB, but local UPF was not discussed in Rel-19 study for NR Femto. It is needed to study and specify the security aspects for local UPF.

# 4 Objective

The objective of this study work is to investigate and identify potential security and privacy enhancements to support NR Femto phase 2.

Specifically, the objectives include:

- WT1: Study the security requirements and potential solutions to enhance the security of NR Femto devices, to detect misconfigured or compromised NR Femto devices, and to eliminate the security impacts from misconfigured or compromised NR Femto devices.

- WT2: Study the security and privacy aspects of local access for NR Femto scenario.

- NOTE: This WT2 includes local access as specified in Annex V of TS 23.501. Also, security specifications for L-GW as defined in TS 33.320 can also be extended for NR Femto.

## TU estimates and dependencies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Work Task ID | TU Estimate  (Study) | TU Estimate  (Normative) | RAN/SA2 Dependency  (Yes/No/Maybe) | Inter Work Tasks Dependency |
| WT1 | 1 | 0.5 | No |  |
| WT2 | 1 | 0.5 | Maybe |  |

Total TU estimates for the study phase: 2

Total TU estimates for the normative phase: 1

Total TU estimates: 3

# 5 Expected Output and Time scale

***{If this WID covers both stage 2 and stage 3, clearly indicate the different completion dates.}***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| New specifications {One line per specification. Create/delete lines as needed} | | | | | |
| Type | TS/TR number | Title | For info  at TSG# | For approval at TSG# | Rapporteur |
| Internal TR | 33.XXX | Study on security aspect for NR Femto phase2 | SA#112  Jun 2026 | SA#112  Jun 2026 | TBD |
|  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} | | | |
| TS/TR No. | Description of change | Target completion plenary# | Remarks |
|  |  |  |  |
|  |  |  |  |

# 6 Work item Rapporteur(s)

TBD

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

RAN3 for architecture aspects of NR Femto.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| ZTE |
| Nokia |
| China Unicom |
| China Telecom |
| China Mobile |
| Huawei |
| CableLabs |