**[Conference Call on 6G Study Preparations]**

***for*** 3GPP TSG-SA3 Meeting #123 **WT-Lenovo-v1**

Goteborg, Sweden, 25 – 29 August 2025 (revision of xx-yyxxxx)

**Source: Lenovo, Motorola Mobility**

**Title: 6G Security Study Work Task Input and objectives**

**Document for: Discussion & Input for 6G Security TR**

**Agenda Item: Conference Call on 6G Study Preparations**

# 3 Rationale

This contribution provides the objectives for the following security work tasks to be considered for the 6G Security Study. The detailed justification and reference related to each security work task is provided in the companion document DP-Lenovo-v1 (6G Security Study Work Task Input(s)).

* WT1: 6G Security Architecture and Key hierarchy
* WT2: Digital Identification and Authentication
* WT3: 6G E2E Trusted and Secure Connections
* WT4: Secure AI/ML
* WT5: Data Exposure Privacy and Security
* WT6: Data Privacy and User Consent

# 4 Objectives

The Objectives of each 6G Security Work Task are described below.

* WT1: 6G Security Architecture and Key hierarchy
  + Study and identify the potential connections and scenarios which falls in the scope of 6G E2E system security.
  + Study and define a holistic 6G Security architecture that covers all possible scenarios as applicable e.g., including but not limited to different PLMN, NPN and PNINPN deployments.
  + Study and define a common 6G key hierarchy to support any required UE to Network connection/communication Security as applicable (e.g., AS, NAS, application services, data collection, data provisioning, sensitive service/network slice cryptographic isolation (e.g., AMF reallocation in case of lack of N14 kind of scenarios) etc.,)
  + Study and define the security establishment procedures (key refresh as applicable) in alignment with the defined 6G Key hierarchy
* WT2: Digital Identification and Authentication
  + Study and identify the security use cases in 6G System which can benefit from Digital identity-based authentication, selective data disclosure and credentials control.
  + Study how the Digital Identification and trust establishment framework can be supported for the 6G System for UE Authentication and Network Authentication.
  + Study how digital identification and authentication can be procedurally supported for the identified security use cases.
* WT3: 6G E2E Trusted and Secure Connections
  + Study the feasible methods to identify security risk/threats at 6G UE, RAN and Core.
  + Study and define resilient access control security approaches to protect the 6G assets (UE, RAN, Core as applicable) in case of potential security breach/threat detection.
* WT4: Secure AI/ML
  + Study the potential security vulnerabilities of AI/ML operations.
  + NOTE: For reference, can consider the AI/ML operations and 6G System usage scenarios described in TR 22.870.
  + Study and define solutions to secure AI/ML operations in 6GS against the identified security vulnerabilities.
* WT5: Data Exposure Privacy and Security
  + Study and define the potential security requirements of UE data exposure
  + Study and define the potential security requirements of Network data exposure
  + NOTE1: Study and list the scenarios from TR 22.780 which requires network level data exposure and list the scenarios which requires application-level data exposure. This information can be used as baseline scenario to define the respective security solution.
  + For Network level/layer data exposure, study and define the security mechanisms to enable unified data exposure security.
  + For Application level/layer data exposure, study and define the security mechanisms to enable unified data exposure security.
* WT6: Data Privacy and User Consent
  + Study and identify the potential scenarios (both 3GPP features and exposure to 3rd party) which requires data privacy and user consent.
  + Case 1: Study the security solution to enable data privacy (and govern user consent) as applicable in case of 3GPP features.
  + Case 2: Study the security solution to enable data privacy (and govern user consent) as applicable in case of UE data exposure to 3rd party.
  + NOTE: There may be a unified or dedicated solution for the above two cases. Study the pros and cons of both.