**3GPP TSG-SA3 Meeting #124 S3-253307-r1**

**Wuhan, China, 13 – 17 October 2025**

**Source: CableLabs**

**Title: General security requirements for 6G – the CAPTAIN framework**

**Document for: Approval**

**Agenda item: 5.3.1**

**Spec: 3GPP TR 33.801-01**

**Version: 0.1.0**

**Work Item: FS\_6G\_SEC**

**Comments**

This contribution proposes general security requirements, as outlined in the CAPTAIN framework, for TR 33.801-01.

\* \* \* First Change \* \* \* \*

# 4 Security areas and high level security requirements

## 4.1 Security areas

Editor's Note: This clause further clarifies the scope of the study by listing the security areas that SA3 is working on.

## 4.2 Potential high level security requirements

Editor's Note: This clause will document high-level requirements that guide the study.

4.2.x General

Security and privacy are considered the cornerstones of 6G systems. Instead of attempting to mitigate security threats only after they arise, 6G systems need to adopt the principle of secure by design to ensure that fundamental security properties are built into 6G system procedures, messages, and information elements from the first release.

More specifically, 6G systems need to consider supporting the following fundamental security properties:

* Confidentiality: ensures that the content of communication is accessible only to authorized entities and remains protected against disclosure to unauthorized parties. Typically achieved through symmetric or asymmetric encryption. Confidentiality needs to take into consideration of hop-by-hop or end-to-end.
* Authentication: includes entity authentication and data origin authentication. The former verifies that a communicating entity (e.g., user equipment, network function, or service) is genuinely what it claims to be. The latter ensures the source of a message or data is indeed as claimed. Authentication needs to take into consideration of hop-by-hop or end-to-end.
* Privacy: protects sensitive subscriber-related information, such as permanent identifiers, location data, and usage patterns, from unauthorized access, inference, or correlation. Privacy may be achieved by means such as encryption, anonymization, and obfuscation. Privacy extends beyond confidentiality by preventing tracking and linkage of communications to specific users.
* Timeliness: guarantees the freshness and validity of received messages, ensuring they are recent and not replays of previously captured communications. Often referred to as anti-replay, and achieved via nonces, sequence numbers, or timestamps.
* Authorization: ensures that authenticated entities are granted access only to the resources, services, or operations for which they have explicit permission. Authorization enforces fine-grained access control policies based on user roles, attributes, or contexts, preventing misuse of legitimate credentials and restricting privileged actions. Effective authorization mechanisms often rely on token-based access, capability-based models, or policy decision points to dynamically evaluate access rights.
* Integrity: protects data and signalling messages are not tampered with during transmission or at rest. Typically achieved with message authentication codes (MACs) or digital signatures, both of which also provide data origin authentication.
* Non-repudiation: provides cryptographic evidence of actions or events so that participating entities cannot deny their involvement in specific communications or actions. Relies on entity authentication, secure logging, and verifiable digital signatures, and is critical for accountability and dispute resolution, particularly in cross trust domain communications.
* Availability: ensures that network services, signalling procedures, and resources remain accessible and reliable for authorized users, even under malicious conditions. Includes resilience against Denial-of-Service (DoS) and resource-exhaustion attacks that aim to disrupt connectivity, mobility, or service delivery.

Those fundamental security properties shall be used to evaluate 6G communication procedures and messages to ensure they are considered and supported if practical during the first release of 6G specifications.

Note that not all security properties need to be supported by every procedure and every message. For example, while authentication may be important to broadcasting messages, confidentiality is not since those messages are intended to be public. For another example, non-repudiation may be important to communications across administrative domains, e.g., in roaming, it may be less critical within a trust domain.

Editor’s Note: Additional security properties and further descriptions are FFS.

4.2.y High level security requirements

\* \* \* End of Changes \* \* \* \*