



Telecommunications
Standards Development
Society, India

TECH DEEP DIVE

TTDD 2025 CONFERENCE (8th EDITION)

STANDARDISING 6G:

ARCHITECTING INTELLIGENT, SECURE AND SUSTAINABLE NETWORKS & SERVICES

 **Date:** 15-18 July 2025

Media Partner

COMMUNICATIONS TODAY

Session #4 - Security in a hyper connected world, especially for 6G

16 July 2025

Securing the Future

: Lessons from 5G and the Blueprint for 6G Security

by

Saurabh Khare, Nokia

Securing the Future

Lessons learned from 5G: Security can not be an afterthought

 UE to Core Network Security • Subscription Identity Privacy • Authentication framework • Multiple Non-Access Stratum Security	Slow deployment More than 50% of features are not deployed in SA due to multiple architecture options (NSA/SA) causing delay in security features as well
 UE to Radio Access Network Security • Access Stratum / PDCP layer Security • Integrity protection (new feature)	Late specifications and no deployment Full Rate User Plane integrity protection (UP IP) introduced only in Rel-17, not yet deployed in networks; not all UEs will be able to cope up with it
 Core Network and Management security • Service Based Architecture Security enhancements • End-to-End Roaming Security • Exposure Function and API Framework Security	Complex solutions and deployments Features specification across different releases introduce complexity, multiplicity of protocols and complicates deployments
 Security for additional features • Edge, enablers for Network Automation (eNA), AI/ML, Non-Terrestrial Networks (NTN), Non-Public Networks (NPN), Proximity Services (ProSe), WWC, etc.	Late specifications of basic features Basic security features added along with the new features complicated the deployment and adoption

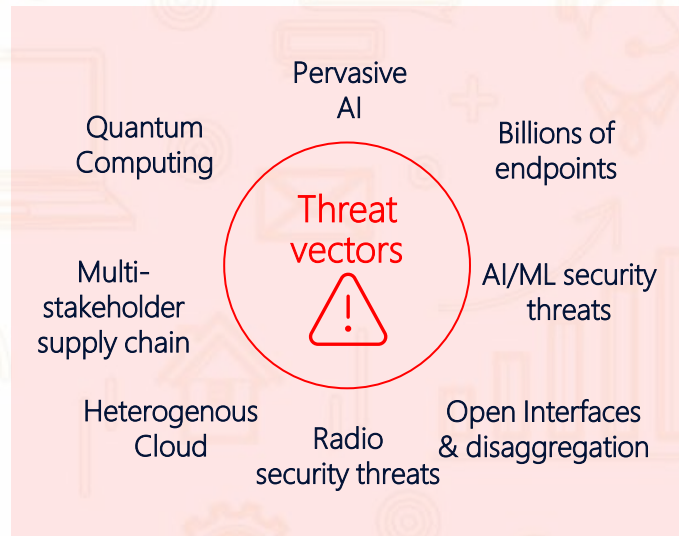
Foundational 6G security features for UE and the network need to be ready from 6G day one

Securing the Future

Blueprint for 6G Security— known and novel threats

Technology perspective

Time horizon of 2030-2040 will bring new technology-induced attack vectors / threat surfaces to (mobile) networks



"Secure by Design"

Design of 6G network security architecture must

- Cater for known/foreseen attack vectors and allow for **flexible migration to updated** security features/ mechanisms
- Efficiently enable **extensions** to address yet unknown threat vectors and assure future-proofness
- Allow for **composable** security solutions

Securing the Future

Blueprint for 6G Security– novel requirements

Build 6G Security on 5G

- 5G security provides already a very strong basis for 6G security
- Even stronger security in 6G with learnings from 5G

Security & Privacy by Design

- Target is to avoid add-up security features after architectural development
- Security considerations should be embedded into 6G architecture design phase

Security of new technologies enabled from 6G Day One

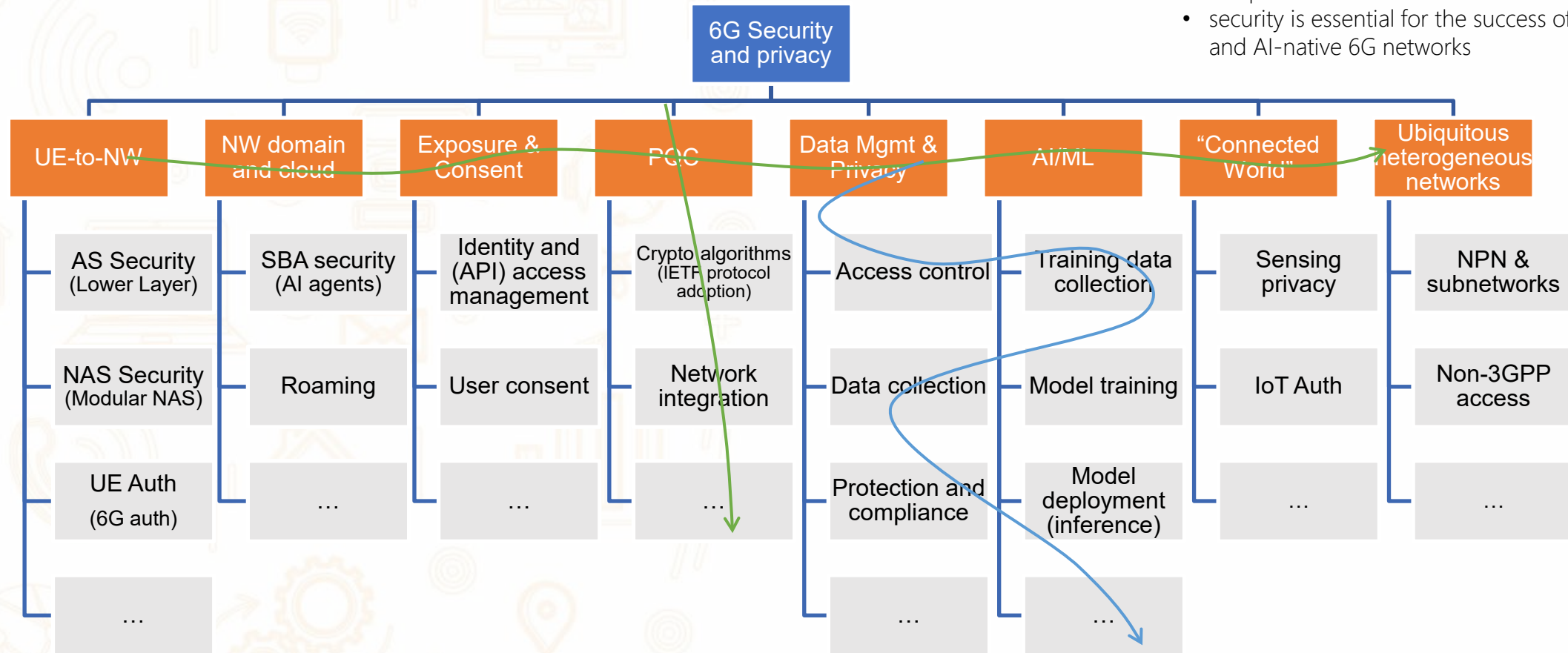
- Quantum Security (asymmetric crypto update- Interfaces, SUCI)
- Radio Security (Lower Layer)
- AI Security (training, data sanitization..)

Foundational 6G security features for UE and the network need to be ready from 6G day one

Securing the Future

Blueprint for 6G Security– novel requirements

- comprehensive security approach when designing 6G networks
- Adaptable PQC solutions in 6G
- security is essential for the success of data-centric and AI-native 6G networks



Thank You
<saurobh.khare@nokia.com>