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

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

**Source: Vodafone**

**Title: Discussion paper on Vodafone’s Priorities for 6G Security Standardisation**

**Document for: Discussion**

**Agenda Item:**

# References

[1] S3-252391- SA3 initial plan for 6G Study.

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

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

# 6G Security Work Tasks Proposal

* 1. Background

As 3GPP SA3 initiates work on 6G security, Vodafone recognises the need to proactively shape the security architecture to ensure resilience, privacy, and trustworthiness. This paper outlines Vodafone’s position on three foundational areas of 6G security standardisation:

1. **Securing architectural changes**
2. **Securing new 6G features**
3. **Introducing enhanced security capabilities beyond 5G.**
   1. Securing Architectural Changes

6G may introduce architectural shifts that may decentralise or distribute core functions and/or procedures. One proposal being discussed involves distributing NAS to terminate in three separate core network nodes.

Vodafone supports innovation but insists on:

* Robust key distribution mechanisms
* Preserving NAS integrity and confidentiality

Recommendation:

* Study item on distributed NAS security termination
* Threat modelling and key management evaluation
* Alignment with GSMA and trust frameworks
  1. Securing New Features and Capabilities

6G is assumed to introduce AI-native functions, integrated sensing, and ambient IoT, expanding the attack surface.

Vodafone advocates for:

* Secure-by-design approach
* Mandatory threat assessments
* Security embedded from feature inception

Recommendation:

* Security review gate for new features
* Security checklist for AI-based features
* Early engagement with GSMA FASG and PQTN
  1. New or Improved Security Features

6G offers an opportunity to enhance baseline security capabilities.

Vodafone supports:

* Post-quantum secure authentication
* Enhanced user privacy through pseudonymisation
* 256-bit encryption and AEAD for radio interface

Recommendation:

* PQC migration for TLS, IKE, and NAS
* Define 256-bit cipher suites
* Standardise AEAD modes for radio encryption
  1. Conclusion

Vodafone proposes addressing the three pillars in the 6G Security study

Additional recommendations:

* Joint workshops with GSMA, ETSI, and others as seen needed
* Align on cryptographic roadmaps and threat models