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

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

**Source: China Mobile**

**Title: Discussion paper on 6G Security Work Tasks**

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.

Thus this discussion paper first analyzes the security requirements from other working groups identified so far and proposes work tasks which could help structure the 6G security study item.

In addition, based on the alaysis, this discussion proposes to establish a new study item on decentralized trust enablement.

1. **Security requirements from SA1 TR 22.870**

|  |  |  |
| --- | --- | --- |
| **Clause No.** | **Security requirements** | **Proposed work tasks** |
| 5.5.1  Network security for 6G | [PR 5.3.1.2-1] The 6G network shall provide security mechanisms for secure access to elements of the core network of the 6G system and secure communication on all 3GPP defined interfaces of the core network of the 6G system.  [PR 5.3.1.2-2] The 6G network shall support establishment of secure communication between elements of the network while protecting network related information (e.g. network element identities, topology) from disclosure to unauthorized parties.  [PR 5.3.1.2-3] The 6G network shall provide security mechanisms that enable the network operator to ensure there are no unintended changes of the elements of the 6G network. | Network security; |
| 5.5.4  6G security requirements | [PR 5.3.4.2-1] The 6G system shall provide efficient mechanisms to support authentication and secure communication in inter-PLMN and intra-PLMN networks.  [PR 5.3.4.2-2] The 6G system shall support fine-grained security isolation based on the security needs of different businesses requirements for intra-PLMN networks.  [PR 5.3.4.2-3] The 6G system shall be able to provide flexible orchestration of security capabilities to ensure customized security requirements from customers.  Editor’s Note: Flexible orchestration is FFS.  [PR 5.3.4.2-4] The 6G network shall support identify potential security threats to communication and network elements.  [PR 5.3.4.2-5] The 6G network shall support security analysis and security enhancement policy generation to mitigate attacks and/or security issues in operator management system.  [PR 5.3.4.2-6] The 6G network shall support security response to implement enhanced security policy from management system to network elements, in order to recover network from disturbance.  [PR 5.3.4.2-7] The 6G system shall enable operators using SIM as trust anchor to provide identity and authentication service to the 3rd parties.  [PR 5.3.4.2-8] The 6G system shall support the verification for the association between the SIM identity and the digital identity of the different digital avatars.  Editor’s Note: Digital avatar is FFS.  [PR 5.3.4.2-9] The 6G system shall authorize the required services of the digital identity of the digital avatars of users and revoke the digital identity if needed.  Editor’s Note: Digital avatar is FFS. | Cross domain trust(to be SA3 independent);  Security management;  Access security (authentication); |
| 5.5.6  Considerations on privacy | [PR 5.3.5.3-1] Subject to regulatory requirements or operator policy, the 6G system shall protect from unauthorised access and disclosure to unauthorised entities any Personal Data belonging to a user and subscriber. | Data security and privacy |
| 5.5.2  Use case on quantum-resistant security | [PR 5.3.2.6-1] The 6G system shall provide security protection for communication (e.g., subscription identifier, authentication methods) against the potential attacks posed by quantum computing. | PQC (SA3 independent) |
| 5.5.3  Use case on UE selecting a base station after assessing its legitimacy | [PR 5.3.3.6-1] Subject to operator policy and regulatory requirements, the 6G system shall support a means for a UE to be able to distinguish a False Base Station from an authentic Base Station. | Access security (AS security); |
| 5.5.5  Use case on enhanced exposure | [PR 5.5.5.2-1] Subject to regulation, operator(s) policy and user consent, the 6G network shall support procedure(s) to expose aggregated (non-sensitive/anonymized/non-personally identifiable) information related to UEs, served by the network, e.g. number of UEs in a geographical location, their mobility pattern, application usage trends, from the network to authorized 3rd parties without exposing UE identities. | Data security and privacy;  Exposure security; |
| 5.5.7  Use case on privacy protection of data exposure | [PR 5.5.7.3-1] Subject to operator policy and regulatory requirements, the 6G system shall support privacy protection for any information exposure to a 3rd party.  [PR 5.5.7.3-2] Subject to national or regional regulatory requirement, the 6G system shall provide user privacy protection, location privacy, identity protection for UEs accessing 6G network for services (e.g. communication, sensing, AI inferencing), and for the corresponding information exposure to an authorized 3rd party. | Data security and privacy;  Exposure security; |
| 5.5.8  Use case on security control enhancements with NDT (Network Digital Twin) | [PR 5.5.8.6-1] Subject to operator’s policy, the 6G network should be able to support a Network Digital Twin for network and service management. | Security management |

1. **Security requirements identified from SA2 6G SID**

|  |  |
| --- | --- |
| **SA2 Work tasks** | **Proposed work tasks** |
| **WT#1**: Define the overall 6G architecture as collection of capabilities and high level functionalities considering the following sub work tasks and other work tasks to support 6G access network:  Study the support for control signalling for 6G for connectivity services and/or beyond connectivity services, including at least the following:  a. Whether and how to enable the introduction of a new non-access stratum functionality without impacting other non-access stratum functionalities.  b. Whether and how to identify a minimal set of non-access stratum functionalities that does not get impacted by additional non-access stratum functionalities.  c. Whether and how to develop generic mechanisms for UE-Core Network interaction to support operator services.  1.2. Study whether and how to support and/or enhance the following aspects in 6G: the SBA framework, network slicing, network sharing, user plane architecture, QoS framework, policy framework, network exposure framework, architecture for specific scenarios e.g. fixed wireless access, localized service access.  1.3. Study whether and how to support and/or enhance different non-3GPP access (e.g. Wi-Fi, wireline) in 6G and support multi-access data connections between 3GPP access and non-3GPP access.  1.4. Study whether and how to support and/or enhance the essential/regulatory services (i.e. voice, Messaging, location services, Emergency services, MPS, Mission Critical services, PWS) in 6G. | Access Security;  Network Security |
| **WT#2:**  Study migration and interworking, including  - How to support migration to 6GS  - How to support interworking with 5GS  - Whether and how to support interworking with EPS  - How to support interworking between 6GS and 4G/5G NTN/satellite access that use EPS/5GS. | Network Security |
| **WT#3**: Study how to support and enable use of AI in 6G (e.g. AI agent, framework). | AI security |
| **WT#4:** Study the integration of Sensing and Communication over 3GPP access, considering the sensing modes to be supported and other sources of sensing data. | Access security;  Network security;  Exposure security;  Data security and privacy; |
| **WT#5:** Study data framework for all aspects related to efficient and scalable data handling including, for example, data collection, distribution, processing, storage, data access and data exposure, with consideration of access control/user consent and privacy where relevant. The example of data may include data for AI and Sensing. This WT can also study any potential enhancements on system and procedure needed for user consent framework.  NOTE 6: The work split with SA3, SA5 and RAN WGs will require TSG coordination | Data security and privacy;  AI security; |
| **WT#6:** Study aspects on support of computing for UE, core network and application server in 6G (e.g. coordination between UE, core network and application server, exposure of computing service in the core network, etc.).  NOTE 7: Application layer mechanism and exposure framework may require coordination with SA6. | Exposure security; |
| **WT#7:** Study how to support 6G RAT for NTN, based on RAN decision, and support service continuity aspects. | Access security;  Network security;  Data security and privacy |
| **WT#8:** Study whether and how to support cellular IoT enablers in 6G, based on RAN decision for 6G IoT. | Access security;  Network security;  Data security and privacy |

1. **Security requirements identified from RAN 6G SID**

|  |  |
| --- | --- |
| **RAN Work tasks** | **Proposed work tasks** |
| 1. Single technology framework based on a stand-alone architecture (Note1) to support the agreed existing and new services, and to satisfy the usage scenarios, requirements, deployment scenarios and design principles with acceptable performance/complexity trade-off, as determined by the RAN requirements in [RP-250810] and [TR38.914], including: [RAN1], [RAN2], [RAN3], [RAN4]    1. Ensuring appropriate set of functionalities, minimize the adoption of multiple options for the same functionality, avoid excessive configurations, excessive UE capabilities and UE capabilities reporting.    2. Energy efficiency and energy saving: both for network and device.    3. Enhanced spectral efficiency.    4. Enhanced overall coverage, focus on cell-edge performance and UL coverage.    5. Wider channel bandwidth (at least 200MHz) support for 6G deployments at least above 2 GHz, around 7 GHz.    6. Re-use of existing 5G mid-band (~3.5GHz) site grid for 6G deployments in at least around 7 GHz and targeting comparable coverage to 5G mid-band.    7. Target scalable and forward compatible design for diverse device types.    8. Improved spectrum utilization and operations taking into account diverse spectrum allocations.    9. Aim at using common 6G Radio design, which meets mobile broadband service requirements as high priority, to also meet vertical needs.    10. Aim at a harmonized 6G Radio design for TN and NTN, including their integration.    11. System simplification, including reducing configuration complexity, enabling more efficient Cell/UE management, etc. | Access Security |
| 1. Physical Layer structure for 6GR,    1. Waveforms (OFDM-based) and modulations. 5G NR Waveforms and modulation should be considered for 6GR and is also the benchmark for other potential proposals. [RAN1, RAN4]    2. Frame structure, including compatibility with 5G NR to allow for efficient 5G-6G Multi-RAT Spectrum Sharing (MRSS). [RAN1]    3. Channel coding, using LDPC and Polar Code as baseline, considering applicable extensions to satisfy 6G requirements and characteristics with acceptable performance/complexity trade-off [RAN1]    4. Channel Bandwidth (at least minimum and maximum), Numerology, avoiding multiple numerologies for the same band / sub-range (e.g., enabling synergies among frequency bands in the ~7GHz range) [RAN1, RAN4]    5. Physical layer control, data scheduling and HARQ operation [RAN1, RAN2]    6. MIMO operation [RAN1, RAN4]    7. Duplexing [RAN1, RAN4]    8. Initial access [RAN1, RAN2, RAN4]       * Studies on synchronization signal and raster, broadcast signals/channel and physical random access channel [RAN1, RAN4]       * Studies on initial access procedure, random access procedures, system information and paging [RAN2, RAN1, RAN4]    9. 6GR spectrum utilization and aggregation. [RAN1, RAN2, RAN4]    10. Other physical layer signals, channels and procedures [RAN1, RAN2, RAN4]    11. Evaluate performance of at least energy efficiency, spectrum efficiency, and coverage compared to 5G NR, and deliver the initial result at the end of study [RAN1].        1. RAN4 can be involved, if necessary, based on the LS from RAN1 | Access Security |
| 1. Radio interface protocol architecture and procedures for 6GR [RAN2, RAN1, RAN4, RAN3] 2. User Plane architecture and protocol design [RAN2] 3. Control Plane architecture (including RRC states) and protocol design [RAN2, RAN3] 4. Access stratum security aspects, in alignment with requirements from SA3 [RAN2] 5. Radio signalling framework for UE capabilities, aiming at improvements and simplification compared to 5G NR [RAN2, RAN1, RAN4] 6. Data transfer design to support various types of data (e.g. AI/ML, Sensing, etc) [RAN2, RAN3] | AI security;  Data security and privacy |
| 1. Mobility for 6GR (for all RRC states), including related RRM [RAN2, RAN1, RAN4, RAN3] | Access Security; |
| 1. 6GR core and performance requirements 2. General RF aspects [RAN4]    * + Intra-3GPP co-existence studies      + Study RF related system parameters and requirements 3. BS RF requirement aspects including band [RAN4]    * + BS RF requirement and testing framework aiming at improvements and/or simplification compared to 5G NR, including MSR and AAS operation      + Study how to improve 6G BS core, conformance specifications, including structure and drafting principles 4. UE RF requirement aspects including band and band combination [RAN4]    * + UE RF requirement framework aiming at improvements and/or simplification compared to 5G NR      + Study how to improve 6G UE RF specification(s), including structure, drafting principles, and database for band combination      + Study UE RF capabilities considering different device types and implementations 5. RRM aspects for 6GR [RAN4, RAN1, RAN2]    * + RRM requirement and procedure aspects aiming at improvements and/or simplification compared to 5G NR      + Study how to improve 6G requirement specification, including structure and drafting principles 6. Demodulation and performance aspects [RAN4]    * + Demodulation and performance requirement framework and key assumptions, aiming at improvements and/or simplification compared to 5G NR for UE and BS      + Study how to improve 6G demodulation and performance specifications, including structure and drafting principles for UE and BS 7. Aspects related to the testability [RAN4]    * + Testability methodology framework and key assumptions, aiming to ensure that requirements can be properly tested considering the applicability and feasibility of conductive and/or OTA testing with reasonable complexity 8. Other aspects    * + Handling irregular channel bandwidths including the definition [RAN4, RAN1]      + Definition of ‘frequency range(s)’[RAN4] | Access Security; |
| 1. Radio Access Network architecture, interface protocols and procedures considering support of various services and functionalities (e.g. AI/ML, sensing, etc). [RAN3, RAN2] 2. Overall RAN architecture aspects [RAN3, RAN2] 3. RAN-CN functional split, interface, protocol stack and procedures [RAN3] 4. RAN internal functional split, interfaces, protocol stacks and procedures, [RAN3, RAN2] | Access Security; |
| 1. Migration from 5G NR to 6GR as well as interworking and mobility between 5G NR and 6GR: 2. 5G-6G Multi-RAT Spectrum Sharing for migration [RAN1, RAN2, RAN4, RAN3] 3. Study if any additional migration mechanism is necessary. [RAN] [RAN2, RAN1, RAN3, RAN4] NOTE: the start of this study objective (b) should be triggered by RAN plenary in time to guarantee proper completion of the WG study. 4. Mobility between 5G NR and 6GR [RAN2, RAN3, RAN4] | Access Security; |
| 1. AI/ML for 6GR and Radio Access Network, leveraging 5G AI/ML framework, as appropriate [See TR38.843] [RAN1, RAN2, RAN3, RAN4] 2. Identify Use Case(s) of interest (either existing or new) with compelling trade-off between e.g., performance, complexity, etc…  Coordinated discussion needs to be ensured with related design areas, where needed (e.g., MIMO, Mobility, etc…)   NOTE: lead WG depends on the use case.   1. AI/ML framework: Extensible AI/ML enablers based on the identified Use Case(s), including    1. LCM procedures [RAN2, RAN1, RAN3, RAN4]    2. Data collection and data management, in coordination with SA WGs [RAN2, RAN3, RAN1] | AI security;  Data security and privacy |
| 1. Sensing – Studies to be based on use cases and associated requirements, as defined in [TR38.914] 2. PHY functions and procedures for sensing technology (e.g., waveform. reference signals, measurement feedback, etc…) [RAN1, RAN4] 3. Evaluate sensing performance and if necessary, extend channel modelling, for the selected use cases [RAN1] 4. Aspects of integration with communication services [RAN1] 5. higher layer procedures and protocol aspects [RAN2] 6. RAN4 aspects of sensing including RF, coexistence, and testability in coordination with other WGs [RAN4]   Note: RAN1 identify detailed requirements, if triggered by TSG RAN | Access security;  Exposure security;  Data security and privacy; |

1. **Necessity to have an independent SID focusing on decentralized trust enablement**

The 5G ecosystem today faces growing complexity, with multi-vendor network functions, diverse cloud infrastructures, and varying security implementations—all built on the same standards yet introducing fragmented risks and attack vectors. As we look toward 6G, deployment requirements must prioritize adaptability to support a wider range of applications and customer needs. To ensure secure and trustworthy operations across diverse scenarios—including intra-operator (e.g., intra-PLMN NF communication, PLMN-NPN communication, etc.) and roaming—6G’s security framework must evolve beyond traditional models, embracing flexibility, decentralization, and cloud-native principles.

The increasing system complexity, driven by hybrid cloud deployments and multi-layered architectures, demands a re-evaluation of current trust and security mechanisms. With 3GPP’s 6G study phase underway, it is critical to explore decentralized trust frameworks and technologies that can address existing gaps while future-proofing security for emerging challenges.

A decentralized trust framework is critical as a core enabler for 6G security, offering:

- Resilience against single points of failure—vital for distributed cloud and edge deployments.

- Dynamic adaptability—ensuring security policies evolve with network conditions, threat landscapes, and regulatory requirements.

- Cloud-native scalability—seamlessly integrating with hybrid and multi-cloud environments.

- Efficient trust establishment—enabling secure, automated interactions between network functions (NFs), even across roaming and multi-operator scenarios.

Thus this shift will be essential and serve as a security infrastructure for securing intra-PLMN NF communications, multi-domain trust establishement, roaming, and emerging decentralized applications. Taking this exploration as an independent study can ensure that 6G’s security infrastructure is not merely reactive but proactively designed to serve as a trusted, universal foundation for the general telecommunications network.

# Conclusion

1. **Based on the above analysis, it is proposed to have the following Working Tasks included in the 6G System Security SID.**

**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.

1. **It’s proposed to have another independent SID to study the decentralized trust enablement which could be considered as a new security framework to enable 6G security.**