**3GPP TSG-SA3 6G Workshop**

**Conference Calls, 6-7 August 2025**

**Source: China Mobile**

**Title: 6G Security Work Tasks Proposal**

# \*\*\*\*\*\*\*\*Proposed WTs for the 6G system Security SID\*\*\*\*\*\*\*

# 1 Justification

3GPP SA1 has started the FS\_6G\_REQ study item to identify use cases and service/operational requirements for 6G system. TSG RAN has initiated the FS\_6G\_RAN\_Scen\_Req study item to develop requirements for 6G Radio. 3GPP SA2 has also started the FS\_6G\_Arc study item to study the architecture of 6G system which also expects to see initial input from and interaction with SA3.

The following proposed working tasks aim to study security aspects of 6G system for improvement of existing system and support of new services and architecture, to meet the 6G system requirements as already defined by SA1, SA2 and RAN groups.

# 2 Work Tasks

**WT#1**: **Access Security**, including access authentication, AS security and NAS security in 6G system.

Access authentication aspects include procedures which determines the entities and protocols required for authentication procedure in the 6G system. Specifically, according to 5G leftover, whether enhancement is needed to the existing authentication protocols, entities and their functionalities are to be determined. Also, based on SA1 study, new forms of digital representations of users (like AI agent) should be considered to ensure the authentic access to the 6G network.

AS security design includes considerations of lower layer protections and so on.

NAS security takes into account of potential new NAS mechanisms from SA2.

**WT#2: Network Security**, including security mechanisms to support the core network architecture and procedures from SA2, as well as interworking security including key handling and security negotiation for interworking procedures.

**WT#3: Service Exposure Security**, including security mechanisms to support the exposure framework or requirements developed by SA2, SA6, etc.

**WT#4: AI Security:** Security for AI framework and potential AI agent communication.

**WT#5: Data Security and Privacy:** Security mechanisms for data framework considering privacy requirements.

# \*\*\*\*\*\*\*\*\*\*\*\*\*\*Proposed WTs for an independent SID\*\*\*\*\*\*\*\*\*\*

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 study on New study on inter-PLMN and intra-PLMN security in 6G

Acronym:FS\_6G\_PLMNSec

{Propose an acronym. Final acronym to be confirmed at the plenary. The sign "-" is a level separator between (Feature)-(Building Block)-(Work Task). The sign "\_" can be freely used. Studies have to start by "FS\_". Each acronym level has to be simple and short, 7 characters max recommended}

Unique identifier:

{A number to be provided by MCC at the plenary}

Potential target Release: Rel-20

# 1 Impacts

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

# 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

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |
| N/A |  | {optional free text} |

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

N/A

# 3 Justification

In TR 22.870, the security issues of operators struggling with the bilateral administration of security to enable interconnection and roaming with other operators has been studied. Similar issues also exist in intra-PLMN cases where different security domains in the core network rely on NDS/IP and NDS/AF to provide transport layer security protection mechanisms. In both inter-PLMN and intra-PLMN interconnections, digital certificates are usually used as identity identifiers and IPSec protocol is used for securing the communication between the two domains. This requires both CA (Certificate Authorities) institutions of each operator/entity at the border of the security domains to crossly trust and certify each other. Frequent cross-domain certification brings about network latency and management cost, as well as threats of single point of security failure. What’s more, it is difficult to establish a common root of trust for cross domain communication.

Thus, an efficient manner of establishing trust among inter-PLMN and intra-PLMN in 6G needs to be studied. For example, the traditional centralized trust infrastructure could be replaced with a decentralized trust foundation within and across the trust regions. With that, the 6G core network would fundamentally eliminate single points of security failure and reduce the cross-domain security management burden in security certification establishment.

The current NF to NF authentication mechanism operates at the transport layer, specifically within the TLS handshake. In contrast, authorization, utilizing OAuth2, is implemented at the application layer. By that, a significant challenge arises from the varying deployment scenarios where the termination point of authentication often differs from the actual NF's operational location. Therefore, it is crucial to investigate the feasibility and security implications of transport-agnostic authentication mechanisms. This involves relocating NF-NF authentication to the application layer, thereby aligning it with the existing OAuth2 authorization framework.

Furthermore, as the number and the type of the intra-PLMN networks is increasing, such as NPN-PLMN and PNI-NPN. Security isolation of these intra-PLMN networks is crucial to avoid cross-attack risks. Fine-grained security isolation based on the security needs of different businesses requirements is needed. Thereby, the security isolation mechanisms in 6G between different security domains in inter-PLMN and intra-PLMN needs to be studied.

# 4 Objective

The objective of this study item is to:

* WT1: Study the trust establishment mechanisms to eliminate single-point-failure, cross-domain security management burden and transport-level authentication dependencies.
  + For inter-PLMN case, study the efficient authentication mechanisms and security protection between operators.
  + For intra-PLMN case, study the authentication and security protection mechanisms among network elements in the same or different security domains.
  + Study the feasibility and potential security implications of moving NF-NF authentication to the application layer.
* WT2: Study the security isolation mechanisms between different security domains in inter-PLMN and intra-PLMN cases.

NOTE：The GSMA and/or other industry organizations may undertake similar topics in similar timeframes. However, 3GPP is responsible for achieving the objectives of this study. Potential liaison communications might be triggered during the study.

# 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 inter-PLMN and intra-PLMN security/security domains in 6G | Sep 2026  TSG#117 | Dec 2026  TSG#118 | 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

None.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| China Mobile |
| Johns Hopkins University |
| Deutsche Telekom |
| AT&T |
| Boost Mobile Network |
| Verizon |
| Vodafone |
|  |