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

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

**Source: Samsung**

**Title: 6G Work Tasks proposal**

**Document for: Approval**

**Agenda Item:**

# 1 Justification

As SA2 and RAN 6G studies is already approved with several work tasks, it would be beneficial, specifically in assisting SA2 and RAN with SA3 inputs for their architectural consideration.

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.

SA1 has already studied use case on UE selecting a base station after assessing its legitimacy as specified in TR 22.870 [2]. According to which it is more feasible now to address the FBS attack issue in beginning of the new generation.

Meanwhile, RAN WGs approved (RP-251881 [3]) SID for 6G anticipating enhancements to Radio interface protocol architecture and procedures for 6G Radio. In release 19 LTM security study, SA3 already acknowledged unprotected MAC CE issue, however we believe a dedicated investigation on threat analysis and mechanism to address the issue needs to be studied for 6G on the need for protection of MAC layer messages.

Further, today the granularity for application of the UPSE information is on per-PDU Session basis. In some applications, the use of the UP integrity protection and UP confidentiality protection does not bring much value and leads to unnecessary processing of resources. There is a need for a study to enhance the UP security mechanism with more granularity.

Further, as per RP-251881 [3] RAN internal functional split, interfaces, protocol stacks and procedures are in consideration. If 6G RAN internal split 5G architecture supports CU-CP/CU-UP Split Architecture similar to 5G architecture then as per the current KDF, same UP keys will be generated for all the CU-UPs for a 6G RAN node which is not a good security practise.

Considering the key security challenges outlined Samsung proposes corresponding Work Tasks in section 2.

# 2 Work Tasks

**WT#1:** Study on security and privacy aspects for 6G system and RAN architecture. To investigate security requirements, threats, and mitigation strategies for 6G, ensuring alignment with SA2’s and RAN’s architectural work tasks.

* 1. Study of primary authentication protocols enhancement (if any) and security procedures to ensure alignment with 6G’s UE-Core Network interaction mechanisms. Further, based on the decision on architecture the authentication protocols and methods, entities (Network Functions involved in the authentication) and their functionalities are to be determined.
	2. Study and investigate the security impacts of 6G control signalling mechanisms (e.g., new non-access stratum functionalities, generic framework for UE-Core Network interaction to support operator services, etc.), if any.
	3. Study and investigate security enhancements for the 6G aspects such as 6G SBA framework, network slicing, network sharing, user plane architecture enhancement, QoS framework, policy framework and network exposure framework.
	4. Study security aspects for migration and interworking with pre-6G systems in terms of transfer or derivation of security context.
	5. Study and define safeguards for AI agents and governance framework for autonomous network decision.
	6. Study the security aspects of secure data handling and exposure for several use cases such as sensing data, compute data, and analytics data.
	7. Study the support for user consent management and enforcement in the context of 6G networks.

**WT#2:** Study on false base station attacks mitigation at earlier stages of communication establishment in 6G. Investigate and define a security mechanism for UEs to verify the authenticity of base stations at the earliest i.e., the 6G system should support a means for a UE to be able to distinguish a False Base Station from an authentic Base Station.

**WT#3:** Study and investigate on threats to signalling information in lower layer (i.e., MAC layer) and define a security mechanism for vulnerable lower layer signalling traffic (MAC CEs, LTM commands like so) to mitigate the identified threats.

**WT#4:** Study enhanced user plane security for 6G with the following objectives:

4.1. Add a finer granularity control for the UP security.

4.2 To support UP key isolation for all the CU-UPs for a 6G RAN node in case of CU-CP/CU-UP RAN split architecture.

# 3 References

[1] SP-250806 - Study on Architecture for 6G System.

[2] 3GPP TR 22.870 Study on 6G Use Cases and Service Requirements.

[3] RP-251881 - New SID: Study on 6G Radio.