**3GPP TSG-SA3 Meeting #123 S3-25xxxx**

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

**Source: vivo**

**Title: Study on Security for 6G System**

**Document for: Approval**

**Agenda Item:**

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 for 6G System

{Free text. It has to be the same as in the "Title:" section above. Studies have to start by "Study on"}

Acronym: FS\_6G\_SEC

Unique identifier:

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 | x | x |  |
| No |  |  |  |  |  |
| Don't know |  |  |  |  | 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

|  |
| --- |
| 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 |
| 1050110 | Study on 6G Use Cases and Service Requirements; Stage 1 | May need SA3 check/alignment with Stage-1 SA3-related requirements |
| 1080057 | Study on Architecture for 6G System; Stage 2 | The architecture design from SA2 may need to be taken into account  |
| 1060079 | Study on 6G Scenarios and Requirements | The architecture related requirements from RAN may need to be taken into account. |
| ? | Study on 6G Radio | The RAN design from RAN may need to be taken into account |

# 3 Justification

The security enhancements introduced with 5G marked a significant advancement in basic security features compared to previous generations. Notable improvements include unified authentication (introducing AUSF for both 3GPP and N3GPP authentication), on-demand UP security (introducing UP integrity), enhanced roaming security (i.e. N32 security), and encryption of the subscriber's permanent identity. Additionally, 5G security also builds security of 5G new features across SA2, SA6 and RAN, addressing features such as CIoT security, URLLC security, CAPIF security, and IAB security.

The 3GPP SA1 has launched the FS\_6G\_REQ study item to identify use cases and requirements for the 6G system, while SA2 has initiated the FS\_6G\_ARC study to explore architectural aspects of 6G networks. The TSG RAN is also engaged in the FS\_6G\_RAN\_Scen\_Req study item for developing 6G radio requirements and the FS\_6G\_RAN study for advancing 6G radio access technology. Both SA2 and RAN are focused on creating a more efficient, sustainable, and innovative 6G network through system simplification and the integration of new technologies. They are also exploring connectivity services and beyond connectivity services.

Throughout the evolution of 5G, various security issues related to basic security features have been discussed yet remain unresolved, e.g. authentication relay attacks, insufficient protection for SI, paging and MAC CE, coarse UP security policy, etc. This indicates room for further improvement in the basic security features for 6G networks.

Thus, this study aims to identify critical security issues in 6G networks, investigating security solutions with respect to security, performance and complexity.

The 6G security encompasses two main aspects: basic security features and security for new features. These will be founded on the requirements, architecture, and designs outlined in the aforementioned study items of SA1, SA2, RAN and potentially SA6. Basic security features will concentrate on enhancing security within the basic architecture and services, while security for new features will focus on safeguarding new features developed by other groups, such as AI, ISAC, etc.

By building on the advancements of 5G and incorporating learnings across various study domains, 6G security aims to create a comprehensive security framework that supports both basic security features and the security of new features. This approach will build the way for a secure, simple, efficient, and extensible security architecture, fostering confidence of security for 6G network.

# 4 Objective

This study aims to define security for 6G mobile networks, aligning with the 6G system requirements and designs as defined by 3GPP SA1, SA2, SA6, and TSG RAN.

SA3 aims to explore security threats, requirements and solutions to enhance the security for 6G network with acceptable performance/complexity trade-off.

The study contains multiple work tasks, with WT#1 to WT#5 addressing basic security features (including basic architecture security and basic service security) and WT#6 to WT#9 focusing on security for new features (including AI, ISAC, data framework and computing). Certain work task objectives, such as authentication, MAC CE protection, are security-driven and may impact architecture and procedures, thereby prioritizing initial investigation by SA3. Other objectives are impacted by architecture and procedures, requiring SA3 to wait for other groups’ progress.

The objectives of these work tasks may be revised based on SA2, SA6 and RAN progress, and the WT numbering does not imply priority.

This study includes the following high level work tasks:

**WT#1**: To guarantee secure and efficient access for UE (including IoT UE) to 6G network (including TN and NTN), study of authentication and ID privacy is essential, including:

1.1 Whether and how to support and/or enhance 5G authentication method in the 6G network, such as primary authentication, secondary authentication, N3GPP authentication, etc.

1.2 Whether and how to support new authentication methods if existing authentication methods are not enough.

1.3 Whether and how to support and/or enhance 5G subscriber privacy in 6G network.

**WT#2**: To protect communication between UE (including IoT UE) and 6G network (including TN and NTN), study of NAS security, AS security and UP security is essential, including:

2.1 How to support NAS security, e.g. security for module NAS.

2.2 How to support AS security, e.g. protection on SI, paging, MAC CE.

2.3 How to support UP security, e.g. UP security policy.

2.4 How to support mobility security.

2.5 How to support migration and interworking security.

NOTE 1: Coordination is required to resolve any potential conflicts between WT#2 and AEAD SID.

**WT#3**: To protect communication within RAN and CN in 6G network (including TN and NTN), study of NDS/IP and SBA security is essential, including

3.1 Whether and how to support and/or enhance 5G NDS/IP security in 6G network.

3.2 Whether and how to support and/or enhance 5G SBA security in 6G network.

NOTE 2: Coordination is required to resolve any potential conflicts between WT#1.3, WT#3 and PQC SID.

NOTE 3: When developing security solutions for WT#1, 2 and 3, SA3 should consider the IoT design principles (i.e. scalability and forward compatibility) established by SA2 and RAN, as well as the NTN design principle (i.e. uniformity).

**WT#4**: To protect communication between 6G network and external network, study of exposure security is essential, including how to support security for exposure framework.

**WT#5**: To protect essential/regulatory services provided by 6G network, study of essential/regulatory service security is essential, including whether and how to support and/or enhance security for essential/regulatory services, such as voice, SMS, emergency, MCS, LCS, SoR/UPU, etc..

NOTE 4: Considering SA2 separates IMS from the SA2 SID, the security for IMS can be divided into an independent SID.

**WT#6**: Study how to support security of AI in 6G, e.g. AI for network, network for AI (e.g. AI agent).

**WT#7:** Study how to support security of the integration of Sensing and Communication over 3GPP access.

**WT#8:** Study how to support security and privacy of data in data framework, , e.g. user consent, access control.

**WT#9:** Study how to support security of computing in 6G.

NOTE 5: WT#6 to WT#9 address security for new features and may potentially conflict with the basic security features outlined in WT#1 to WT#5. Coordination is required to resolve any conflicts that arise.

NOTE 6: WT#1, WT#2.2, and WT#2.3 can proceed independently because they are security-driven, and other group will be aligned with SA3. In contrast, the advancement of other work tasks relies on progress of other groups.

The conclusions of this study will form the basis for the normative work and/or for any further study.

During the study, the progress and results of 3GPP TR 22.870(SA1 study), TR 38.914(RAN study), TR 23.801-01(SA2 study) shall be taken into account.

A single TR is expected to capture the output of this study.

# 5 Expected Output and Time scale

|  |
| --- |
| 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 |
| TR |  | Study on Security for 6G System | TSG#114(Dec2026) | TSG#xx(TBD) |  |

NOTE: The timeline for the study will be decided at SA#111 (March 2025)

# 6 Work item Rapporteur(s)

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

Potential RAN impact to be covered by RAN WGs.

Potential architecture impact to be covered by SA2.

Potential application enabler related aspects to be covered by SA6

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| vivo |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |