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

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

**Source: 6G SID moderator**

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

**Document for: Approval**

**Agenda Item: xxx**

3GPP™ Study Item Description

Title: Study on Security for the 6G System Enhancements

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

# 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 than the existing 5G 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 from the existing gaps 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. During the study key issues are expected to further define the topic

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

The study of security and privacy should consider at least the following aspects: cloud native, sustainability and energy efficiency, robustness and resiliency, etc.

The study contains multiple work tasks. The scope of these work tasks and potential key issues derived from these work tasks may be refined during SA3#123-#126 before solutions for a given key issue can be studied. Some work task(s) might not result in key issue(s). WT numbering does not imply any priority order.

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:

( Disclaimer: For the preparation of the 6G Security SID, a list of Work Tasks has been consolidated from the different company contributions as below. Since the format, groupings are different in many company contributions, proposals with similar theme have been grouped together.

The aim is to first agree on the WT topic (1st column) then the description of the WT (2nd column). In the final SID table will be converted to text and source company names will be deleted.)

|  |  |  |
| --- | --- | --- |
| **WT Topic** | **Summary of the WT proposal** | **Source companies for the WT (similar proposals are grouped)** |
| #1 RAN related generic security WT | Study security and privacy aspects of 6G RAN architecture. Investigate on threats to signaling information in radio lower layer (e.g. MAC layer) and define a security mechanism for vulnerable lower layer signaling traffic (MAC CEs, LTM commands etc) to mitigate the identified threats. | Samsung, Vivo, LG, Xiaomi, Nokia |
| #2 Radio Lower layer protection | Study security and privacy aspects of radio lower layers including protection of MAC/MAC-CE, SIBs to avoid FBS attacks. | China Mobile, SKT, Samsung, Vivo, LG, CATT, Xiaomi, OPPO, Nokia, IDCC |
| #3 Msg 3/5 protection | Study security for messages exchanged prior to AS Security Mode Command procedure | Qualcomm, Nokia |
| #4 RAN UP security enhancements | Study enhanced user plane security for 6G to enable finer granularity control for the UP security, support UP key isolation for all the CU-UPs for a 6G RAN node in case of CU-CP/CU-UP RAN split architecture, service security requirements. | Samsung, Qualcomm, CATT, Xiaomi   |
| #5 Phy Layer Security | Taking security into consideration at the beginning of 6G reference signal or channel design to effectively preventpotential PHY layer security and privacy threats for MIB/SIB , Paging protection | SKT, Vivo, CATT, OPPO |
| #6 PQC/256 bit Algorithms, AEAD mode. | Adoption of Post-quantum secure authentication, migration of TLS, IKE, NAS etc in 6G. Adoption of 256-bit cipher suites in AS and NAS including AEAD mode. | AT&T, CATT, Vodafone |
| #7 SA2, SA4, SA5, SA6 related generic security WT | Study security and privacy aspects for 6G system architecture. To investigate security requirements, threats, and mitigation strategies for 6G, ensuring alignment with SA2/SA4/SA5/SA6 WGs security references. | AT&T, Samsung, Vivo, LG |
| #8 New NAS functionality | Security and privacy of a new non-access stratum functionality, including independent 6G security anchor function (SEAF), separate security anchors at HPLMN and VPLMN, Independent and secure access to control plane services,e.g., for easier service deployment. | Vodafone, China Mobile, Samsung, Vivo, CATT, IDCC, Xiaomi, Huawei, Nokia, Qualcomm.  |
| #9 Authentication enhancements | Study 6G Primary authentication enhancements including known gaps in primary authentication, secondary authentication and service authentication for network slice, external DN , including revocation and re-authentication. | SKT, Vivo, LG, Samsung, Xiaomi, Nokia, Lenovo, QC  |
| #10 RAN-Core Service based interface | Security aspects of RAN-Core Service based interface. | T-Mobile, IDCC, EricssonIDCC |
| #11 AI for network security | Study use of AI to automatically and efficiently enable 6G security e.g. anomalous behavior detection, autonomous network decision etc. | AT&T, T-Mobile, Nokia, Samsung, Vodafone,    |
| #12 Security for AI/AI Agents. | Identify security controls to protect AI-based systems from adversarial machine learning (AML) attacks on the 6G system. AI agent authentication and authorization, agent’s security and privacy, lifecycle data governance, data framework’s own security, and/or enhancement for user consent framework. | AT&T, Vodafone, China mobile, Samsung, Lenovo, Vivo, LG, CATT, Nokia, Huawei, Xiaomi  |
| #13 Data Security and privacy | Study mechanisms for privacy and security of data framework particularly for AI/Sensing etc. | AT&T, China Mobile, LG, Lenovo, IDCC, Xiaomi, Charter, OPPO, Ericsson, HuaweiNokia, Lenovo, Vodafone |
| #14 User Consent management | Unified privacy control framework (incl. dynamic user consent, data privacy, etc.) | Samsung, Vivo, LG, CATT, Nokia, IDCC, Xiaomi |
| #15 Service Exposure | Security mechanisms to support the exposure framework for requirements developed by SA2, SA6, etc. | China Mobile, Samsung, Vivo, Ericsson, Xiaomi, Huawei, Nokia |
| #16 Digital identity | Authentication, privacy and security aspects of both SIM based and SIM-less device digital identities. | T-Mobile, CATT, Lenovo, Xiaomi, Huawei |
| #17 Sensing | Security and privacy aspects of sensing services, (aligned with SA2). | Vivo, CATT, Xiaomi, E//, Huawei, Nokia |
| #18 Non 3GPP access Security | Multi access data connectionMigration and interworking with non 3GPP access | Charter |
| #19 Interworking | Study 6GS-5GS IWK, 6GS-N3GPP IWK, EPS IWK. | Xiaomi, E//, OPPO, Huawei and many other companies. |
| #20 SBA Enhancements | Enhancements to CN SBA security including endpoint security at transport and application layers. | Samsung, Xiaomi, Vivo, Huawei, Nokia, DT, Ericsson |
| #21 Regulatory services | Regulatory/Emergency services security including SMS, MCS, LCS, SoR/UPU | Vivo, Ericsson |
| #22 NTN | Security for UE-Satellite-UE communication, Lightweight authentication etc. | CATT, Ericsson, Nokia  |
| #23 Computing Security | Study security aspects of computing for UE, core network and application server in 6G, such as user authorization, service authorization, etc. | CATT |
| #24 Roaming | Study end to end roaming security taking roaming intermediatory into account | CATT, Ericsson, Nokia. |
| #25 CIOT Security | Study light weight authentication procedure, efficient key negotiation mechanism, efficient small data secure transmission protocol for IoT devices. | CATT   |
| #25 SNPN and CH  | dynamic connections between SNPN and CH other than current pre-configuration of addresses and certificatesenable SNPNs to be used to support emergency service and public safety use case | CISCO |
| #26 Cert management | identity information, certificates management for inter-PLMN and intra-PLMN communication, or even for other types of communication such as with service providers or over the top (e.g., apps) | Huawei  |
| #27 SECHAND for 6G | Study resilient access control security approaches to protect the 6G assets (of UE, RAN, Core NFs as applicable) to detect security breach/threat detection based on behavioural, contextual, and device posture metrics. | AT&T, T-Mobile, Lenovo |
| #28 Security event monitoring function | Study the integration of Security event monitoring Function, including the methods to implement closed-loop automation to adjust access permissions, network slice bandwidth, or service quality based on threat intelligence, device state information, behaviour monitoring, HW/SW version etc. | T-Mobile, Qualcomm   |
| #29 Local area based security | Study Use case on 6G Local Area Networks (TR 22.870[1] clause 5.9.6 ), clause11.9 Use case on 6G localized network for vertical, clause 11.10 Use case on in-vehicle local communication propose use cases on 6G localized network for different vertical scenarios. | China Telecom   |
| #30 decentralized trust enablement | Study the decentralized trust enablement which could be considered as a new security framework to enable 6G security. | China Mobile, Vodafone  |
| #31 DNS security | Identify the threats and operational challenges for intra-domain and inter-domain DNS used by 6G Core NFs. | JHAPL |
| #32 Slice specific security | Each network slice could have its own policy set, authentication/authorization logic, telemetry, and visibility — reducing lateral movement, cross-slice traffic interception, etc | T-Mobile |
|  #33 Micro segmentation | Support native micro-segmentation across all domains (NFs, RAN, UEs, Slices, NPN, NTN, etc.) with granular policy management/enforcement | T-Mobile |

 NOTE: Above table to be converted to text, remove company names before approving.

**TU estimates and dependencies**

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

# 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

{At least 4 supporting Individual Members are needed. There is an expectation that these companies will provide resources to progress the work. Note that having 4 supporting companies is a necessary but not sufficient condition: the usual TSG approval process by consensus is needed for the WID approval}

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