Post-Quantum

Cryptography Conference

PQC in Mobile Networks: Insights from the GSMA Task Force

David Turkington
Head of Technology APAC at GSMA

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKI Consortium

GSMA™

GSMA Post Quantum Teleco Network – Task Force

Background and Update

David Turkington
Head of Technology
GSMA

GSMA

“If you have nothing to hide, you have nothing.”

GSMA™

The USIM Card

SIM cards use symmetric encryption – they keys are stored securely in the SIM and the network (HLR, HSS, UDM)

eSIM are the software in the SIM that can be downloaded securely to the phone eUICC

Pros
Secure key exchange in physical hardware

Cons
Needs slot in device (esp. IoT devices)

Distribution of physical cards e.g distribution across the 1000's of islands in APAC

If device stolen – SIM can still be used.

Pros
Instant activation with appropriate device phone – no logistics

First enabling the devices need PKI to trust each other. TLS used.

(Some) Differences between 4G and 5G

4G

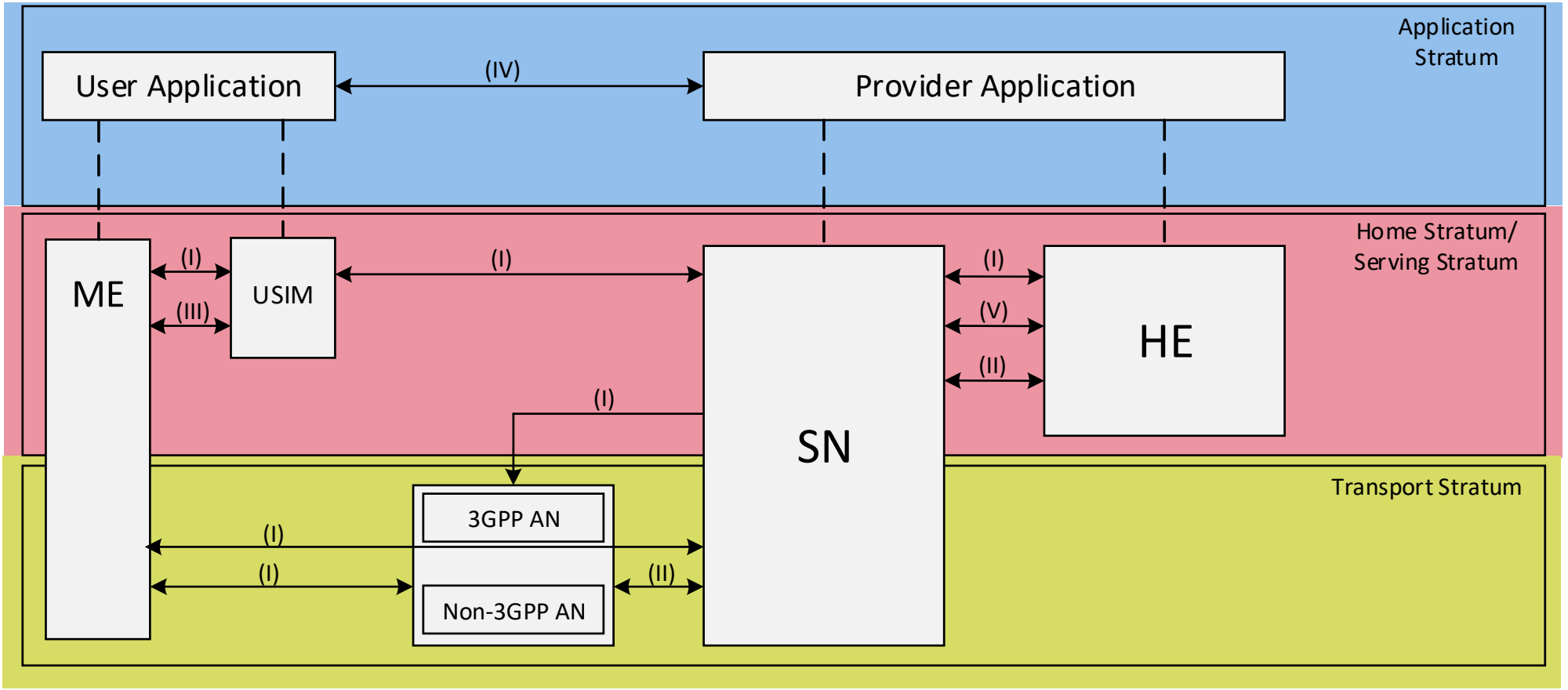
- Core network components typically bespoke hardware (separate box for each function)
- Network functions integrated
- Vendor controlled
- Traffic through well defined paths

5G

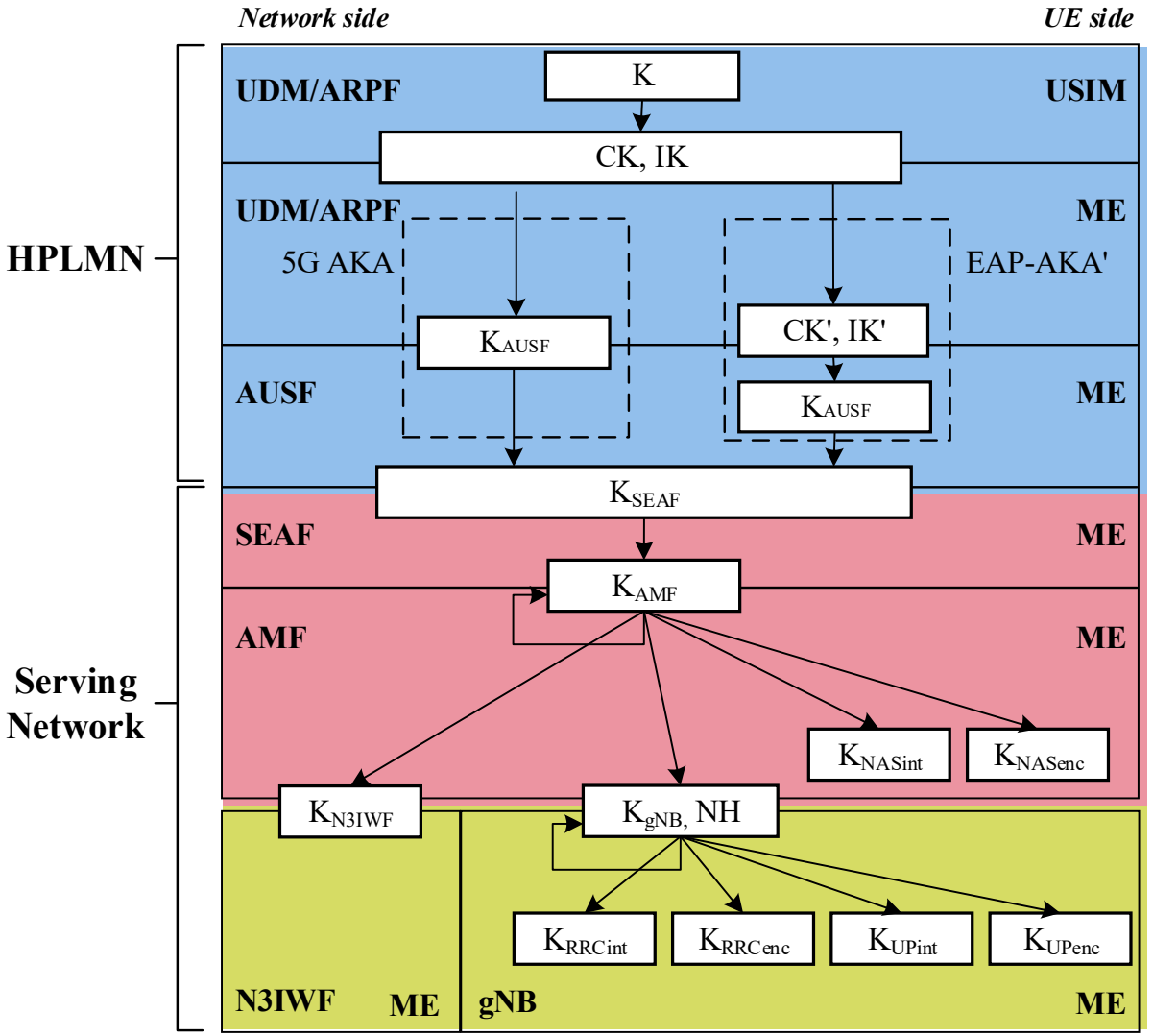
- Designed for virtualization, software defined, distributed infrastructure
- Deployed public and Private clouds
- More flexible
- Wider attack surface
- Interfaces open. Traffic between components in the cloud

3GPP TS 33.501 Security architecture and procedures for 5G system (345 pages)

5G core is disaggregated – can be running across private and public clouds



3GPP TS 33.501 Key Hierarchy

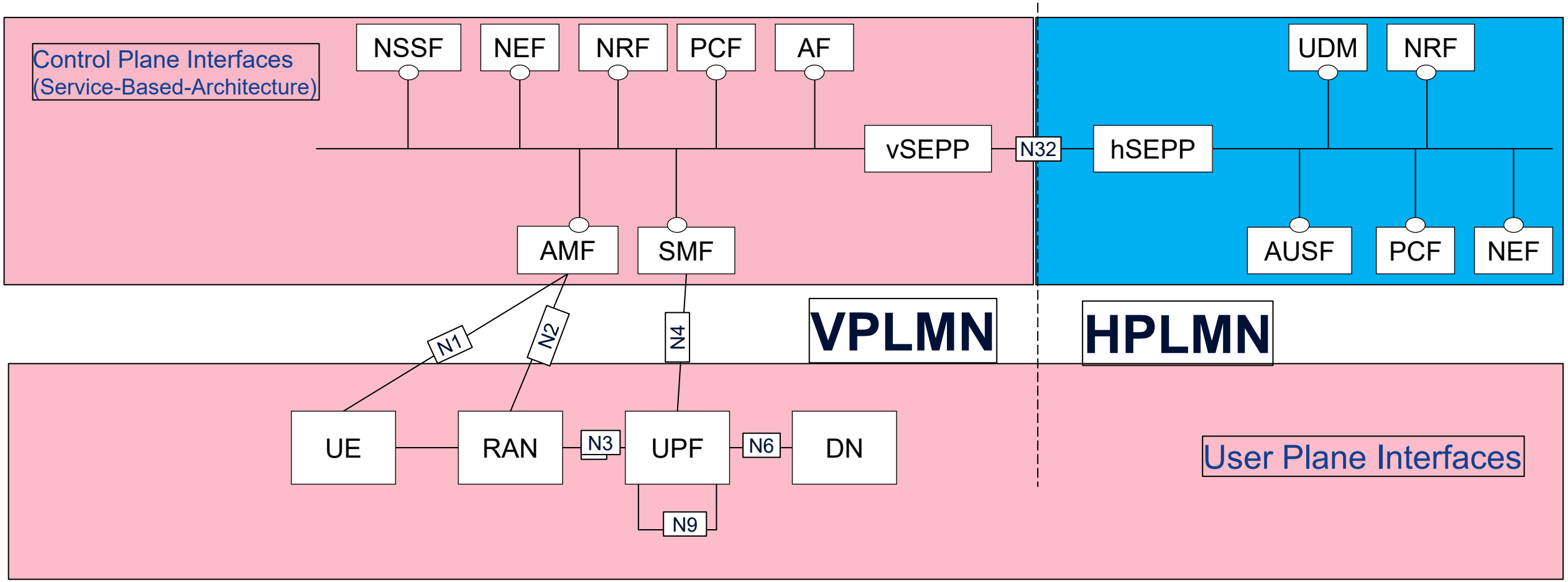


In the USIM:

K – secret symettric key (also in UDM)
SUPI – subsciber permanent identity
MNO name
MNO Public key
Routing info

SUPI encrypted [concealed] into SUCI (with home network public key)
the SUCI is used for initial Authentication – so SUPI never sent in clear. (not like in 4G)

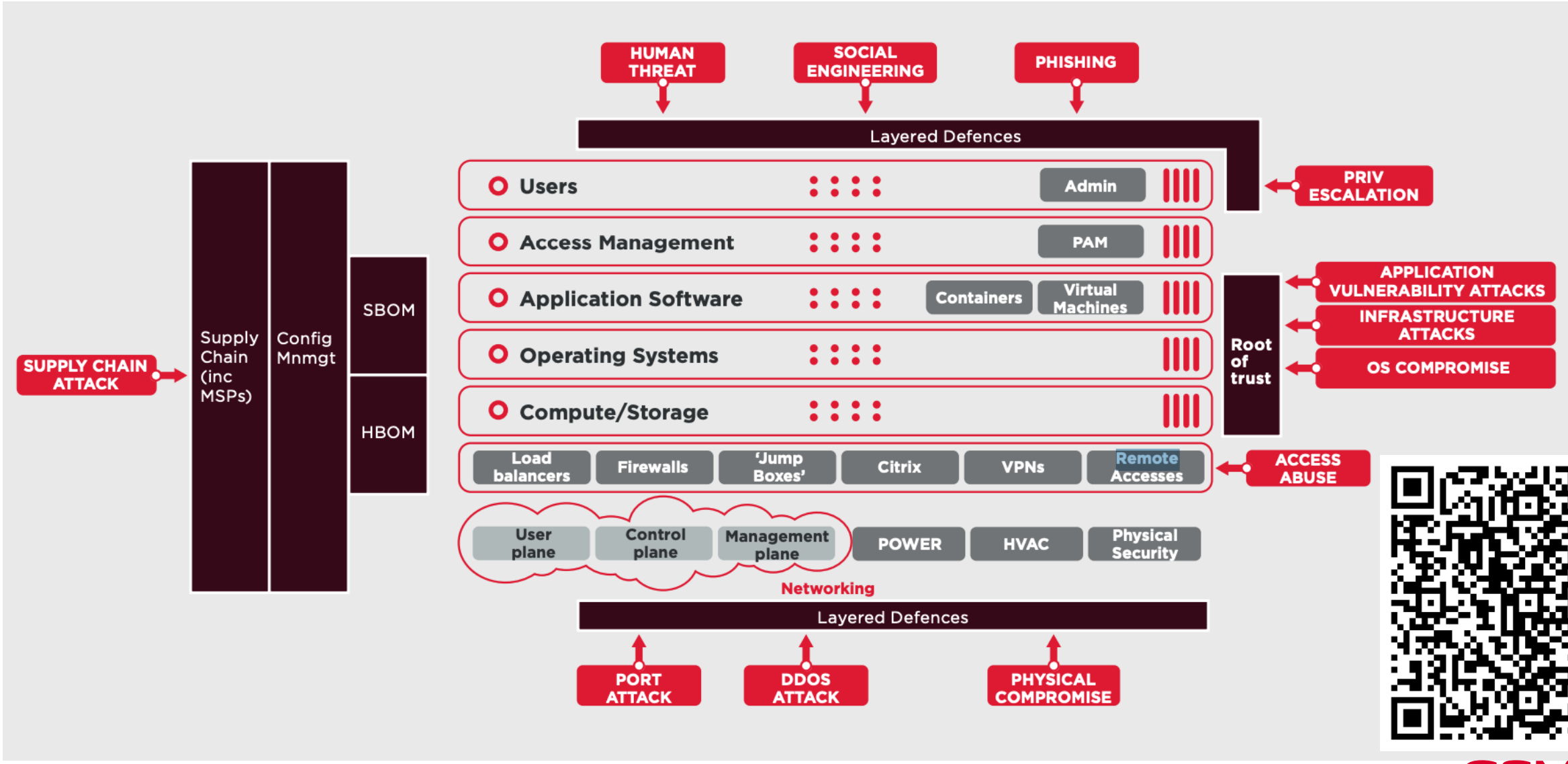
5G Network - Service Based Architecture (SBA)



VPLMN – visited public land mobile network, HPLM- Home public land mobile network

GSMA

Defence and Attack Vectors – Landscape Report



Lots of encryption used in Mobile

Features	4G	5G
Authentication Protocol	Uses EPS-AKA with symmetric keys	Multiple methods, unified framework
Identity Protection	Permanent ID sent in clear text	Permanent ID always encrypted
Network Architecture	Centralized core network	Service-based, modular core
Encryption Strength	AES with 128-bit keys	AES with 256-bit keys
Privacy Measures	Temporary IDs with flaws	Temporary IDs change each session
Network Slicing	Not supported	Supports isolated virtual networks
Vulnerability Risks	Legacy flaws, IMSI catchers	New API risks, IoT threats
User Impact	Higher risk of tracking	Better privacy and protection
Transition Security	Susceptible to downgrade attacks	Stronger but mixed risks remain

Example of Encryption Downgrade - SMS Blasters

What is is ? How Does it work?

SMS Blaster is a fake base station configured to transmit like real BS

- Select the fake base station (strong local signal)
- Force the mobile to downgrade security by selecting 2G signal
  - 2G does not have network authentication – so the mobile doesn't realize it's fake.
- Send a signaling message to the mobile
  - This is done independent to the 'real' network
- Very difficult to detect
  - It happens on downlink frequencies that are not monitored by the network.
  - The signals are usually localized – so even drive testing might not find them

GSMA

SMS Blaster – How it works…

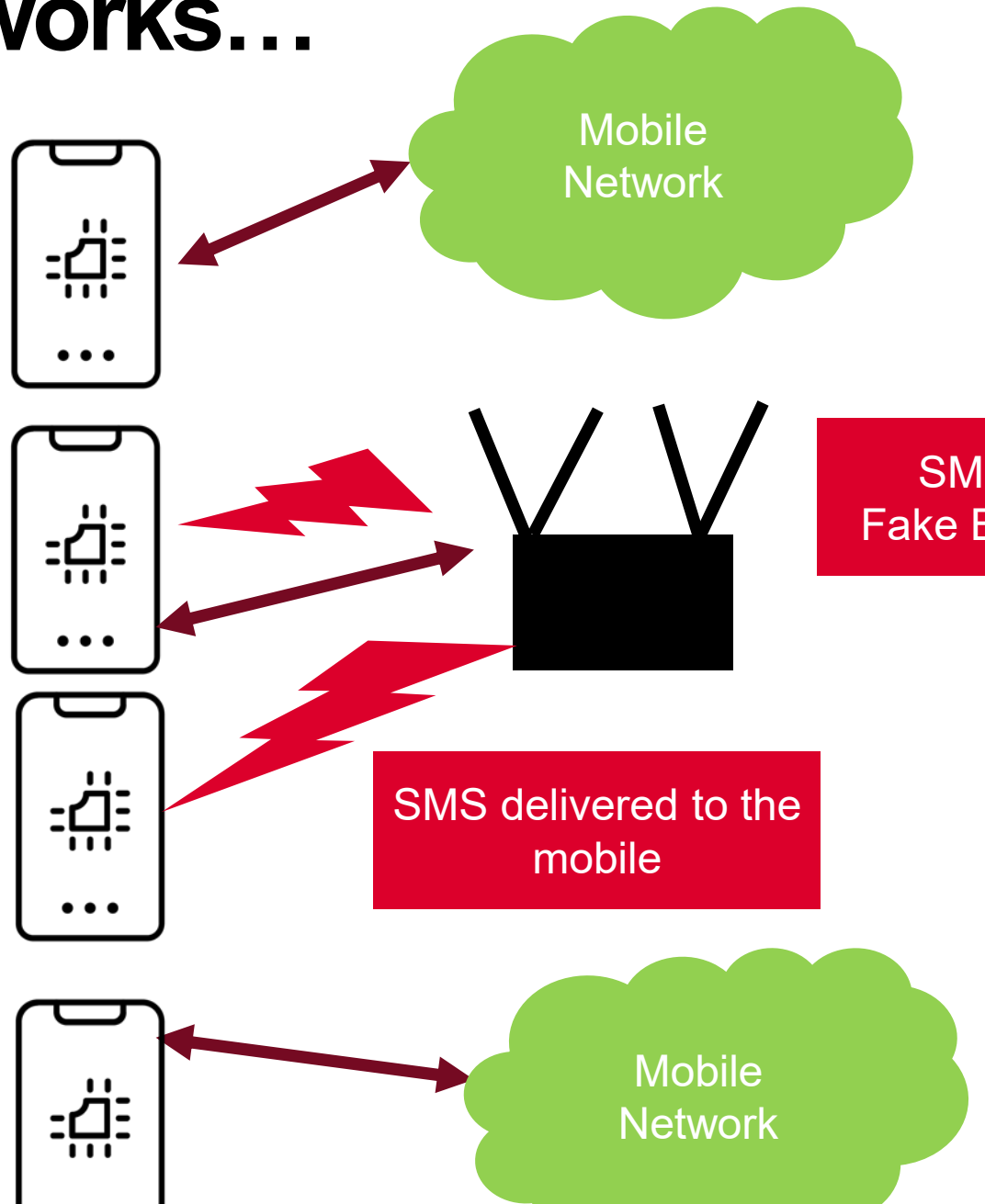
Step by step

Mobile connected to Network

Strong local 4G/5G signal captures the mobile

Forced to 2G (weaker encryption – no network authentication)

Mobile released back to Network



SMS Blaster Messages

Where did that come from?

- Messages have not been sent using the home network
  - No logs, no record of them, no traces, no signaling to monitor the contents
- SMS Blaster operator promote avoiding fees for marketing messages
  - Alternative to internation A2P SMS

- SMS Blasters seem readily available – with several configurations
  - Law enforcement (Stingray) , IMSI catcher, multi band, multi operator
  - Some sort-of legitimate use cases (prisons, police interception)

GSMA

SMS Blaster

Easy to get

SMS BROADCASTER 4G LTE & 5G NSA

The Most Effective and Revolutionary technology Broadcaster SMS engine that working with ALL 4G/LTE Frequencies (Band1, Band3, Band5, Band8, Band34, Band39, Band40, and Band41), and also Support with 5G NSA frequencies. Its Sending to 4 Operators simultaneously working on all 4G Frequencies and 5G NSA Frequencies and Supported SenderName, and able to add up to 40 Operators and working automatically to maximize the delivery of your messages to the public.

Learn more

66%

SS7 - Global Title and Global Title Leasing?

The addressing system of telecoms networks

- SS7 was the original internetwork signalling system and was extended for mobile network use.
- A Global Title (GT) looks like a phone number and is used to identify and communicate with certain nodes within a telecommunications network –(a bit like an IP addresses is in an IT network)
- In mobile networks, a GT is used, to support the exchange of SMS and to enable 2G, 3G and even 4G roaming, roaming traffic steering and other things.
- Some operators made part of their GT number ranges available for use for rent. These were sometime sub-leased and so the original GT owner was not aware of the uses – e.g. bulk SMS sending or more nefarious actions
- But then serious flaws (or features?) in SS7 meant that the inter-network signalling network could be used to intercept/redirect calls and SMS and locate users.

Global Title (GT) Leasing

- GT leasing enables entities to buy access the global SS7 signalling network and exchange signalling messages using network addresses (GTs) associated with the GT owner.
- The loss of transparency introduces security risks for mobile network operators and their customers.
- Example companies provide bulk A2P SMS and perhaps other dubious services operating in a grey area.


HAARETZ LOG IN

Flag March | Temple Mount/Al-Aqsa | Israel - Settlements | Elon Musk | Netanyahu | Russia Prisoners | Gaza - Israel | Lipstadt | Israel's judicial overhaul

How a Secretive Swiss Dealer Is Enabling Israeli Spy Firms

The international mobile system is exposed and a loophole allows hackers, cybercriminals and states to geolocate targets and even hijack email and web accounts. Israelis can be found among the victims - and the attackers

https://www.haaretz.com/israel-news/security-aviation/2023-05-14/ty-article- magazine/.highlight/global-surveillance-the-secretive-swiss-dealer-enabling-israeli-spy- firms/00000188-0005-dc7e-a3fe-22cdf2900000

GSMA Post Quantum Telco Network Task Force

60+ Companies
100+ Participants

Network Operators across all regions

Technology Providers from across the ecosystem

Government and Regulators

Collaboration and communication

- Raise awareness of the quantum threat and what it means for the telecommunications sector
- Cooperation and coordination with industry and standardisation bodies
- Liaise with relevant government organisations

Work Items and Deliverables

- Foster ecosystem collaboration to address the challenges around implementation of post quantum cryptography and crypto agility in the telecommunication industry and beyond
- Publication of whitepapers, guidelines and information with a view of providing practical support to organisations and individuals that are involved in the quantum safe and crypto-agility process

PoC and testing

- Platform for executing demos and trials
- Knowledge, best practice sharing and lessons learnt

GSMA

Post Quantum Telco Network Group – Industry Collaboration

60+ Members

Telco operators | Technology providers | Regulators | Governments

GSMA

PQTN: Government Initiatives

A multi-country overview of published government guidance, highlighting the *increased momentum and activities in progress globally*

Given this is a rapidly evolving area for governments globally, ongoing monitoring *will be required to ensure consistency with strategic plans and roadmaps for telco*

https://www.gsma.com/newsroom/post-quantum-government-initiatives-by-country-and-region/

GSMA

PQTN: Government Initiatives

Country	PQC Algorithms Under Consideration		Timeline (summary)
Australia	NIST		Complete transition to quantum resistant cryptography by 2030.
Canada	NIST		Start planning and inventory. Introduce standards-based PQC from 2025-26. CSE is updating detailed PQC guidance.
China	China Specific		Start Planning PQC algorithm program.
Czech Republic	NIST (but not restricted to)		Migrate by 2027 (key establishment, encryption). As soon as possible for firmware & software signing.
European Union	NIST Plan to select PQC EU algorithms		Start planning Define a coordinated PQC roadmap for Member States by 2026. Actions for financial services
France	NIST (but not restricted to)		Start planning; Transition from 2024
Germany	NIST (but not restricted to)		Start planning
Israel			Start planning, create cryptographic inventory. Add PQC to contracts. Requirement for financial services firms to manage quantum risk, develop inventory and initial plan
Italy	NIST		
Japan	Monitoring NIST		Start planning; initial timeline. CRYPTREC is preparing detailed PQC guidelines.
Netherlands	ML-KEM, Classic McEliece and FrodoKEM recommended in hybrid mode for TLS.		Draft action plan with timeframes
New Zealand	NIST		Start planning. Transition from 2026-27.
Singapore	Monitoring NIST		No timeline available. Financial services firms required to prepare plan.
South Korea	KPQC signatures: AIMer, HAETAE. KPQC KEM: SMAUG-T and NTRU+.		PQC algorithms selected PQC Roadmap for completion 2035 Pilot transition plan 2025-2028.
Spain	NIST and FrodoKEM.		Four phase approach today to post-2030.
United Kingdom	NIST		Start planning; cryptographic discovery; use only standards in production. NCSC is preparing detailed PQC guidance.
United States	NIST		Implement 2023-2033

PQTN TF Publications

September 2022

PQTN TF *formed*

February 2023

1st Post Quantum *Seminar Barcelona*

Telco Impact *Assessment Whitepaper*

September 2023

2nd Post Quantum *Seminar Las Vegas*

Guidelines for Quantum Risk *Assessment*

February 2024

3rd Post Quantum *Seminar Barcelona*

Post Quantum Cryptography *Telco Use Cases Guidelines*

May 2024

4th Post Quantum *Seminar Singapore*

August 2024

Blog: NIST Release 3 Post Quantum Algorithms

October 2024

5th Post Quantum *Seminar Las Vegas*

Post Quantum Cryptography *Migration Plan*

March 2025

6th Post Quantum *Seminar Barcelona*

Post Quantum Cryptography in IoT

What are the risks for Telco Operators?

Telco Operator Risks

Store Now, Decrypt Later	Copy/store high-value data (e.g. financial, bioinformatic, confidential), with the goal to decrypt later.
Code-signing and Digital signatures	Software update authentication can become vulnerable given reliance on PKI.
Rewriting History	Digital timestamps for high-value targets (e.g. contracts) could be attacked.
Key Management Attacks	Long-term data storage is vulnerable by attacking the wrapping mechanisms used for keys.

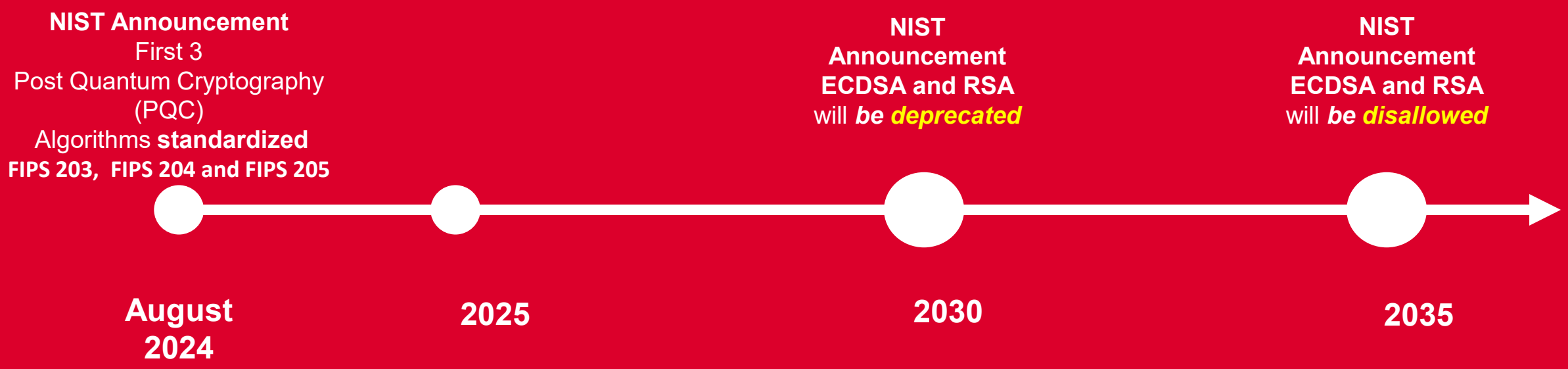
Telco Ecosystem

- SD-WAN services
- Base station to security gateway link
- Operator e-commerce portals
- SIM cards, eSIM provisioning
- IoT / Consumer devices

Customers

- Breach of privacy
- Reputational damage
- Network disruption

Post Quantum Cryptography - NIST Timelines



GSMA

Quantum Computing Migration – Telco Challenges

Key Management

Larger key sizes are required

Performance

Require more computational resources

Interoperability

Ensure the interoperability between Network Functions, Applications, and interfaces

© GSMA 2025

Quantum Computing Migration – Key Recommendations

Following the PQC standardization process

Preparing your organization for the quantum threat to cryptography

Test PQC Hardware and Software for standardization PQC algorithms

Address gaps between theoretical possibilities offered by PQC and its implementations

Identity critical assets affected by Quantum Computers attacks to prioritize

Early adopters are likely to implement PQC for critical networks

Join Us

Yolanda Sanz, Head of Working Groups
ysanz@gsma.com

Lory Thorpe, PQTN Task Force Chair
lory.thorpe@ibm.com

Luke Ibbetson, PQTN Task Force Deputy Chair
luke.ibbetson@vodafone.com

https://www.gsma.com/solutions-and-impact/technologies/security/post-quantum-telco-network-task-force/

GSMA