**TSG SA Meeting #102 SP-231720**

**December 11 – 15, 2023, Edinburgh, Scotland**

**Source: SA WG3**

**Title: New SID on security enhancement for mobility over non-3GPP access to avoid full primary authentication**

**Document for: Approval**

**Agenda Item: 6.1.3**

**3GPP TSG-SA3 Meeting #113 S3-235105**

**Chicago, US, 6 - 10 november 2023** **(revision of S3‑234563 )**

**Source: Nokia, Nokia Shanghai Bell, CableLabs, Charter Communications, Broadcom, Lenovo, Xiaomi, ChinaMobile, Google, ZTE, Apple Keysight Technologies, LGE,** **Rogers Communications, Philips International B.V., IIT Delhi, Intel Corporation (UK) Ltd,**

**Title: New SID on security enhancement for mobility over non-3GPP access to avoid full primary authentication**

**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: Security for mobility over non-3GPP access to avoid full primary authentication

Acronym: FS\_Non3GPPMob\_Sec

Unique identifier: 1020045

Potential target Release: Rel-19

# 1 Impacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  | X |  | X |  |
| No |  |  |  |  |  |
| Don't know | X |  | 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) |
| WWC-Ph2-Sec  | SA3 |  | Study on security enhancement for mobility over non-3GPP access |

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
|  |  | {optional free text}  |

# 3 Justification

The support of wireless and wireline access has been specified in TS 23.501/502/503 and in TS 23.316, and security aspects are defined in TS 33.501.

For non-3GPP access technologies, multiple options are defined in 3GPP:

* Trusted Non-3GPP access: UE connects to 5GC via TNGF.
* Untrusted Non-3GPP access: UE connects to 5GC via N3IWF.
* Trusted WLAN access: N5CW device connects to 5GC via TWIF.
* Wireline Access: RG and devices behind RG connect to 5GC via W-AGF.
* NSWO where UE can connect to a WLAN access network using its 5GS credentials via NSWOF without registering with 5GS to offload the traffic.

As per the current specification, mobility scenarios are not optimally addressed for Non-3GPP access. For example, when a UE or N5CW/AUN3 device disconnects from a non-3GPP access node and connects to a new non-3GPP access node, full primary authentication is performed even if 5GC has valid security context content. This leads to extra signalling between the device (UE or N5CW/AUN3) and 5GC that causes a delay in the device's connection to the network.

The following table summarizes the use cases where full authentication is performed even if 5GC has a security context and that leads to a delay in UE connection time:

|  |  |  |
| --- | --- | --- |
| Categories | Use case | Description |
| Cat-A: Mobility scenarios in trust and non-trust non-3GPP access related use cases. | **Use case A.1:** UE disconnecting from an N3IWF and connecting to a new or the same N3IWF. | When UE disconnects from an N3IWF and connects to a new or the same N3IWF, full primary authentication is performed even if AMF has a valid security context available. Please refer to TS 33.501, Section 7.2.1, for details. |
| **Use case A.2**: UE disconnecting from an TNGF and connecting to a new TNGF. | When UE disconnects from an TNGF and connects to a new TNGF, full primary authentication is performed even if AMF has a valid security context available. Please refer to TS 33.501, Section 7A.2.1, for details. |
| **Use case A.3**: UE disconnecting from an TNAP and connecting to a new TNAP within the same TNGF. | This use case was discussed and debated in the 5WWC Rel18 study; however, it was not concluded in Rel18. In this use case, when UE disconnects from an TNAP and connects to a new TNAP within the same TNGF, full primary authentication is performed. Please refer to TS 33.501 Section 7A.2.1 and TR 33.887 KI4 for details. |
| Cat-B: AUN3 device and N5CW device related use cases. | **Use case B.1**: AUN3 device disconnecting from 5G-RG/WAGF and connecting to a new 5G-RG/WAGF. | AUN3 devices are introduced in Rel18, where these devices are non-NAS-capable devices sitting behind RG. As per the current standards, when an AUN3 device disconnects from a 5G-RG/WAGF and connects to a new 5G-RG/WAGF, full primary authentication is performed even if AMF has a valid security context available. Please refer to TS 33.501, Section 7B.7, for details. |
| **(Sub) Use case B.2**: AUN3 device disconnecting from 5G-RG/WAGF and connecting to the same 5G-RG/WAGF. | When an AUN3 device disconnects from a 5G-RG/WAGF and connects to the same 5G-RG/WAGF, full primary authentication is performed even if AMF has a valid security context available. Please refer to TS 33.501, Section 7B.x, for details. |
| **Use case B.3**: AUN3 device disconnecting from 5G-RG and connecting to the same 5G-RG within the same WAGF. | When an AUN3 device disconnects from a 5G-RG and connects to a new 5G-RG under the same WAGF, full primary authentication is performed even if AMF has a valid security context available. Please refer to TS 33.501, Section 7B.7 for details. |
| **Use case B.4**: N5CW device disconnecting from TWIF and connecting to a new TWIF | As per the current standards, when a N5CW device disconnects from a TWIF and connects to a new TWIF, full primary authentication is performed even if AMF has a valid security context available. Please refer to TS 33.501, Section 7A.2.4, for details. |
| **(Sub)Use case B.5**: N5CW device disconnecting from TWIF and connecting to the **same** TWIF . | As per the current standards, when a N5CW device disconnects from TWIF and connects to the same TWIF, full primary authentication is performed even if AMF has a valid security context available. Please refer to TS 33.501, Section 7A.2.4.*Even if the AMF already has a security context identified by 5G-GUTI, the AMF shall initiate the primary authentication.* *NOTE 1: To avoid key stream reuse when deriving KTWIF from KAMF, the KAMF always needs to be refreshed by a renewed primary authentication.*This issue of N5CW that it does not support NAS and key generation needs to be aligned was found recently in the standards. So, this limitation was added in the TS because SA3 does not want to impact much on the maintenance release. However, it can be corrected in Release 19. |
| **Use case B.6**: N5CW device disconnecting from an WLAN AP and connecting to a new WLAN AP within the same TWIF. | As per the current standards, when a N5CW device disconnects from a WLAN AP and connects to a new WLAN AP within the TWIF, full primary authentication is performed even if AMF has a valid security context available. Please refer to TS 33.501, Section 7A.2.4, for details. |
| **Cat-C:** NSWO mobility use cases. | **Use case C.1**: UE disconnecting from WLAN access (authenticated by NSWO) and connecting to a new WLAN access/NSWO causing a full primary authentication. | NSWO allows a UE to connect to a WLAN access network using its 5GS credentials without registering to 5GS. Therefore, 5GC does not holds any context in this case. As per the current standards, when UE disconnects from WLAN access and connects to a new WLAN access sharing the same NSWO, the full primary authentication is performed by NSWOF. Please refer to TS 33.501, Section Annex S.3.2.  |

Note: Regarding use cases A.1,A.2, current procedures are not fully aligned. As discussed in the last meetings, this should be aligned via maintenance CRs, and study is not required for these use cases.

Use case #A.3, where UE disconnects from an TNAP and connects to a new TNAP within the same TNGF, has been studied in Release 18 but without conclusion. The other use cases have not been studied before. Therefore, it is important to study all use cases together to provide a seamless user experience across non-3GPP access.

# 4 Objective

Based on the above justification, the following objectives will be studied:

1. Study the security aspects and procedure enhancements needed to support UE connecting to a new target TNAP within the same TNGF without performing full primary authentication.).
2. Study the security aspects and procedure enhancements needed to support AUN3 connecting to a new target RG under the same WAGF without performing full primary authentication.
3. Study the security aspects and procedure enhancements needed to support N5CW devices connecting to a new target Trusted WLAN AP within the same TWIF without performing full primary authentication.
4. Study the security aspects and procedure enhancements needed to support UE connecting to a new WLAN AP that shares the same NSWOF without performing full primary authentication.

In all the above scenarios (except the 4th objective because NSWOF is stateless), the 5GC is already holding a valid UE security context, and the objective is to study the optimised mobility procedures to avoid full primary authentication and reduce latency.

This study does not have any architecture (SA2) level changes.

## TU estimates and dependencies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Work Task ID | TU Estimate(Study) | TU Estimate(Normative) | RAN Dependency(Yes/No/Maybe)  | Inter Work Tasks Dependency Editor’s Note: This column should highlight if WT#x is self-contained, or is dependent on completion of other WTs |
| 1. | .5 | .5 | Maybe | Self-contained |
| 2,3 | .5 | .5 | Maybe |  |
| 4. | .5 | .5 | No |  |

Total TU estimates for the study phase: 1.5 TUs (3 meeting cycles)

Total TU estimates for the normative phase: 1.5 TUs (3 meeting cycles)

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 | 33.702 | Study on security enhancement for mobility over non-3GPP access | SA#105Sep 2024 | SA#106Dec 2024 | Saurabh Khare |
|  |  |  |  |  |  |

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

# 6 Work item Rapporteur(s)

Saurabh.Khare@nokia.com

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

Stage 3 aspects covered by CT WGs

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Nokia |
| Nokia Shanghai Bell |
| Charter Communications |
| CableLabs |
| Lenovo |
| Broadcom |
| Xiaomi |
| ChinaMobile |
| Google |
| ZTE |
| Apple |
| Keysight Technologies |
| LGE |
| Rogers Communications |
| Philips International B.V. |
| IIT Delhi,  |
| Intel Corporation (UK) Ltd, |