**3GPP TSG-SA3 Meeting #123 S3-252576**

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

**Source: 6G SID moderator**

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

**Document for: Agreement**

**Agenda Item: 6.3**

3GPP™ Study Item Description

Title: Study on Security for the 6G System

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 …

{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 |  |  |
|  |  |  |  |

### 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 | *6G use cases and service requirements from SA1 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. |
| 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 ad 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.

Considering all the aspects, specific Work Taks 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.

# 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 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 includes 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, policy framework.
* Additionally, AI driven security, data framework, user privacy and exposure risks need security evaluation.

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

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 shall investigate the security and privacy requirements, assumptions and high level principles for 6G architecture.

All work tasks aim at supporting multi-vendor interoperable interfaces.

The study includes the following high level work tasks, and the conclusion will consolidate the 6G security specifications among all work tasks:

6G RAN Architecture Security:

WT#1: Study security and privacy aspects of 6G RAN architecture and features. .

Overall 6G security architecture:

WT#2: Study security and privacy aspects for overall 6G system architecture including security domains, threat and risk analysis, security requirements, general design principles ensuring alignment with SA2/SA4/SA5/SA6 WGs security references.

UE to Network Security:

WT#3: Study security aspects of 6G network access, primary authentication including known gaps in current authentication mechanisms.

Core Network Security:

WT#4: Study enhancements to CN SBA security including endpoint security at transport and application layers, and study end to end roaming security taking roaming intermediatory into account.

**TU estimates and dependencies**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Work Task ID | TU Estimate  (Study) | TU Estimate  (Normative) | RAN Dependency  (Yes/No/Maybe) | Inter Work Tasks Dependency |
|  | 50 |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# 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 |
| {Possible values:  "TS" or  "Internal TR" or  "External TR". See Note 1} | {e.g.  "22.XXX" or actual number if known} | {Title of the specification (as per TR 21.801 §6.1.1), to be aligned as much as possible with the WI/SI title} | {e.g.  "TSG#87"} | {e.g.  "TSG#89"} | {<FamilyName>, <GivenName>, <Company>, <email address>. See Note 2} |
|  |  |  |  |  |  |

{Note 1: Only TSs may contain normative provisions. Study Items shall create or impact only TRs.  
"Internal TR" is intended for 3GPP internal use only whereas "External TR" may be transposed by OPs.}

{Note 2: The first listed Rapporteur is the specification primary Rapporteur. Secondary Rapporteur(s) are possible for particular aspect(s) of the TS/TR. In this case, their responsibility has to be provided as "Remarks".}

|  |  |  |  |
| --- | --- | --- | --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} | | | |
| TS/TR No. | Description of change | Target completion plenary# | Remarks |
| {e.g. "22.281"} | {Possible values:  - either free text (e.g. “CS aspects to be removed")  - or “Specification to be withdrawn”} | {e.g. "TSG#89"} | {Free text, e.g. "This TS covers Stage 2" or "This TS covers Stage 3" or "This TS covers both stages 2 and 3"} |
|  |  |  |  |

# 6 Work item Rapporteur(s)

{Mandatory: <FamilyName>, <GivenName>, <Company>, <email address>}

{Optional: <FamilyName>, <GivenName>, <Company>, <email address>: Secondary task(s)}

# 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 |
| CATT |
| China Mobile |
| Cisco |
| Deutsche Telekom |
| Ericsson |
| ETRI |
| Huawei |
| John Hopkins University |
| Lenovo |
| MITRE |
| Nokia |
| NTT DoCoMo |
| OPPO |
| Qualcomm |
| Samsung |
| Thales |
| TMobile USA |
| Uangel |
| Verizon |
| Vivo |
| ZTE |