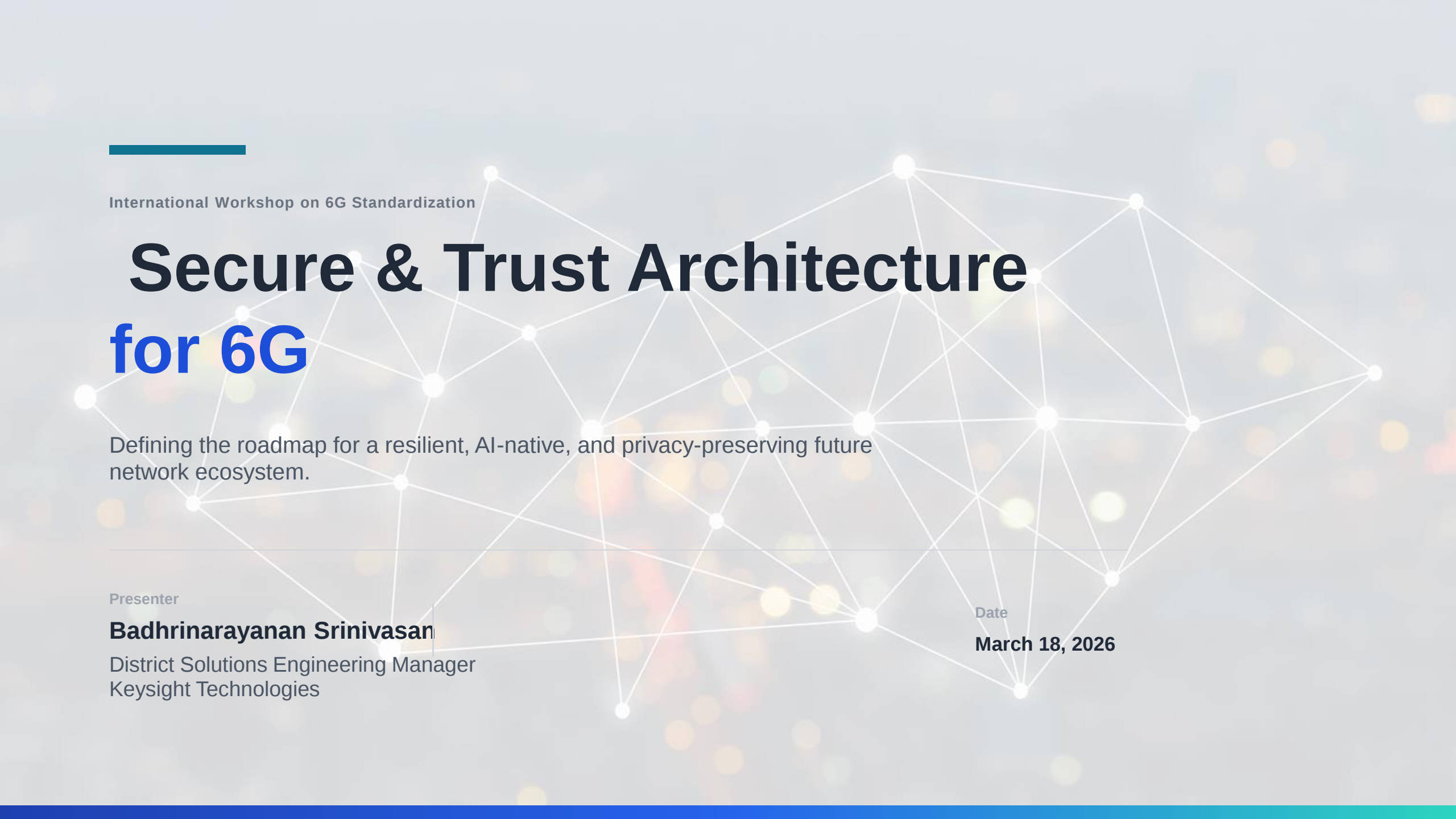




International Workshop on 6G Standardization

Secure & Trust Architecture for 6G

Defining the roadmap for a resilient, AI-native, and privacy-preserving future network ecosystem.

Presenter

Badhrinarayanan Srinivasan

District Solutions Engineering Manager
Keysight Technologies

Date

March 18, 2026

From 5G Today to 6G Tomorrow

5G Scale & Maturity

By mid-2025, global 5G subscriptions reached **~2.9 billion** (approx. 1/3 of all mobile users). India alone accounts for **~400 million** subscribers, demonstrating rapid massive-scale adoption.



6G Vision (ITU IMT-2030)

Targeting **100x higher peak data rates** and sub-0.1 ms latency. Moving beyond terrestrial constraints to achieve **ubiquitous connectivity** via integrated satellite/UAV networks.



Why Security Matters

Hyper-connectivity expands the attack surface. We must evolve from 5G's identity-based trust to a **unified, AI-native security architecture** protecting physical sensing data and multi-domain environments.



Motivation & Digital Ecosystem Vision

Driving forces behind the 6G transformation:

Immersive Reality

Holographic telepresence, volumetric video, and extended reality (XR) demanding Tbps throughput.

Digital Twins

Instantaneous, high-fidelity replicas of cities, factories, and networks for real-time simulation.

Tactile Internet

Sub-millisecond control loops for remote robotics, autonomous vehicles, and tele-surgery.

Pervasive AI-IoT

Billions of intelligent edge devices creating a massive, distributed compute fabric.

Cyber-Physical

Deep integration of sensing, computing, and actuation in physical environments.

Global Continuity

Seamless service across ground, air, sea, and space via integrated NTN.

The Trust Imperative

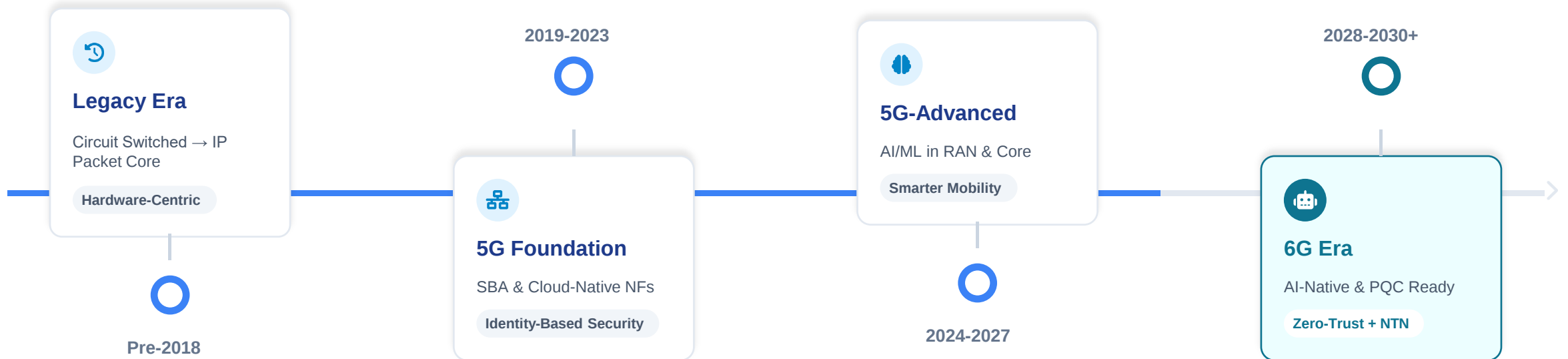
As digital and physical worlds merge, **trust becomes critical infrastructure**. Security must ensure human safety, privacy, and system resilience by design.



6G Ecosystem

Convergence of Digital, Physical & Biological Worlds

Evolution of Networks: 5G → 6G



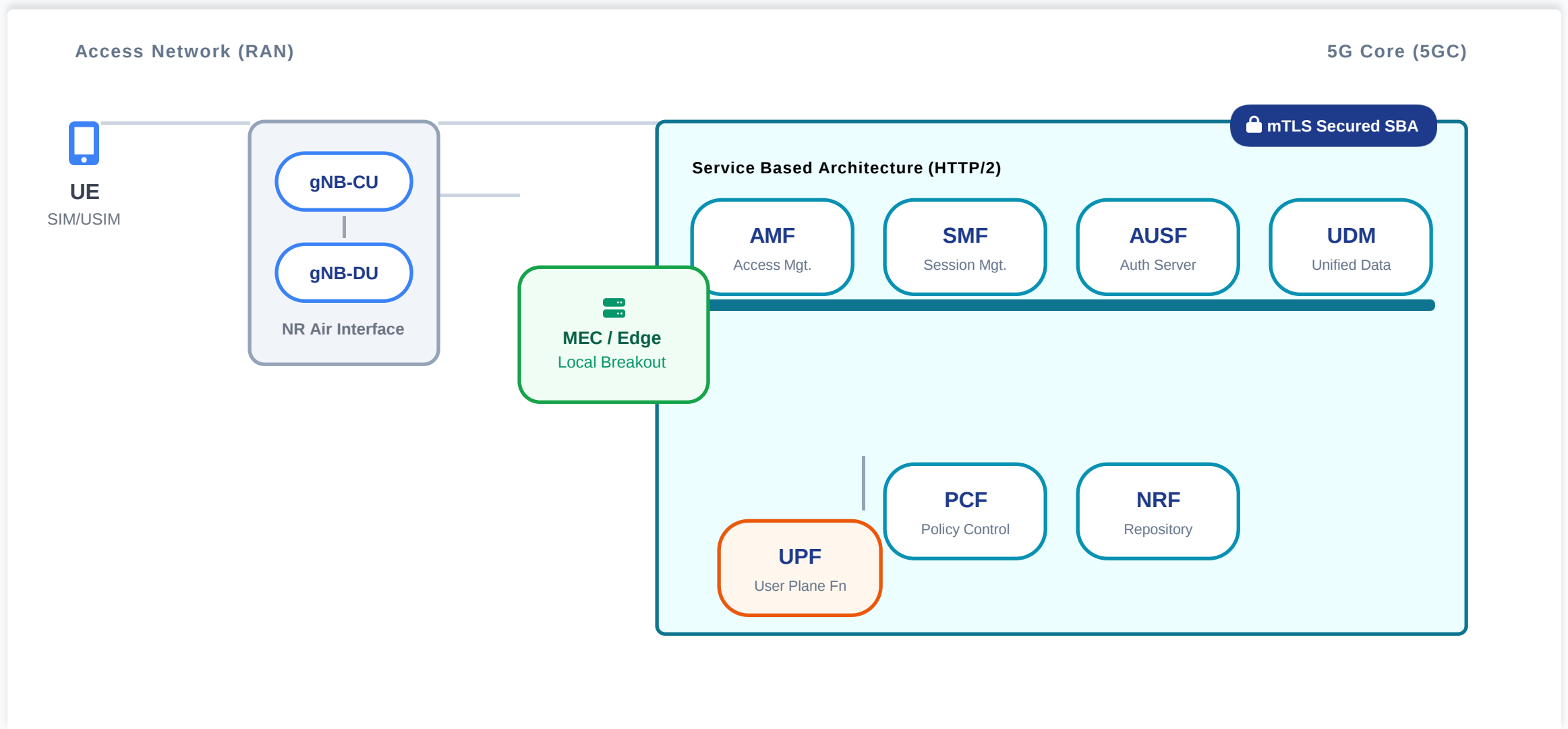
💡 Architectural Shift

Moving from **Cloud-Native (5G)** to **AI-Native (6G)** architecture. Security evolves from explicit identity checks to continuous zero-trust verification with post-quantum resilience.

Technology Pillars of 6G



5G Architecture Reference



6G Architecture Vision



**ZERO-
TRUST
SECURITY
FABRIC**

5G vs 6G – Architectural Comparison

Intelligence

5G: AI-Assisted (Overlay optimization via NWDAF)

6G: AI-Native (Intrinsic to air interface & core fabric)

Coverage

5G: Terrestrial-First (Limited NTN)

6G: Space–Air–Ground–Sea (Integrated 3D coverage)

Security

5G: Perimeter Defense & Classical Crypto

6G: Zero-Trust Architecture & Post-Quantum Crypto

Spectrum

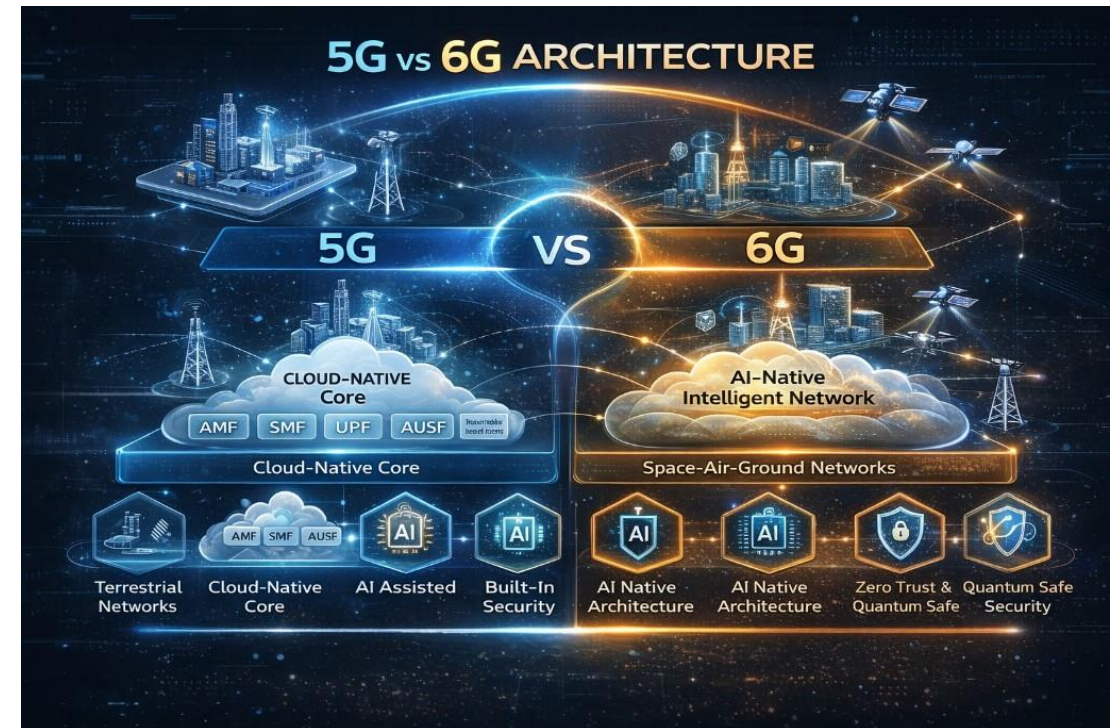
5G: mmWave Centric (~100 GHz)

6G: Sub-THz & THz (0.1–10 THz)

Data Privacy

5G: Centralized Data Lakes

6G: Privacy-by-Design & Decentralized Consent



Security Challenges in 6G

	📱 Device / IoT	📶 RAN / Edge	🏠 Core / SBA	☁️ Cloud / AI
Massive Scale Heterogeneity	Endpoint Diversity Managing billions of identities across varied form factors.	Edge Congestion AuthN storms from massive IoT attach requests.	Signaling Load Handling state for billions of active sessions.	Resource Scale Elastic scaling of security VNFs/CNFs.
New Attack Surfaces Physical & Cyber	Sensing Spoofing Injecting fake radar/lidar data to fool systems.	Jamming / MitM Physical layer attacks on THz & sensing signals.	API Vulnerabilities Exposure via open interfaces (CAPIF/NEF).	SATCOM Threats Orbital link interception & constellation DoS.
AI / ML Risks Adversarial AI	Model Evasion Crafting inputs to bypass device security.	Data Poisoning Corrupting training data at the edge.	Model Inversion Extracting user data from shared models.	Automated Attacks AI-driven swarming & zero-day generation.
Quantum Threat Crypto-Agility	Key Storage Vulnerable SIM/eSIM root keys.	Air Interface Decryption of recorded RAN traffic (Harvest Now).	Control Plane Breaking current PKI/TLS trust chains.	Long-Term Data Risk to archived encrypted user data.
Trust & Privacy Zero-Trust	Attestation Verifying integrity of diverse HW/SW.	Location Privacy Precise tracking via sensing/THz beams.	Cross-Domain Federated trust across MNOs & hyperscalers.	Compliance Sovereignty & regulatory alignment (GDPR/AI Act).

● Critical Risk
● High Risk
● Medium Risk
● Low Risk

Secure 6G Architecture Layers



Cross-Domain & Supply Chain

Inter-Operator Trust

Roaming Security



Security Operations (SecOps)

AI Telemetry

UEBA

SOAR



Data & AI Governance

PETs / Encryption

Model Signing



Core Network (SBA / API)

mTLS + PQC

Token AuthZ (OAuth)



Access & Transport (RAN)

PHY/MAC Auth

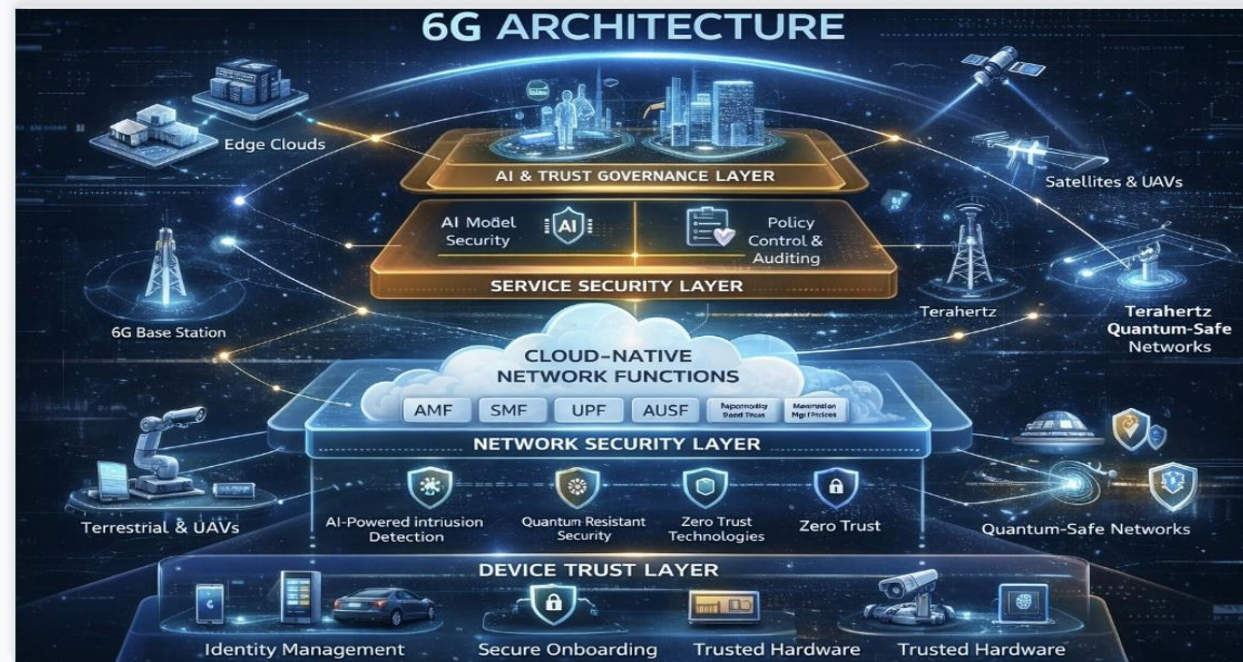
RRC Integrity



Device & Platform Trust

Secure Boot

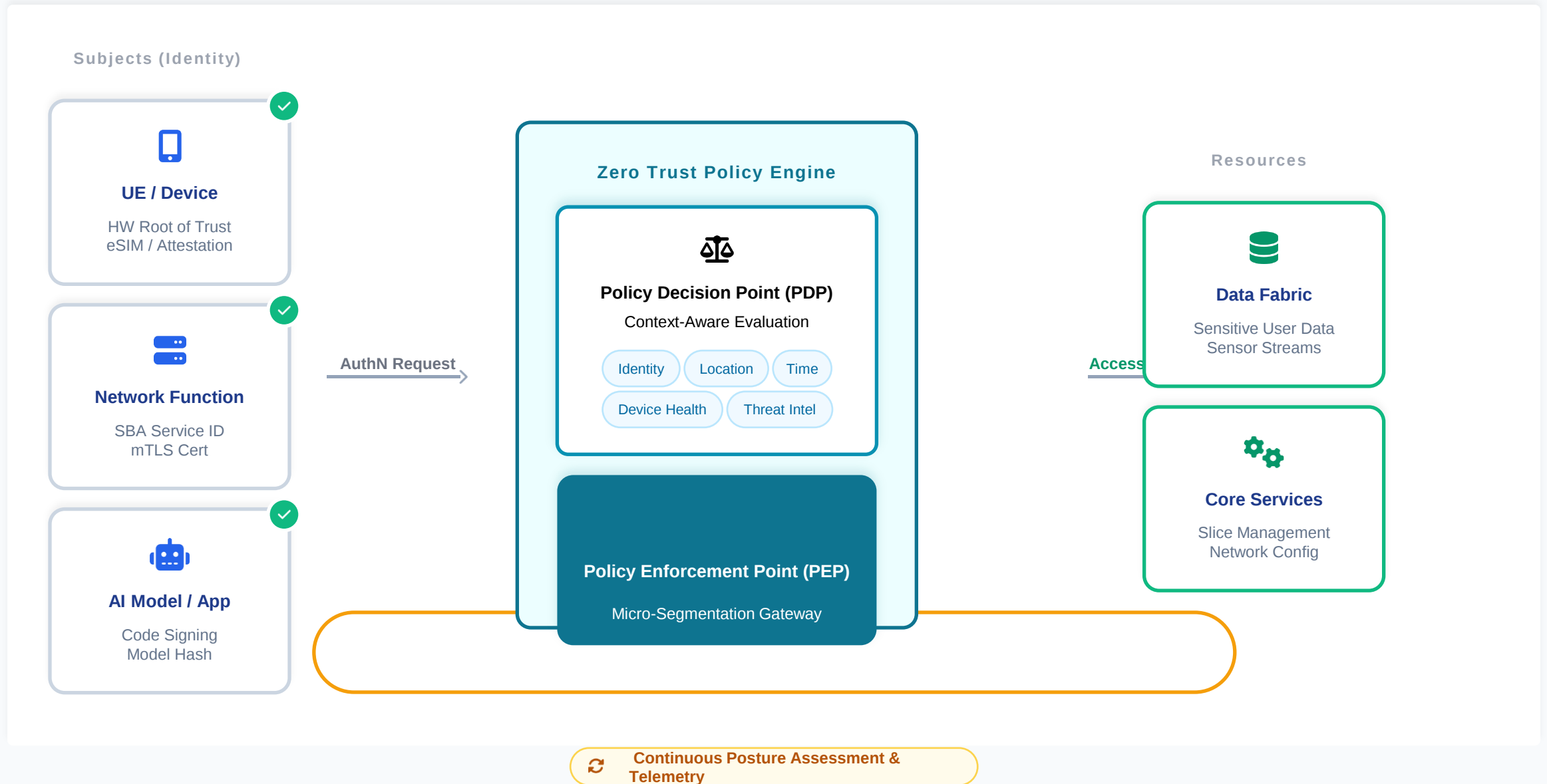
TEE / HW Root of Trust



Defense-in-Depth Strategy

- ✓ **Hardware Root of Trust:** Security starts at the silicon level with TEE and secure boot to ensure device integrity.
- ✓ **Quantum-Safe Transport:** Control plane (SBA) and user plane traffic protected by PQC-enabled mTLS.
- ✓ **AI Governance:** Explicit layer for securing AI models and privacy-preserving data handling.
- ✓ **Automated Ops:** AI-driven SOAR and telemetry enable real-time threat response.

Zero-Trust and Identity in 6G



Post-Quantum Cryptography (PQC)

⚠ Critical Threat: "Store Now, Decrypt Later"

Adversaries are harvesting encrypted 5G traffic today to decrypt it once quantum computers become available (approx. 2030+). 6G must be quantum-safe from Day 1.

🔄 Migration Strategy

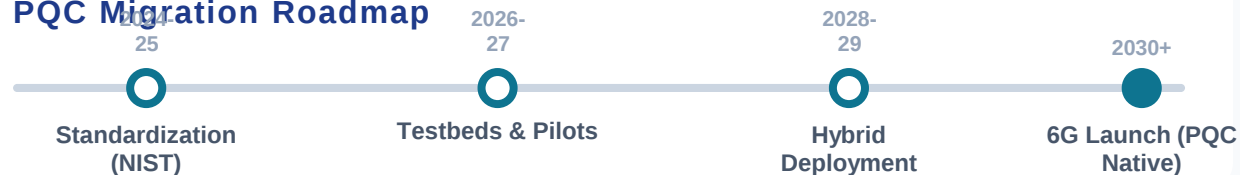
NIST PQC Selections: Kyber (KEM) for key exchange, Dilithium/Falcon for signatures.

Hybrid Cryptography: Combine classical (ECC) + PQC algorithms during transition to ensure safety against both classical and quantum attacks.

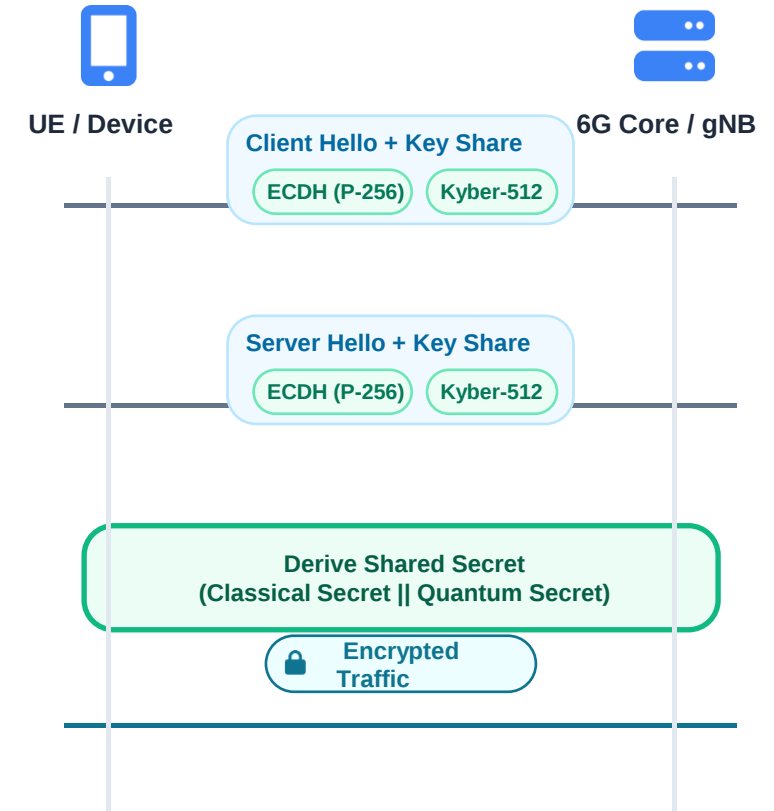
Crypto-Agility: Designing protocols (TLS, IKEv2) to negotiate algorithms and support rapid key rollover without hardware replacement.

PKI Impact: Upgrade to larger certificates/keys; budget for increased transmission overhead and processing time.

PQC Migration Roadmap

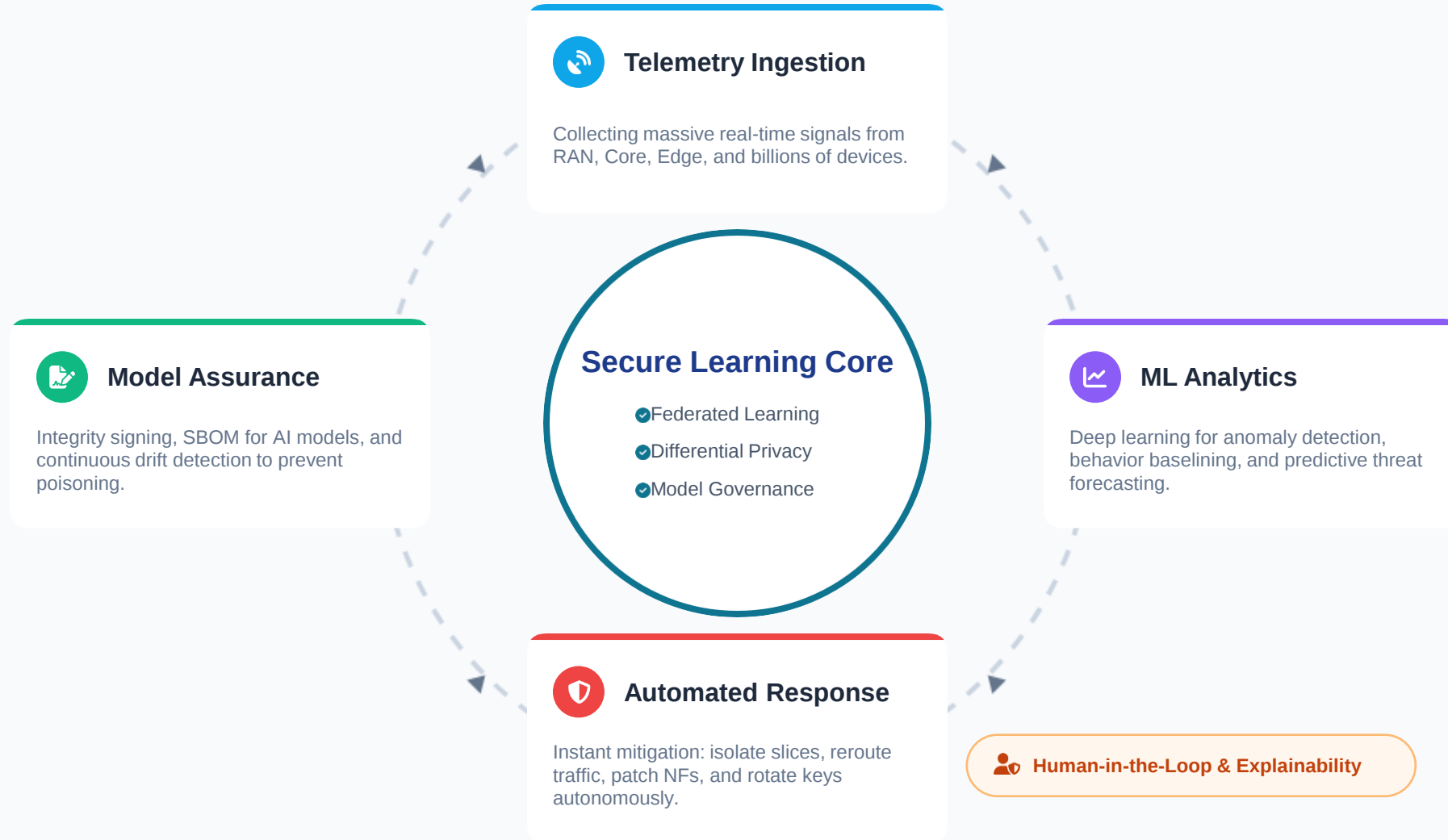


Hybrid Key Exchange (Concept)



Hybrid approach ensures security even if one algorithm is broken.

AI-Driven Security



Trust Framework & Privacy by Design

Compliance Overlays

 **GDPR / AI Act**

 **Sectoral Policy**

 **Data Sovereignty**

Consent Management

Fine-grained, machine-readable policies attached to user data. "Opt-in" defaults for sensitive sensing data.

Data Minimization

Collect only what is needed. Edge filtering ensures raw sensor streams don't leave the local domain unnecessarily.

Privacy Enhancement Engine

Privacy-Preserving Computation Layer



PETs

Differential Privacy & Anonymization



Homomorphic Enc.

Compute on Encrypted Data



Federated Learning

Local Training, Global Model



Zero-Knowledge

Proofs of Identity / Age

Data Lineage & Audit

Immutable logs (blockchain/ledger) tracking data access and policy enforcement trails for compliance.

Secure Sharing (CTI)

Cross-operator threat intelligence sharing using privacy-preserving aggregation to protect user identities.

● Privacy by Design

● Transparency & Control

● Accountability

● End-to-End Security

Testing, Validation & Standards Roadmap

6G Validation Testbed Architecture



Digital Twins

Protocol & Security
Simulation



AI Orchestration

Native Intelligence
Validation



NTN Integration

Satellite & UAV Links



PQC Pilots

Quantum-Safe algorithms



Industry Collaboration



3GPP SA3



O-RAN Alliance



6G-IA



Next G Alliance



GSMA



ETSI

Standardization & Deployment Milestones

2024-25



ITU IMT-2030

Framework & Vision
Definition

2026-27



3GPP Rel-20

Initial 6G Study Items (SI)

2028



PQC Standards

NIST Finalizes Algorithms

2029



3GPP Rel-21

First Full 6G Specs

2030+



Commercial Launch

Global 6G Deployment

Security is the Fabric, Not a Layer

We are building on 5G's robust foundation but extending trust into a new era of AI-native operations, post-quantum resilience, and zero-trust principles across every domain.



**Device &
Platform Trust**



**Secure RAN
& NTN**



**Zero-Trust
Core**



**AI-Native
Defense**



**Privacy &
Governance**

✓ End-to-End Trust

Extend identity-based security from silicon to satellite. Every packet, slice, and AI model must be verifiable in real-time.

👤 Privacy by Design

Embed PETs and fine-grained consent into the architecture to handle pervasive sensing data responsibly and securely.

🔧 Validation First

Use digital twins and open testbeds to stress-test PQC migration and AI resilience before deployment at scale.