**TSG SA Meeting #109 SP-251132**

**16 - 19 September, 2025, Beijing, China**

**Source: Orange, CMCC, Vodafone, 6G SID moderator (Nokia), China Unicom, OPPO, Vivo, Ericsson, Deutsche Telekom, Samsung, Thales, Idemia**

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

**Document for: Approval**

**Agenda Item: 6.7**

3GPP™ Study Item Description

Title: Study on Security for the 6G System

Acronym: FS\_6G\_SEC

Unique identifier: 1090044

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 …

{Tick one or more box(es). The full structure of all existing Work Items is shown in the 3GPP Work Plan in <https://ftp.3gpp.org/Information/WORK_PLAN>}

|  |  |
| --- | --- |
| 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) |
| FS\_6G\_REQ | SA WG1 | 1050110 | Study on 6G Use Cases and Service Requirements; Stage 1 |
|  |  |  |  |

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
|  |  |  |
| 1060079 | Study on 6G Scenarios and Requirements | The architecture related requirements from RAN may need to be taken into account. |
| 1080057 | Study on Architecture for 6G System | 6G system architecture from SA2 need to be taken in to account for 6G security study. |
|  |  |  |

# 3 Justification

Technology is developing at a fast pace bringing new spectrum and RF features, chipset capabilities, compute and storage platforms contributing to new architectural features on the network side. The ever evolving communication needs of the human beings continue drive the development of new device types and new features. Security and privacy being the cornerstone of communications, 3GPP SA3 has the primary responsibility to address this challenge effectively. 6G security study in SA3 is expected to address the privacy and security challenges comprehensively brought out by the technology advancements and the architecture and feature enhancements of 6G. In the next generation of communication technology such as 6G networks, the level of security needs to be at a much higher level from the day1.

To define the SA3 6G study, different inputs need to be considered, SA1 6G specifications on the Use cases and broad security requirements, the 6G architecture study in SA2 study and the 6G RAN study.

In addition to these use cases and requirements, there are independent security topics at different layers of the network as well as from the evolving technology developments like Quantum computer threats, new quantum safe algorithms and protocols, cloud and virtualization of RAN and core network functions, widespread adoption of AI/ML etc.

RAN WGs approved (RP-251881) SID for 6G anticipating enhancements to Radio interface protocol architecture and procedures for 6G Radio.

The SA2 approved study item SP-250806 [1] FS\_6G\_ARC outlines key architectural work tasks for 6G, many of which have direct security implications that SA3 should address in parallel such as:

* SA2 will define overall 6G architecture based on which SA3 must analyze and decide/conclude on authentication (protocols & methods) and secure communication in alignment with 6G’s UE-Core Network interaction mechanisms.
* Security impacts of 6G control signaling mechanism (e.g., new non-access stratum functionalities, generic framework for UE-Core Network interaction to support operator services, etc.), if any.
* Key areas of focus include security aspects for transfer or derivation of security context for interworking with pre-6G systems, and security assessments to architecture enhancements: SBA, network slicing, network sharing, QoS framework, user plane architecture, network exposure framework, Non-3GPP access, policy framework.
* Additionally, Sensing, NTN, AI driven security, data framework, user privacy and exposure risks need security evaluation.

Considering all the aspects, specific Work Task to clearly identify the study in each security domain are listed below. During the study key issues are expected to define the study of the topics of interest further.

From the first release of 6G, 6G security needs to consider cyberattacks and malicious abuse.

# 4 Objective

This study aims to define a security and privacy architecture and procedures for 6G mobile networks for improvement of existing services and support of new services, to meet the 6G system requirements as defined by 3GPP SA1 and TSG RAN for the system architecture defined by 3GPP SA2.

The study will work towards goals endorsed at TSG#107(Mar 2025) to "create lean and streamlined standards for 6G, e.g. by dimensioning an appropriate set of functionalities, minimizing the adoption of multiple options for the same functionality, avoiding excessive configurations, etc. Any exception to the above shall be well justified."

The study includes the following high level work tasks:

WT#1: Study security and privacy aspects for overall 6G system architecture (ref: SP-250806).

NOTE1: The above WT contains security aspects that do not fit into any other tasks, e.g. security aspects that affect both the RAN and Core Network, enhancements to the security architecture and security aspects related to work from other groups.

WT#2: Study security and privacy aspects of 6G RAN architecture (including all UE – RAN interactions and ref: RP-251881).

WT#3 : Study security and privacy aspects of 6G UE to core network interactions.

WT#4: Study enhancements to Core Network security including endpoint security at transport and application layers, internal and external interfaces as well as end to end roaming security taking roaming intermediary into account.

NOTE2: For roaming, coordination with GSMA is required.

NOTE3: In the above WTs, the study will cover possible security enhancements of the procedures from previous generations and new security aspects that arise from work in other working groups (including the developments regarding different particular verticals and deployments).

NOTE4: SA3 will have checkpoint with RAN groups on AS security by June 2026.

**TU estimates and dependencies**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Work Task ID | TU Estimate(Study) | TU Estimate(Normative) | RAN Dependency(Yes/No/Maybe)  | Inter Work Tasks Dependency  |
| WT#1, WT#2, WT#3, WT#4 | 50 |  | WT#1 - #3: Yes, WT#4: No  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# 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 |
| Internal TR | TR 33.801-01 | Study on Security for the 6G System  | TSG#114(Dec 2026) | TSG#116(June, 2027) | Suresh Nair (Nokia) |
|  |  |  |  |  |  |

|  |
| --- |
| 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)

Primary Rapporteur: Todor Gamishev (Orange)

Secondary Rapporteur : Suresh Nair (Nokia)

# 7 Work item leadership

SA WG3

# 8 Aspects that involve other WGs

Potential RAN impact to be covered by RAN WGs.

Potential architecture impact to be covered by SA2.

Potential multimedia and codecs aspects to be covered by SA4.

Potential charging and OAM impact to be covered by SA5.

Potential application enabler related aspects to be covered by SA6

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Apple  |
| AT&T |
| BMWE |
| BSI  |
| Cable Labs |
| CATT  |
| Charter |
| China Mobile |
| China Telecommunication Corporation  |
| China Unicom |
|  |
| Deutsche Telekom |
| Ericsson |
|  |
| Huawei  |
| Idemia  |
| IIT Bombay |
| Interdigital  |
|  |
| Lenovo |
| LG Electronics  |
|  |
| NEC |
| NIST |
| Nokia |
| Nokia Shanghai Bell |
| NTT DoCoMo  |
| OPPO |
| Orange |
| Philips International B.V  |
| Qualcomm  |
| Samsung |
| SK Telecom  |
| Telecom Italia  |
| Thales |
| TMobile USA  |
|  |
| Verizon  |
| Vivo |
| Vodafone |
| Xiaomi  |
| ZTE |