GSMA

HOSTED AT MWC GSMA

MWC Shanghai Roundtable

The Future of Telco Security: Post Quantum Cryptography Use Cases in Action

Wednesday, 24 June I 14:00 – 16:00 CST
Tower Function Room 11, Kerry Hotel

Agenda:

MWC GSMA | 上海 · SHANGHAI 2026年6月24–26日 24–26 JUNE 2026

Timing	Presentation/Demo Title	Presenter	Company
2:00 pm	Welcome and Introduction	**Yolanda Sanz**, Head of Working Groups	**GSMA**
2:00 – 2:20 pm	Is IoT ready for Quantum?	**Tim Hatt**, Head of Research and Consulting	**GSMA Intelligence**
2:20 – 2:40 pm	Post-Quantum Cryptography for Automotive (PQC4Auto)	**Maxime Flament**, CTO	**5GAA**
2:40 – 3:10 pm	Quantum-safe pre-SGP.42 In-Factory Profile Provisioning (IFPP)	**Alex CHAN (Chiou Nan)**, Vice President **Richard Mao**, Product Manager **Onur Kasaba**, Managing Director	**Idemia** **Quectel** **Tele2 IoT**
3:10 – 3:40 pm	Enabling Multiple key exchanges on post-quantum IPsec protocol	**Lun Li**, Senior Engineer	**Huawei**
3:40 – 4:00 pm	**PQC Activities within GSMA**: PQTN TF Update	**Yolanda Sanz**, Head of Working Groups	**GSMA**

MWC GSMA

上海 · SHANGHAI
2026年6月24－26日
24－26 JUNE 2026

Welcome and Introduction

Yolanda Sanz

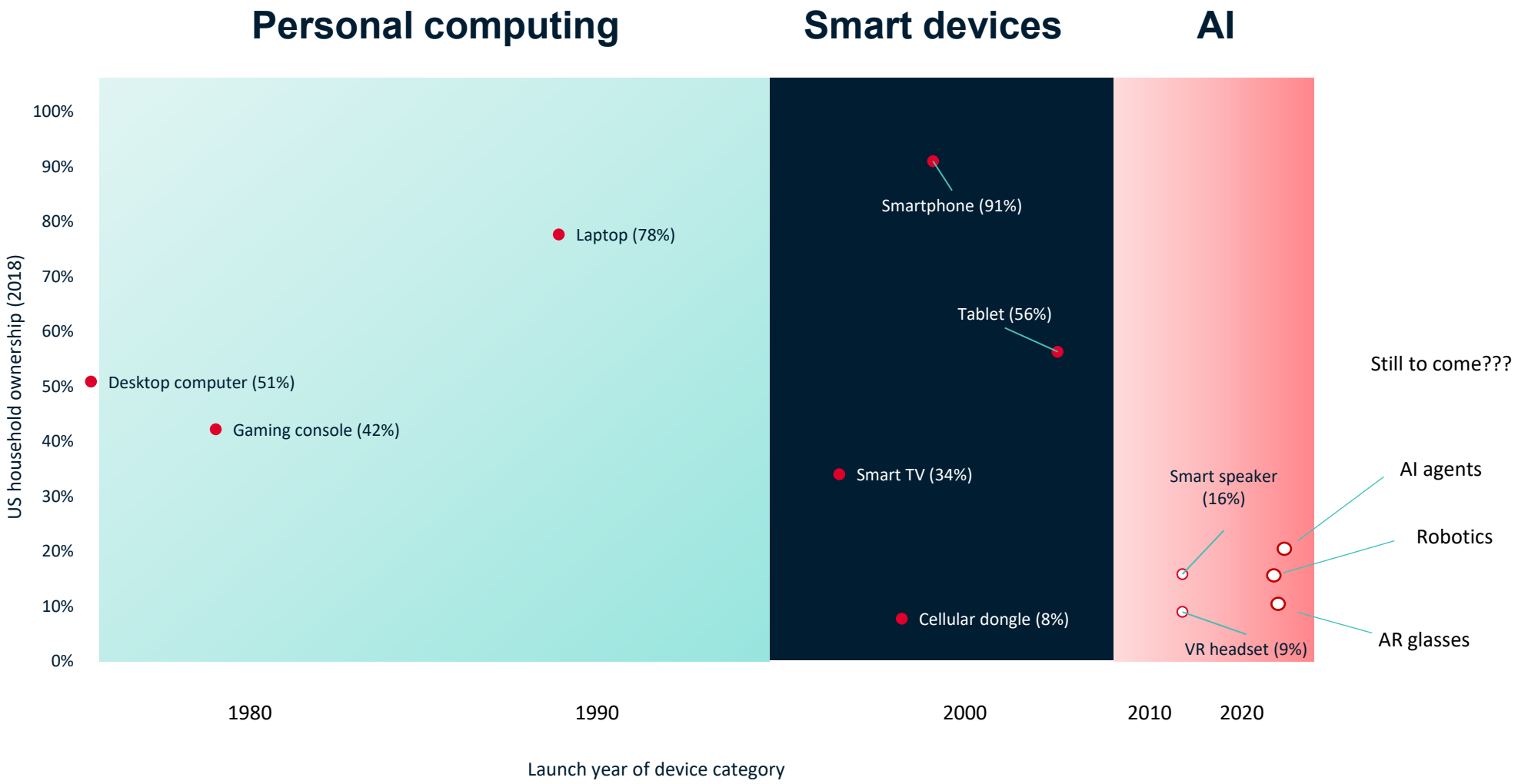
Head of Working Groups, GSMA

MWC GSMA
上海 · SHANGHAI
2026年6月24－26日
24－26 JUNE 2026

Is IoT ready for Quantum?

Tim Hatt
GSMA Intelligence, Head Of Research & Consulting, GSMA

AI shows us innovation cycles are shortening



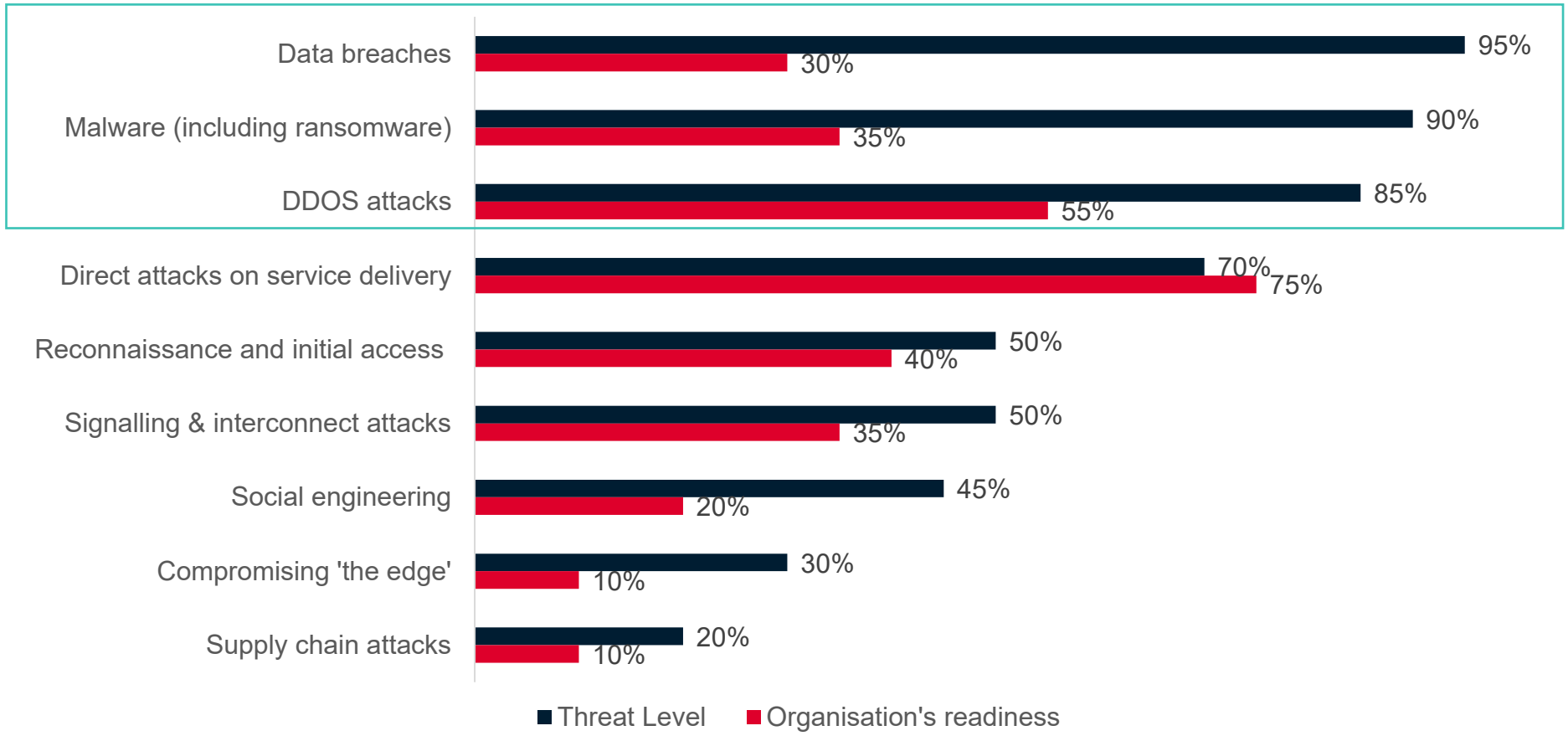
- New tech era
- Devices + services = higher compute workloads
- Wider attack surface = wider range of threats

Source: GSMA Intelligence

GSMA Intelligence

Security threats expanding and moving further out

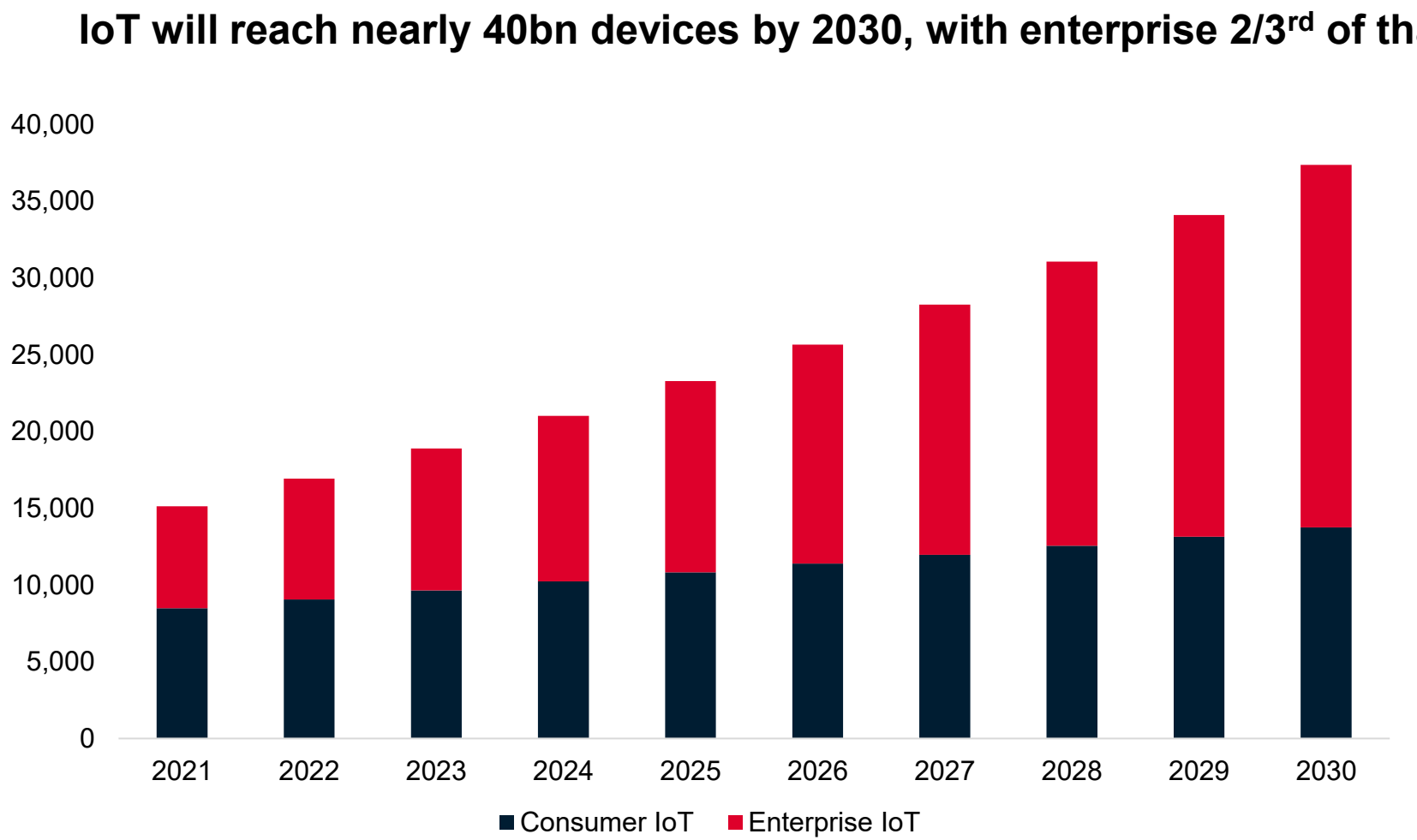
Telco perception of threats vs. readiness to defend against them



Source: GSMA Intelligence Security Survey 2025

GSMA Intelligence

IoT = large, distributed…and vulnerable



Source: GSMA Intelligence

GSMA Intelligence

Quantum readiness works along a spectrum

	Upgrade and lifecycle	Performance	Algorithms (public vs. PQC)
Quantum readiness (qual)			
None	• Mostly longer lifecycle devices requiring physical swap-outs to upgrade security systems (i.e. can't be done via SW over the air) • Typical in sectors with legacy IoT (e.g. weather sensors, some telematics)	• Devices with low RAM memory (e.g. 8-64 kb in IoT vs. 6-8 GB in latest smartphone models) • Clock processing speeds (e.g. 8-20 MHz for lower end IoT and 100-300 MHz for higher end vs. GHz level speeds for smartphones, e.g. iPhone 17 using A19 pro processor at 4.26 GHz)	• Relies mostly on public cryptographic standards (e.g. RSA, ECC)
Partial	• Split between legacy and newer IoT capable of OTA security upgrades	• Mixed	• Mix of public and PCQ • May use hybrid approach (e.g. public cryptography for digital signature and PQC algorithms for verification)
Full	• Substantially all devices capable of OTA security upgrades	• Devices with high RAM memory (e.g. applications at the edge like drones, VR headsets, AR glasses, industrial robotics and AGVs - may reach 2-8 GB, bringing closer to smartphone-level specs)	• Substantially all PCQ for both digital signatures and key verification

Source: GSMA Intelligence

Measuring quantum readiness

- Multiple factors (device age, performance capabilities, encryption)
- Some matter more than others
- Know your assets

Category		Weighting (sum = 1)	PQC readiness
Device age (years)		30%	
	5+		None
	2–5		Partial
	<2		Full
Performance specs	RAM	20%	
	<64 kb		None
	64–512 kb		Partial
	>512 kb		Full
	Clock speed	20%	
	<24 MHz		None
	25–100 MHz		Partial
	>100 MHz		Full
Encryption model		30%	
	Public (e.g. RSA, ECC)		None
	Hybrid		Partial
	PQC		Full

Source: GSMA Intelligence

GSMA Intelligence

Only 7% of IoT devices are (currently) quantum ready

Quantum readiness	Smart home	Automotive	Energy and utilities	Retail	Healthcare	IoT overall
Share of devices						
None	76%	76%	75%	74%	78%	75%
Partial	16%	16%	21%	22%	19%	18%
Full	9%	9%	5%	8%	7%	8%
Number of devices (million)						
None	3,079	673	1,766	489	416	18,103
Partial	632	138	486	146	102	4,325
Full	367	80	119	50	35	1,842
Total IoT device base (active use, million, 2025)						
	4,079	892	2,370	665	537	24,030

- Readiness <10% on average (=billions of exposed IoT assets)
- Biggest exposure risk: homes, energy, cars
- Retrofits vs. pre-emptive planning

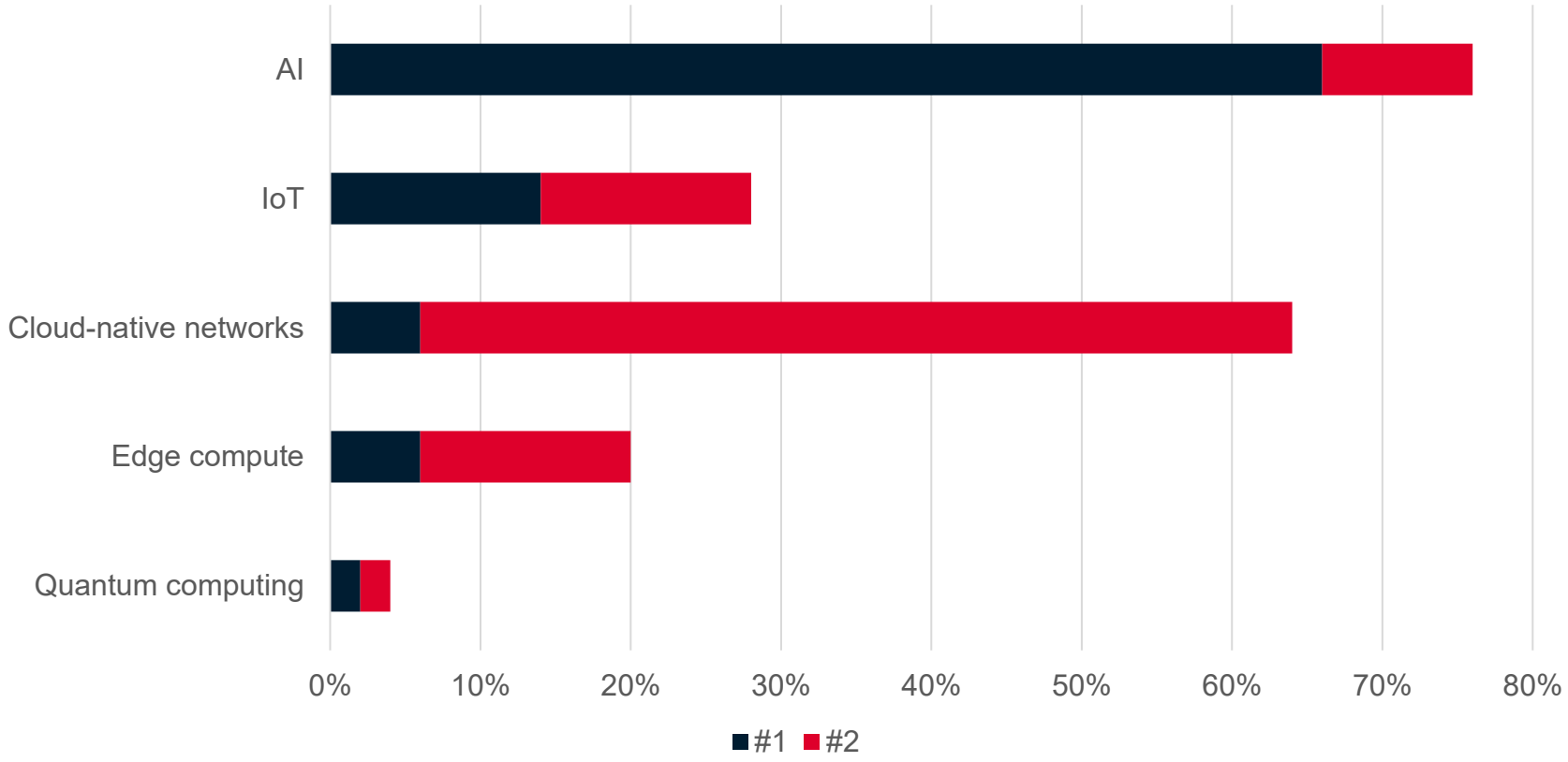
Source: GSMA Intelligence

GSMA Intelligence

This means quantum is a blind spot

- AI = double edged sword
- Cloud = widened attack surface + lack of control
- Quantum = blind spot
- Pays to act now vs. later

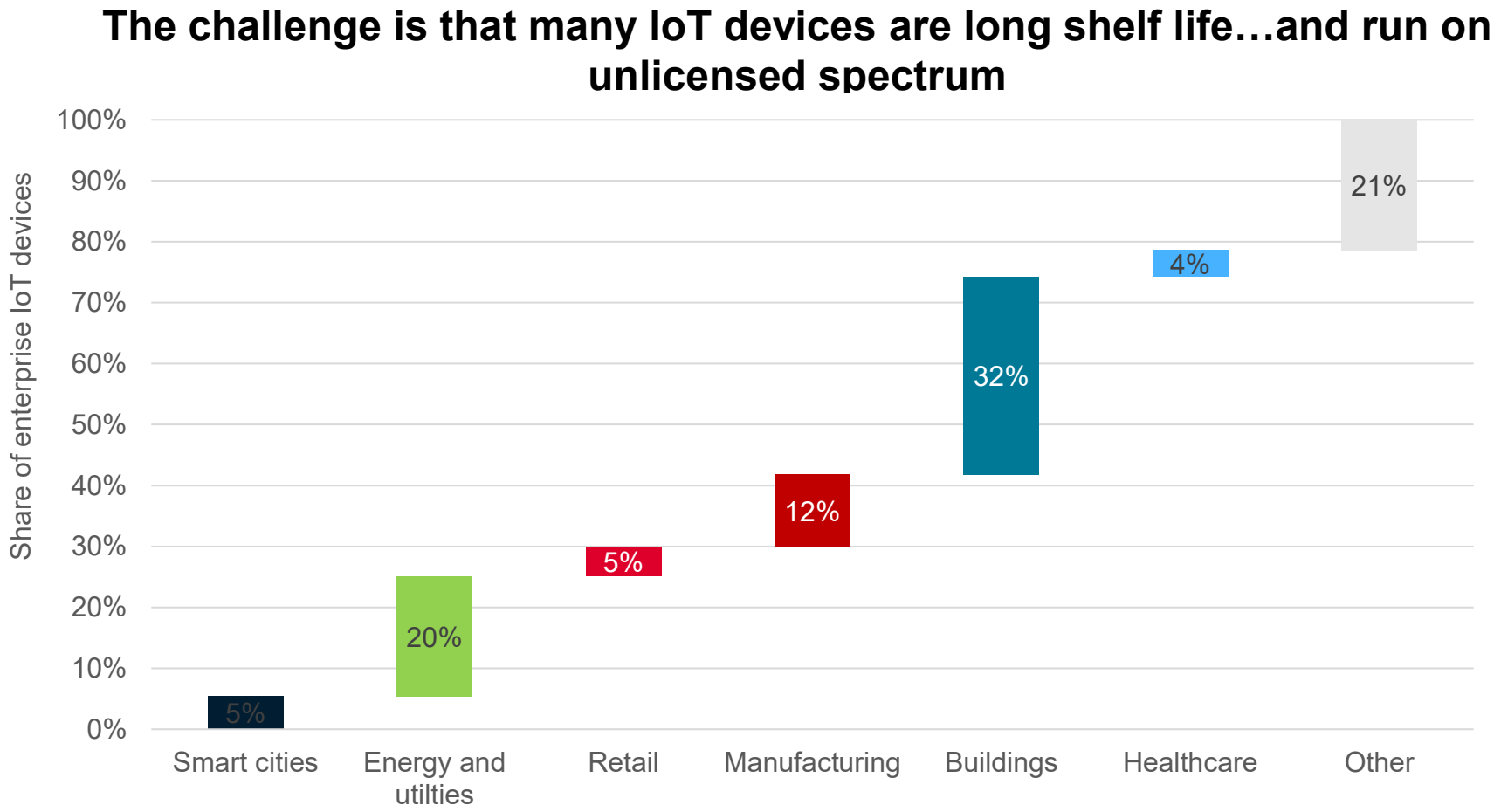
Which emerging technologies do you expect to have the greatest impact on your organisation's security strategy over the next 2 years?



Source: GSMA Intelligence Security Survey 2025

GSMA Intelligence

How to retrofit vulnerable devices?



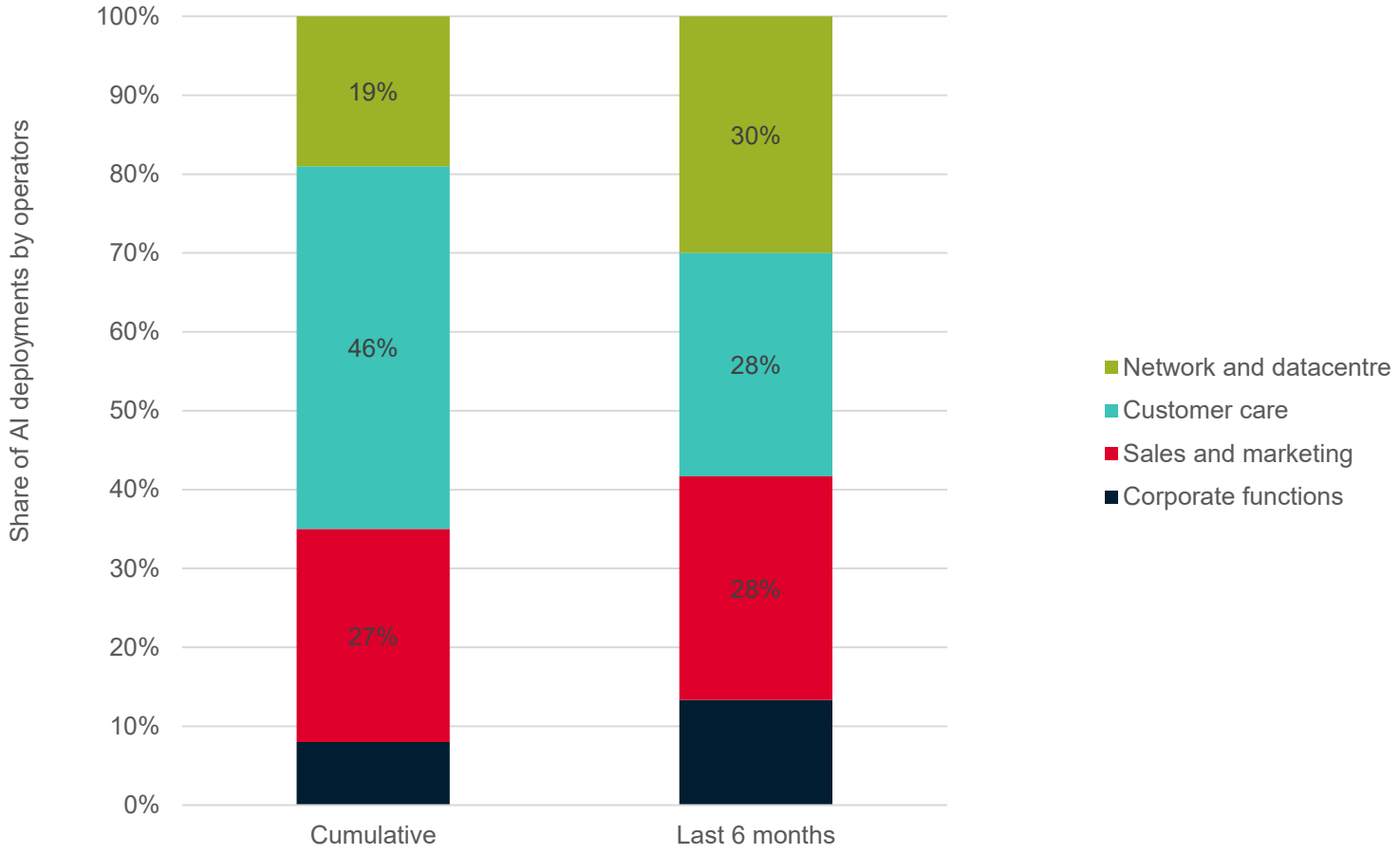
Source: GSMA Intelligence

GSMA Intelligence

Distributed AI pushes compute to edge, widening perimeter

- Branching out
- What's to come?
  - Continued efficiency gains (e.g. customer care)
  - Inference
  - AI factories
- Plug the USP
  - Distributing traffic to the edge
  - Sovereignty
  - Resiliency
  - Cost savings

Telcos are moving beyond the early wins for AI in customer care to support monetizing network assets



Source: GSMA Intelligence

GSMA Intelligence

GSMA Intelligence
Who are we? What do we know?

GSMA Intelligence is the definitive source of mobile industry insights, forecasts, and research, used around the world. Our insights cover every mobile operator, network, and MVNO in every country worldwide.

COMPREHENSIVE DATA PLATFORM | **INSIGHTFUL RESEARCH** | **EXPERT ANALYSIS** | **BESPOKE CONSULTING** | **EVENT SUPPORT**

Who we work with

Mobile Network Operators
Regulatory Bodies
Government Departments
Financial Corporations
Cybersecurity Firms
OEMs and Manufacturers
Technology Companies
Consulting Businesses

BY THE NUMBERS

7/10

of Forbes' Top digital companies worldwide, rely on our data and insights

50m+

individual datapoints covering everything from operational to economic

4,600+

networks tracked, spanning every country

9/10

of the top Telecoms in the world work with GSMA Intelligence

Thank you!

Tim Hatt. Head of Research and Consulting, GSMA Intelligence

thatt@gsma.com

GSMA Intelligence

MWC GSMA
上海 · SHANGHAI
2026年6月24–26日
24–26 JUNE 2026

Q&A

MWC GSMA

上海 · SHANGHAI
2026年6月24–26日
24–26 JUNE 2026

Post-Quantum Cryptography for Automotive (PQC4Auto)

Maxime Flament
5GAA, CTO

Post-Quantum Cryptography for Automotive (PQC4Auto)

5GAA Impact Assessment &
Automotive Industry Perspective

Maxime Flament, 5GAA CTO

Driving the Future of Connected Mobility Solutions Together

5GAA unites the automotive, telecommunication, and technology industries globally, turning collaboration into real-world, scalable connectivity solutions that deliver smart, safe, secure, and efficient mobility for all road users, now and in the future.

AUTOMOTIVE INDUSTRY

Vehicle Platform, Hardware and Software Solutions

TELECOMMUNICATIONS

Connectivity and Networking Systems, Devices & Technologies

5GAA – a global cross industry association

10 of the top 15 OEMs

8 of the top 10 MNOs

2 top smartphone vendors

Today, 5GAA unites +**100 members** from around the world working together on all aspects of C-V2X

In September 2016, **8 companies** teamed to create the 5G Automotive Association (5GAA) to help develop, test, and promote 5G standards

SEPT 2016

Q2 2026

Joint collaboration GSMA and 5GAA

Guiding the telecommunications and automotive industries in the transition to post-quantum cryptography.

GSMA™

Post Quantum Telco Network Task force

5GAA Automotive Association

Executive Takeaways

- Quantum computing will break current public-key cryptography
- Connected vehicles are exposed (direct and network V2X – PC5/Uu)
- Transition is inevitable but complex
- Requires coordinated and phased industry approach

Why PQC Matters

RSA and ECC become vulnerable with quantum computing

Risks include loss of trust, security breaches, and data exposure

‘Harvest now, decrypt later’ already relevant

Automotive-Specific Challenges

Long vehicle lifecycle (10–15+ years)

Safety-critical and heterogeneous systems

Strict latency, compute, and availability constraints

What is Post-Quantum Cryptography (PQC)?

- New cryptographic algorithms designed to resist quantum attacks
- Replace vulnerable public-key cryptography (RSA, ECC)
- Based on new mathematical problems (e.g. lattice, code-based)
- Standardisation led by NIST (ML-KEM, ML-DSA, etc.)

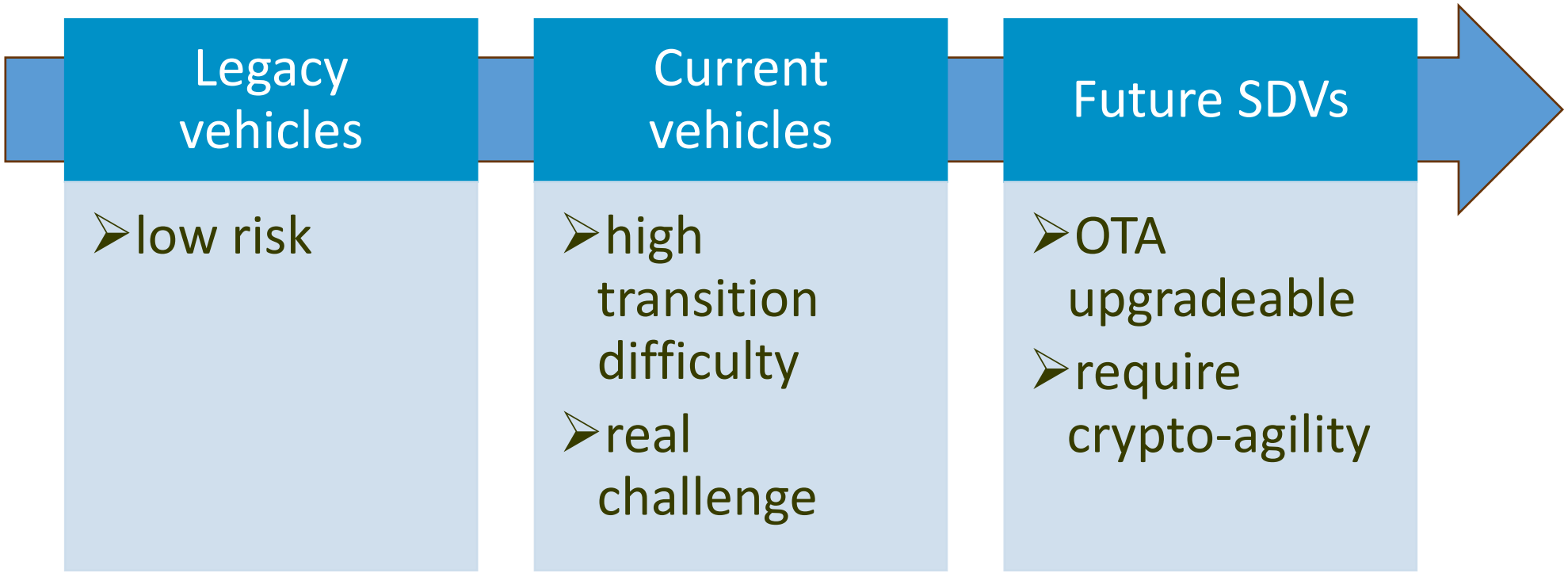
PQC vs Current Cryptography (Key Difference)

- Symmetric cryptography (e.g. AES) → remains largely secure
- Asymmetric cryptography → **must be replaced**
- PQC = not always “drop-in replacement”

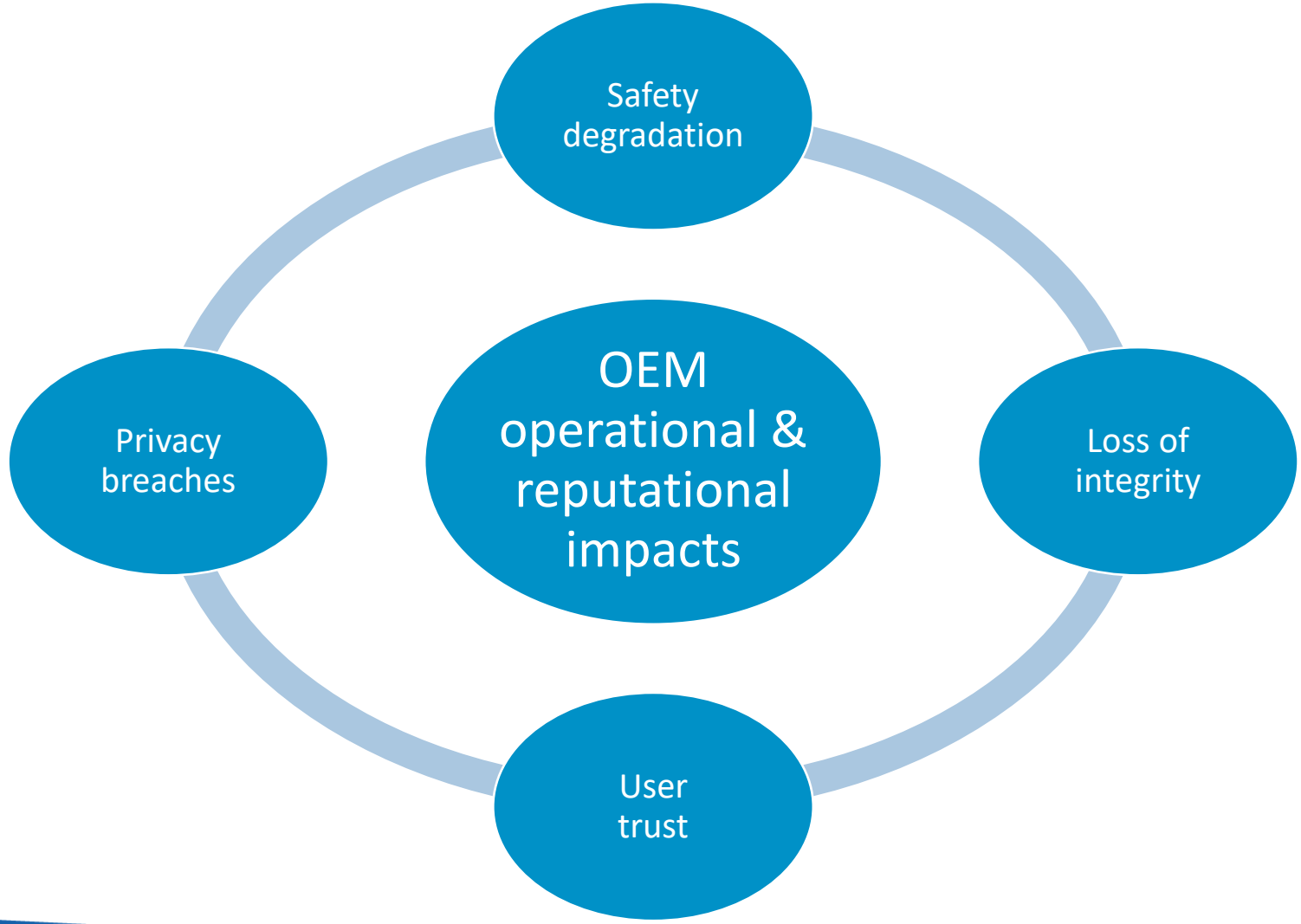
Impacted Use Cases

- V2X safety messaging
- Telematics and backend communication
- OTA / SDV services
- Digital key, payments, charging

Three Vehicle Generations



Key Risks for the Automotive Industry



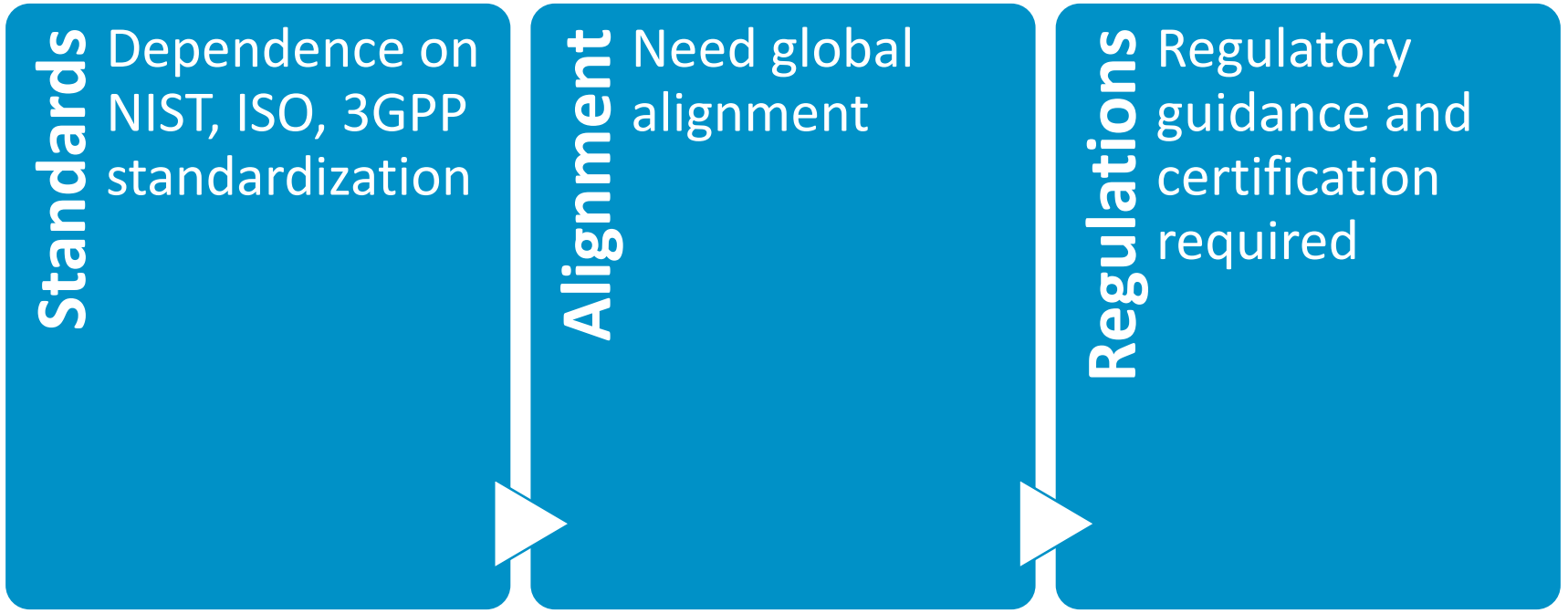
Ecosystem Implications

Requires coordination across OEMs, suppliers, MNOs

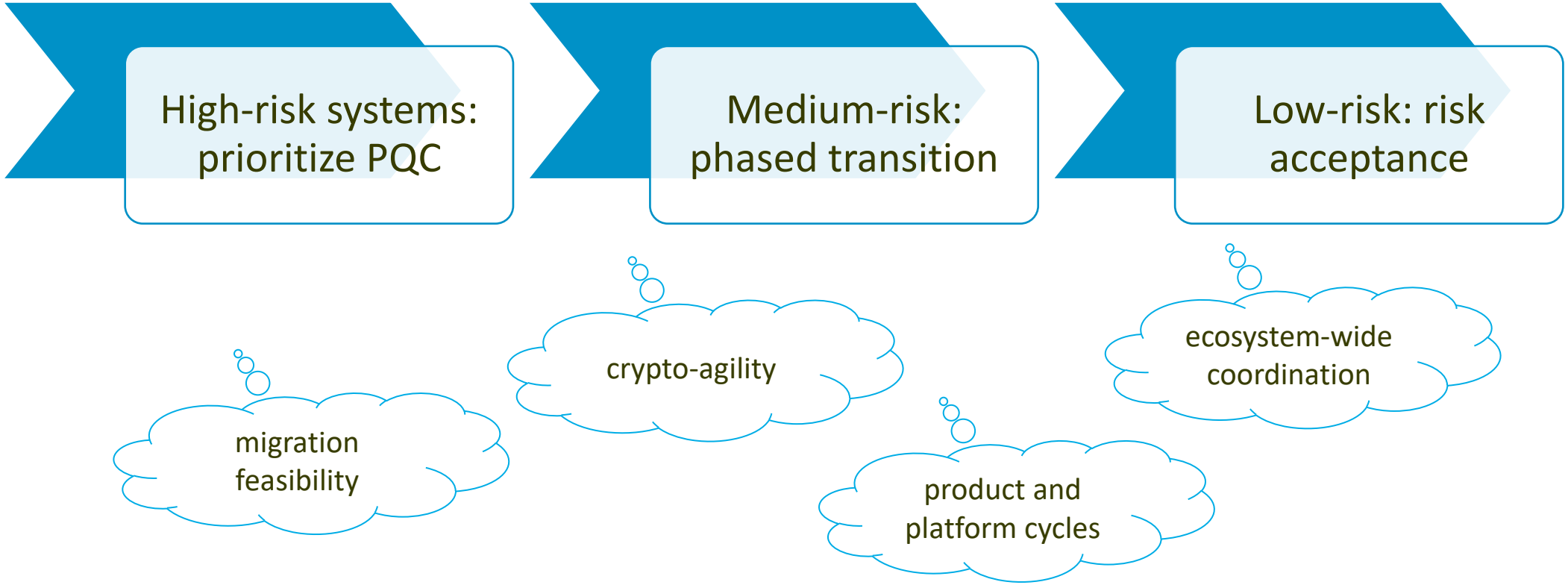
Need for aligned standards and migration approaches

Supplier readiness is critical

Regulatory & Standards



Transition Strategy



Key Strategic Messages

PQC is essential

Crypto-agile SDV platforms are key

Ecosystem alignment critical

Target timeframe: the time is now!

MWC GSMA
上海 · SHANGHAI
2026年6月24–26日
24–26 JUNE 2026

Q&A

Connected
Service BU, Product and
Cyber Security Business
Line
IDEMIA

Richard Mao

Richard Mao, Product Manager at
Quectel

Onur Kasaba

Managing Director
Tele2 IoT

IDEMIA
SECURE
TRANSACTIONS

Crossing the Void Between Manufacturing and Connectivity

Secure connectivity tailored in the factory, built for the quantum future

QUECTEL TELE2 Internet of Things

IDEMIA SECURE TRANSACTIONS

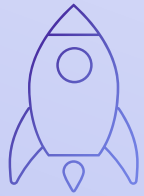
+

QUECTEL

+

TELE2 Internet of Things

Global leader in connectivity and security solutions



Global leader on cellular IoT module vendor with 40%+ market share

Leading global managed IoT connectivity providers

WHY CONNECTING DEVICES AT SCALE REMAINS A CHALLENGE: SKUs, COSTS & FIELD CONSTRAINTS

PART NUMBER MANAGEMENT

Multiple regional variants and SIM configurations drive up to **20% additional storage, handling, and logistics costs**, reducing margins

MANUFACTURING & TESTING COMPLEXITY

High SKU diversity slows production, complicates testing, and limits manufacturing agility

CONNECTIVITY LOCALIZATION LIMITATIONS

Field profile provisioning for battery-powered devices (e.g., water meters, trackers) can consume **up to 15% of battery life**

IDEMIA SECURE TRANSACTIONS

QUECTEL

TELE2 Internet of Things

SHIFTING CONNECTIVITY TAILORING FROM FIELD TO FACTORY: IN-FACTORY PROFILE PROVISIONING

FACTORY BINDING SHIFT

Carrier credentials are securely provisioned at end-of-line rather than during SIM manufacturing

SINGLE GLOBAL SKU

Generic eSIMs eliminate carrier-specific eSIM variants

LATE CARRIER CHOICE

Operator selection moves closer to deployment, reducing forecasting risk, logistics complexity, and cost

STORE NOW, DECRYPT LATER: A TIME BOMB IN CARRIER PROFILE CONFIDENTIALITY

CLASSICAL CRYPTO DEPENDENCY

Carrier profile packages under GSMA SGP.41/42 depend on ECC-based encryption to ensure confidentiality

QUANTUM INEVITABILITY

Encrypted profile packages can be retained today and decrypted once quantum capabilities mature

CROWN JEWEL EXPOSURE

Decrypted carrier credentials enable profile cloning and device identity impersonation at scale

IDEMIA SECURE TRANSACTIONS

QUECTEL

TELE2 Internet of Things

IDEMIA'S QUANTUM-SAFE APPROACH: IFPP READY FOR POST-QUANTUM SECURITY

1 Profile ordering

OEM

Establish contract with MNO using existing commercial interfaces and processes

2 Profile generation

MNO

Generate IFPP-compatible profiles in GSMA SAS-SM certified environments

3 Quantum-safe profile package creation

IDEMIA

Bind MNO profiles to target eIDs with **quantum-safe algorithms in GSMA SAS-SM certified environments** and orchestrate delivery to the target factory

4 Profile loading onto eSIM

OEM

Loads profiles onto target devices securely and efficiently

5 Profile reconciliation

IDEMIA

Ensure reconciliation between delivered and installed profiles and coordinate installation status reporting back to the MNO

IDEMIA SECURE TRANSACTIONS

QUECTEL

TELE2 Internet of Things

WHY QUANTUM-SAFE IN-FACTORY PROVISIONING IS NON-NEGOTIABLE FOR MNOS

LONG-TERM CREDENTIAL EXPOSURE

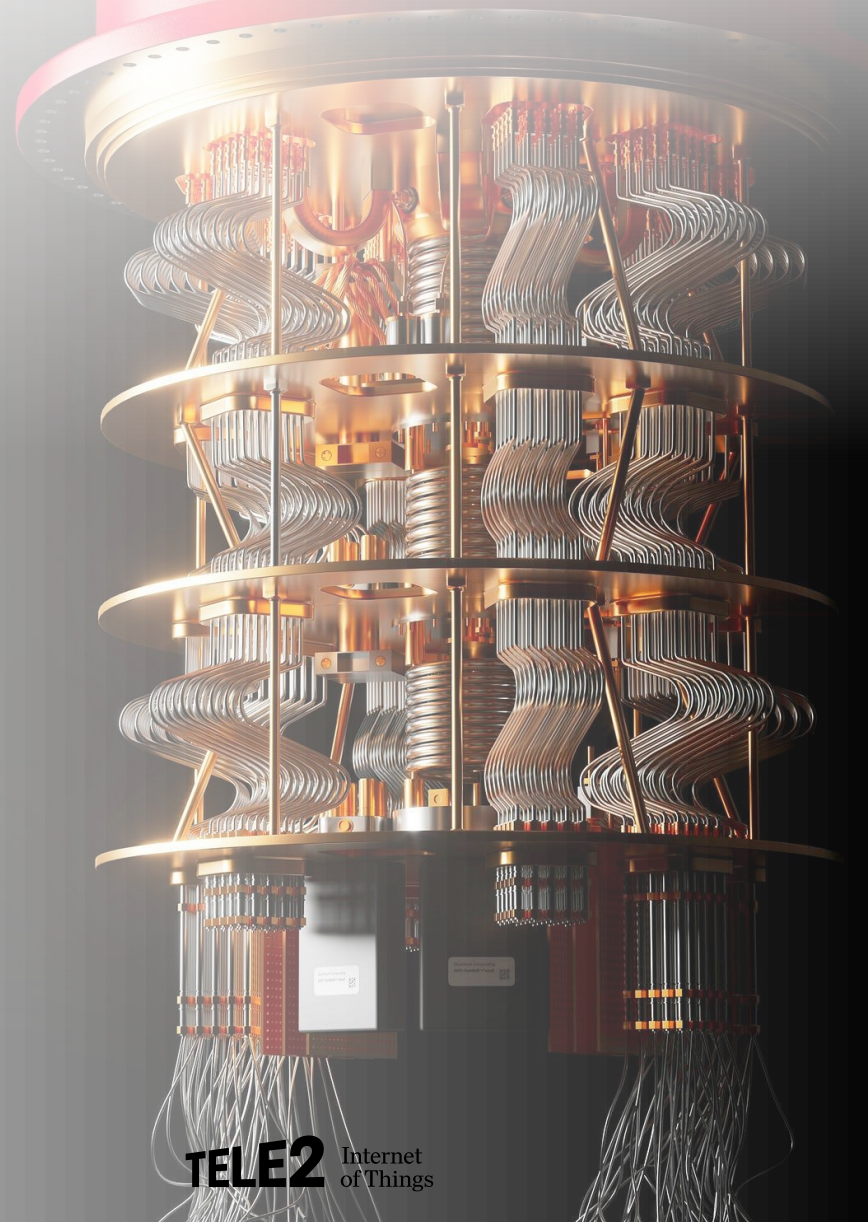
Without quantum-safe protection, IFPP creates deferred confidentiality risk for carrier profile credentials

REVENUE & TRUST PROTECTION

Compromised credentials enable cloning and identity fraud, directly threatening revenue and brand trust

CRYPTO-AGILE CONTINUITY

Operators require provisioning architectures capable of evolving cryptography to protect carrier credentials throughout the supply chain



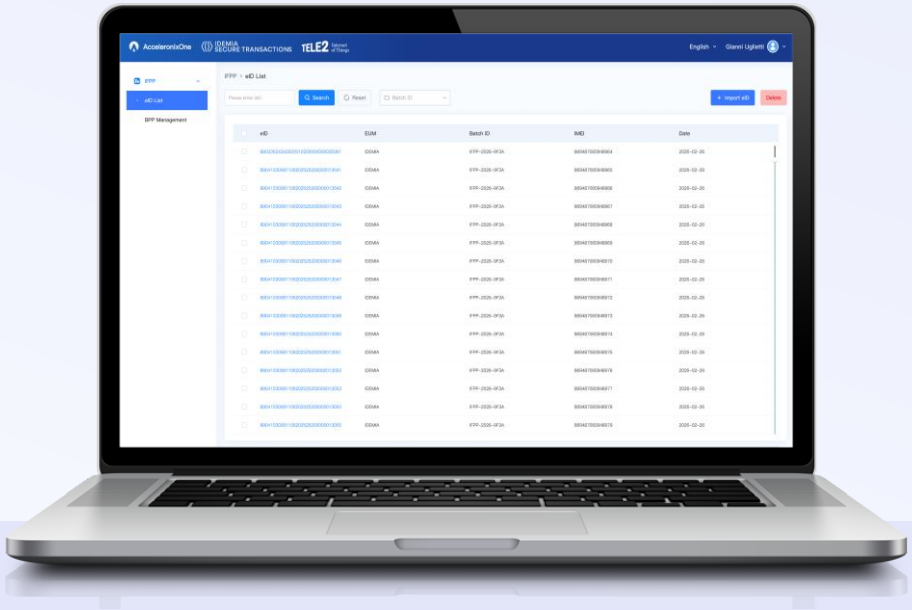
IDEMIA SECURE TRANSACTIONS

QUECTEL

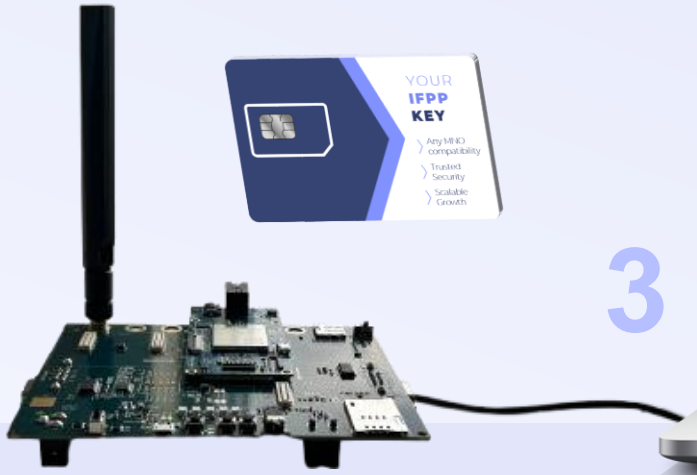
TELE2 Internet of Things

THE IDEMIA RECIPE: SEAMLESS INTEGRATION, TRUSTED SECURITY, SCALABLE GROWTH

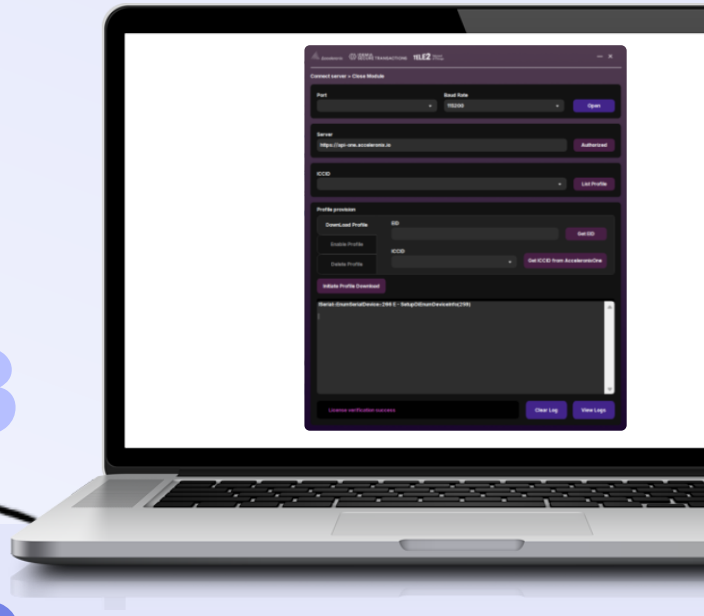
1



2



3



Quantum-safe profile generation and binding

MNO profiles are requested by the OEM and cryptographically bound to their target eSIMs, ensuring authenticity and preventing post-production tampering or misrouting. Quantum-resistant algorithms are applied for long-term security.

Standardized device production

The OEM manufactures a single global device SKU with a vanilla eSIM, not tied to any MNO, enabling secure provisioning with carrier credentials after production.

Offline profile provisioning

Profile packages are delivered to the factory and loaded onto eSIMs offline. Packages may be retained but remain resistant to SNDL-style attacks.

IDEMIA
GROUP

www.idemia.com

MWC GSMA
上海・SHANGHAI
2026年6月24–26日
24–26 JUNE 2026

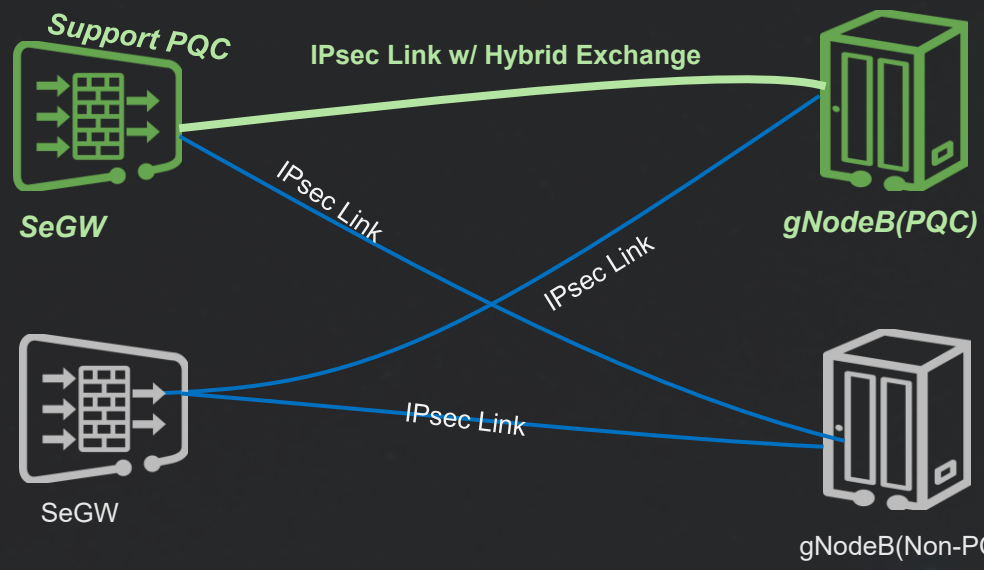
Q&A

MWC GSMA
上海 · SHANGHAI
2026年6月24–26日
24–26 JUNE 2026

Enabling Multiple key exchanges on post-quantum IPsec protocol

Lun Li
Senior Engineer
Huawei

IPsec multiple key exchanges for access network

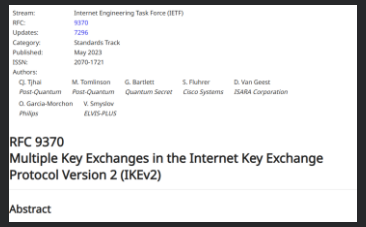


Stage name	Function	Description
IKE_SA_INIT	***Negotiate Algorithm***	Negotiate multiple PQC algorithms,
IKE_AUTH	Identity authentication	Authentication using certificates
CREAT_CHILD_SA	***Generating symmetric session keys***	Export/update session keys **using PQC key materials**
INFORMATIONAL	Management function	Management Messages

In Showcase

IETF RFC 9370

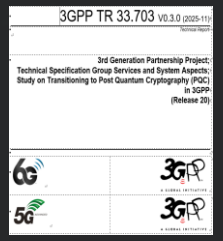
- IETF publishes IPsec multiple key exchanges specification


RFC 9370
Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)

Abstract

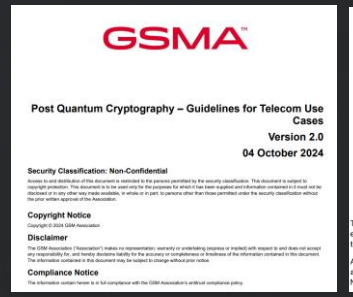
3GPP telecom study

- 3GPP Study on Transitioning to Post Quantum Cryptography (PQC)


3GPP TR 33.703 V0.3.0 (2025-11)

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Study on Transitioning to Post Quantum Cryptography (PQC) in 3GPP
(Release 20)

PQTN whitepaper on PQC use case


GSMA

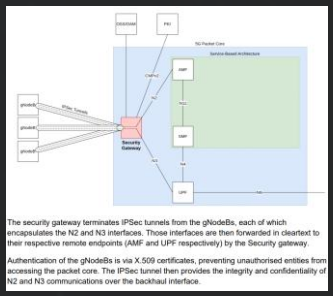
Post Quantum Cryptography – Guidelines for Telecom Use Cases
Version 2.0
04 October 2024

Security Classification: Non-Confidential

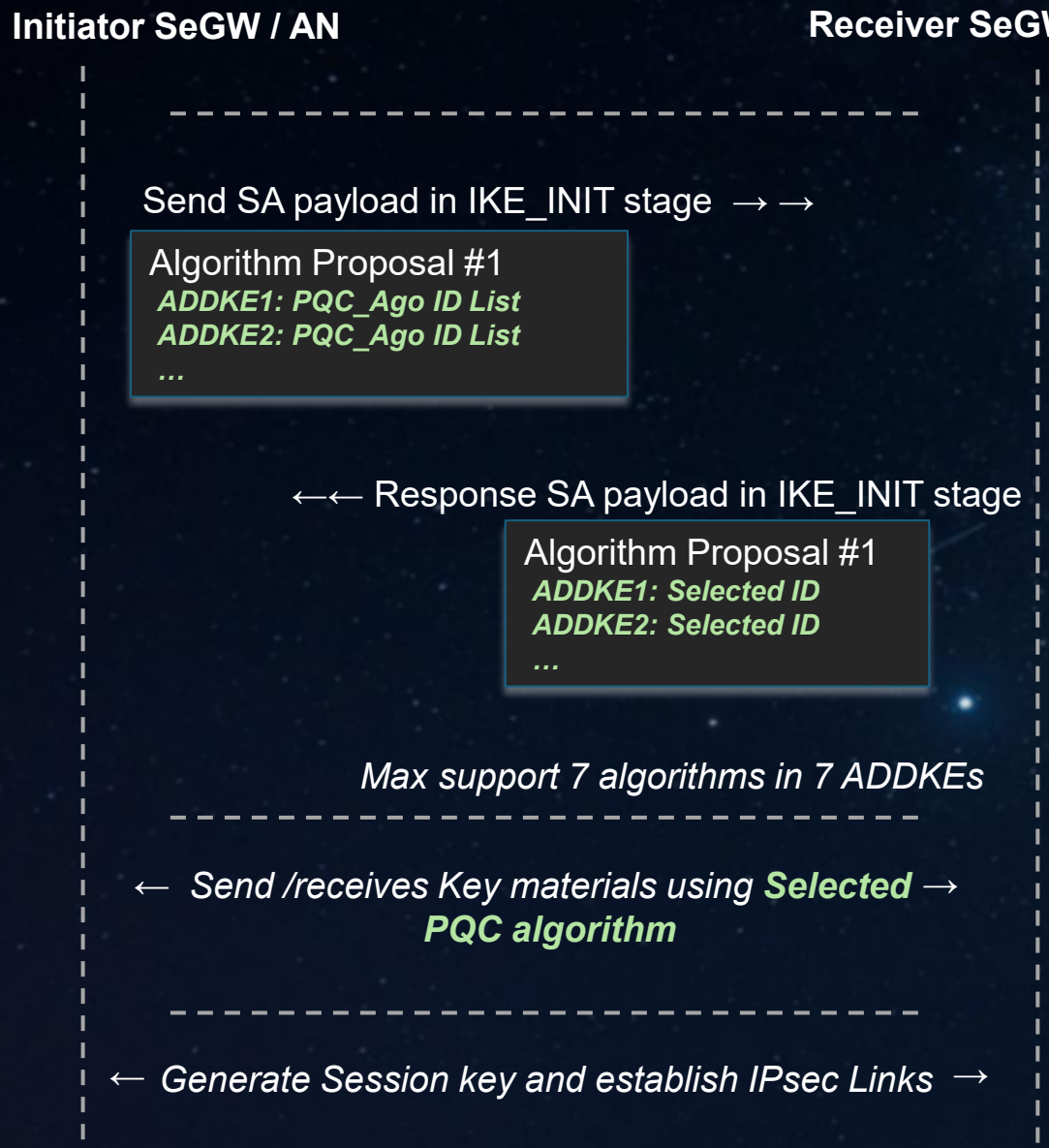
Copyright Notice

Disclaimer

Compliance Notice


The security gateway terminates IPSec tunnels from the gNodeBs, each of which encapsulates the N2 and N3 interfaces. Those interfaces are then forwarded in cleartext to their respective remote endpoints (AMF and UPF respectively) by the Security gateway.

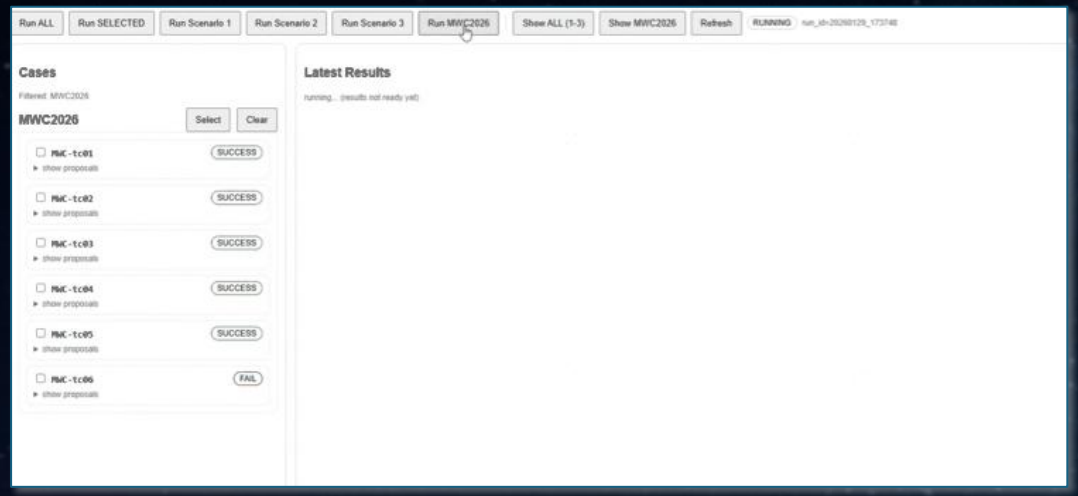
Authentication of the gNodeBs is via X.509 certificates, preventing unauthorised entities from accessing the packet core. The IPSec tunnel then provides the integrity and confidentiality of N2 and N3 communications over the backhaul interface.

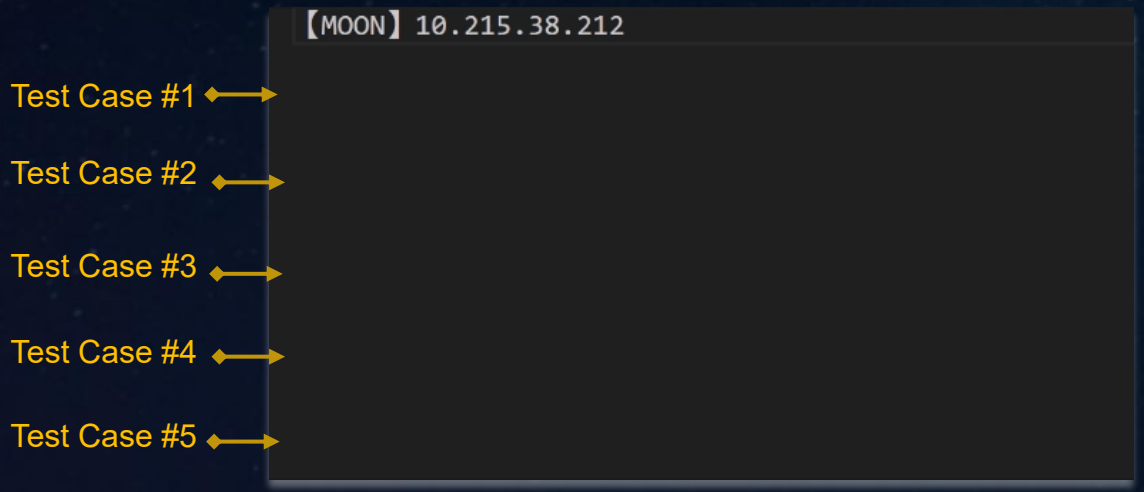


*Test procedure based on IETF RFC 9370

Test Case	Selected Proposal
01	Classical DH (Non-PQC)
02	ADDKE1: ML-KEM-512
03	ADDKE1: ML-KEM-768
04	ADDKE1: ML-KEM-1024
05	ADDKE1: ML-KEM-512 ADDKE2: ML-KEM-768
06	Mismatch

Test cases and Benchmark





* No Test Case #6 result: algorithm negotiation Failed

Test#	Selected Algorithm	KE timing affected by PQC migration	ESP time
01	Classical DH (Non-PQC)	**Classic (around 50-100ms)**	20-30ms
02	ADDKE1: ML-KEM-512	**+2.3%**	20-30ms
03	ADDKE1: ML-KEM-768	**+10.11%**	20-30ms
04	ADDKE1: ML-KEM-1024	**+17.9%**	20-30ms
05	ADDKE1: ML-KEM-512 ADDKE2: ML-KEM-768	**+18.0%**	20-30ms
06	Mismatch	**Failed**	Failed

* The video is processed to play in 1.5x speed
* Benchmark is tested using non-commercial platform

Explain Lessons and learnings

Lessons:
1. Since key exchange protocols (IKEv2) and payload encryption are decoupled in IPsec, the PQC migration of the critical key exchange protocols can be prioritized

Explain: The DH is migrated to multiple key exchange in IKEv2. After the IKEv2, the session key is generated and PQC will not impact on the data protection in transmission of IPsec since the algorithm is symmetric. We learned that key exchange should be prioritized.

Lessons:
2. Based on test results, choosing on ML-KEM key sizes have limited impact on total benchmark timings.

Explain: 512/768/1024 of ML-KEM only increase key generation by 2.3%-18% Therefore, we have learned that there is no need to consider performance impact when selecting an algorithm.

Lessons:
3. The placement of ADDKEs is critical for successful implementation, especially as the complexity of the algorithm list grows.

Explain: According to RFC 9370, the algorithms SHALL only be selected in the SAME ADDKE with no repeat. If there are mis-configuration either side, algorithm negotiation in IKE_INIT may fail even when both telecom entities support the same algorithm.

Failure cases1 : mis-match of ADDKEs

SeGW proposal	*AN Configuration:*
• *ADDKE1: ML-KEM-768*	• *ADDKE1: ML-KEM-1024*
• *ADDKE2: ML-KEM-1024*	• *ADDKE1: ML-KEM-768*
• *ADDKE4 – ADDKE7: none*	• *ADDKE2: - ADDKE 7 :none*

Failure cases2: Cannot fulfill the ADDKE3 without repeat

SeGW proposal
- *ADDKE1: ML-KEM-768/512*
- *ADDKE2: ML-KEM-768/512*
- *ADDKE3: ML-KEM-768/512*

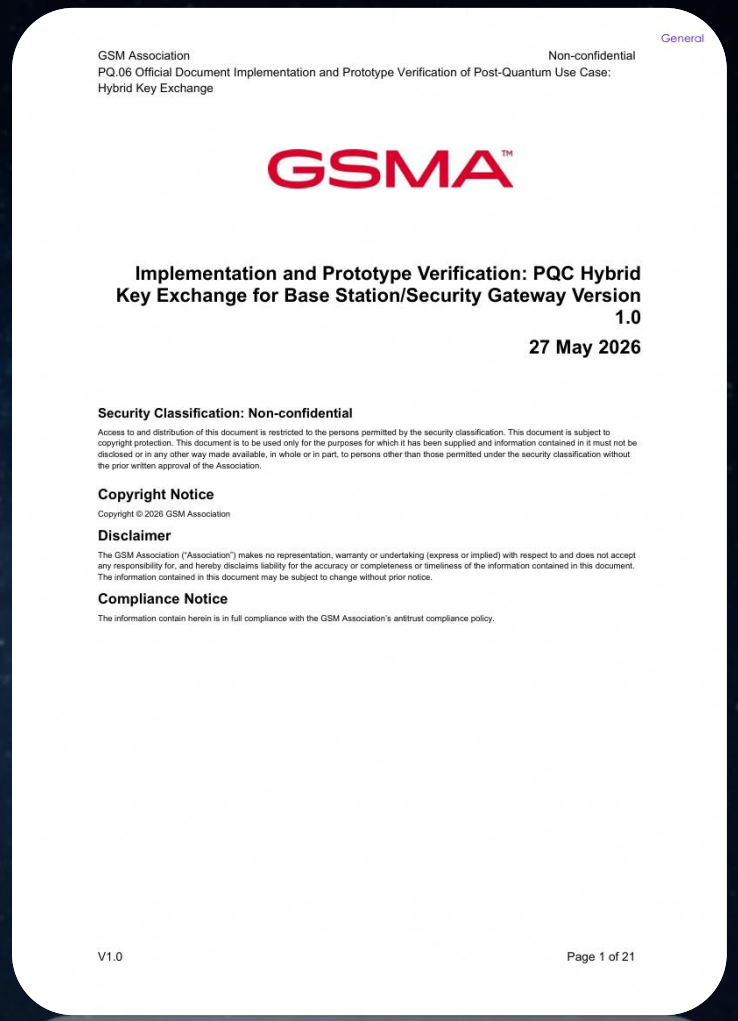
https://datatracker.ietf.org/doc/draft-li-ipsecme-extensions-for-robust-negotiation/

Related Publications in PQTN (PQ.06)

Monday April 27, 2026

PQ.06 Implementation and Prototype Verification: PQC Hybrid Key Exchange for Base Station/Security Gateway Version 1.0

Download PQ.06



General

GSM Association Non-confidential

PQ.06 Official Document Implementation and Prototype Verification of Post-Quantum Use Case: Hybrid Key Exchange

GSMA

Implementation and Prototype Verification: PQC Hybrid Key Exchange for Base Station/Security Gateway Version 1.0

27 May 2026

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2026 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Compliance Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

V1.0 Page 1 of 21

LINK: https://www.gsma.com/newsroom/gsma_resources/ig-06-implementation-and-prototype-verification-pqc-hybrid-key-exchange-for-base-station-security-gateway-version-1-0/

MWC GSMA
上海 · SHANGHAI
2026年6月24–26日
24–26 JUNE 2026

Q&A

MWC GSMA

上海 · SHANGHAI
2026年6月24–26日
24–26 JUNE 2026

Post Quantum Telco Networks Task Force Mision

Yolanda Sanz

Head of Working Groups, GSMA

Post Quantum Cryptography – Its Significance in the Telecommunications Industry

Problem

Quantum Threat
Shor's algorithm & quantum computers could break current asymmetric crypto: RSA or ECC

Quantum Treat in Telco
Asymmetric key protocols are used in whole Telco Infrastructure: eSIM, TLS,

NIST Timelines
Well-defined timelines are crucial in guiding the cryptographic migration process.

Solution

Post Quantum Cryptography Algorithms
New encryption methods that remain secure from both classical computers and quantum computers

Standards

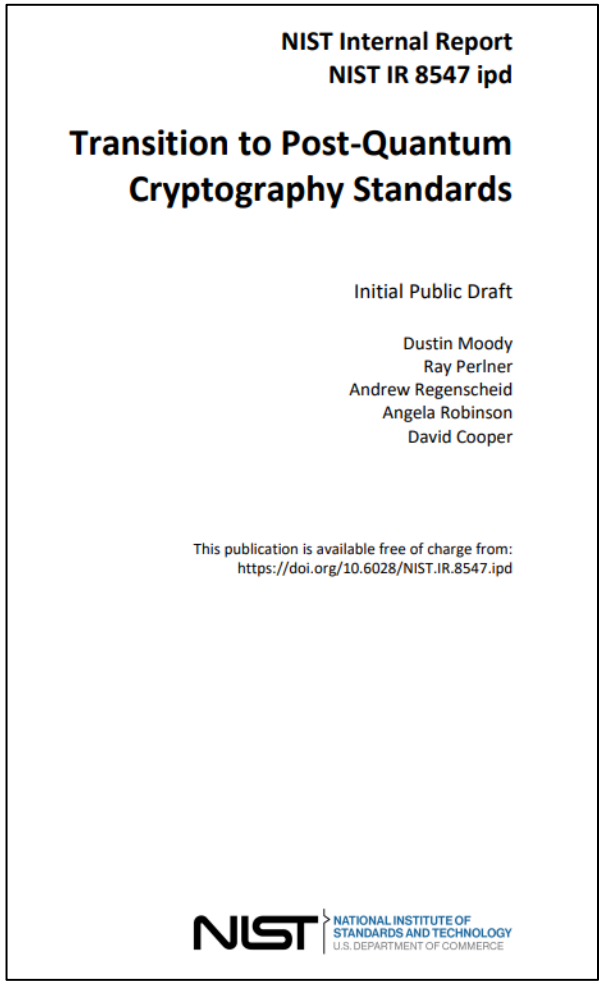
ML-KLEM (FIPS 203)
Standard for Key Establishment

ML-DSA (FIPS 204)
Standard for Digital Signature

SLH-DSA (FIPS 204)
Standard for Hash-based digital signature scheme

GSMA™

Post Quantum Cryptography – Necessary (1/2)



NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

Initial Public Draft

Dustin Moody
Ray Perlner
Andrew Regenscheid
Angela Robinson
David Cooper

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8547.ipd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Identifies quantum-vulnerable standards

- Key establishment based on Diffie-Hellman and elliptic curves (SP 800-56A)
- Key establishment based on RSA (SP 800-56B)
- Digital signatures include RSA, ECDSA, EdDSA (FIPS 186-4)

Proposed transition timelines for quantum-vulnerable algorithms

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

Key Establishment Scheme	Parameters	Transition
Finite Field DH and MQV [SP80056A]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
Elliptic Curve DH and MQC [SP80056A]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [SP80056B]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

GSMA

Post Quantum Cryptography – Necessary (2/2)

CNSA v2.0

By 2027, Migration Roadmaps

By 2031, Priority migration

By 2030, Deprecate RSA, ECC and

By 2035, Full migration and disallow

CCCS

By April 2026, Quantum Safe roadmap

By 2031, High priority system migrated

By 2026, Medium priority system migrated

NCSC

By 2028, define migration goals

By 2031, carry highest priority PQC migration

By 2035, complete migration to PQC

NIS CG

By Dec 2026, Quantum Safe roadmap

By Dec 2030, High risk use cases transitioned

By Dec 2035, Medium risk use cases transitioned

Takeaway - Mandate **Post Quantum Cryptography Completion** by 2030–2035

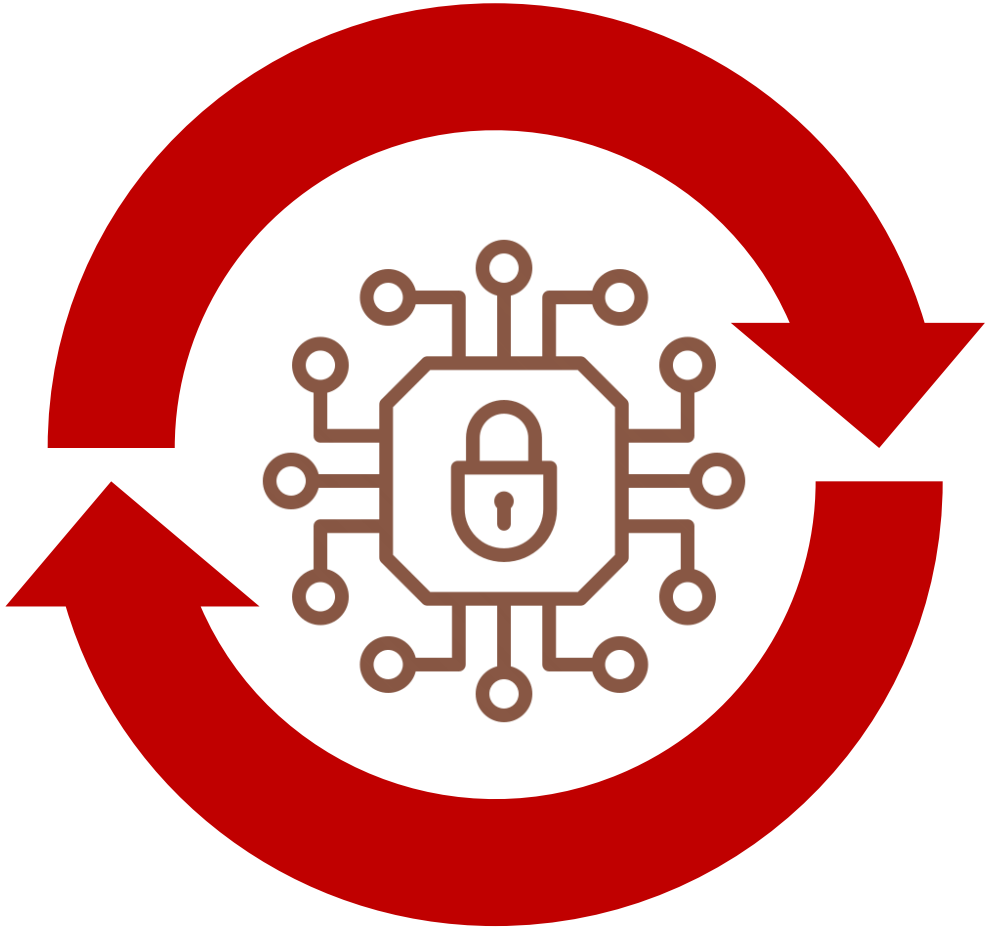
GSMA

Post Quantum Cryptography – Quantum Computers Attacks

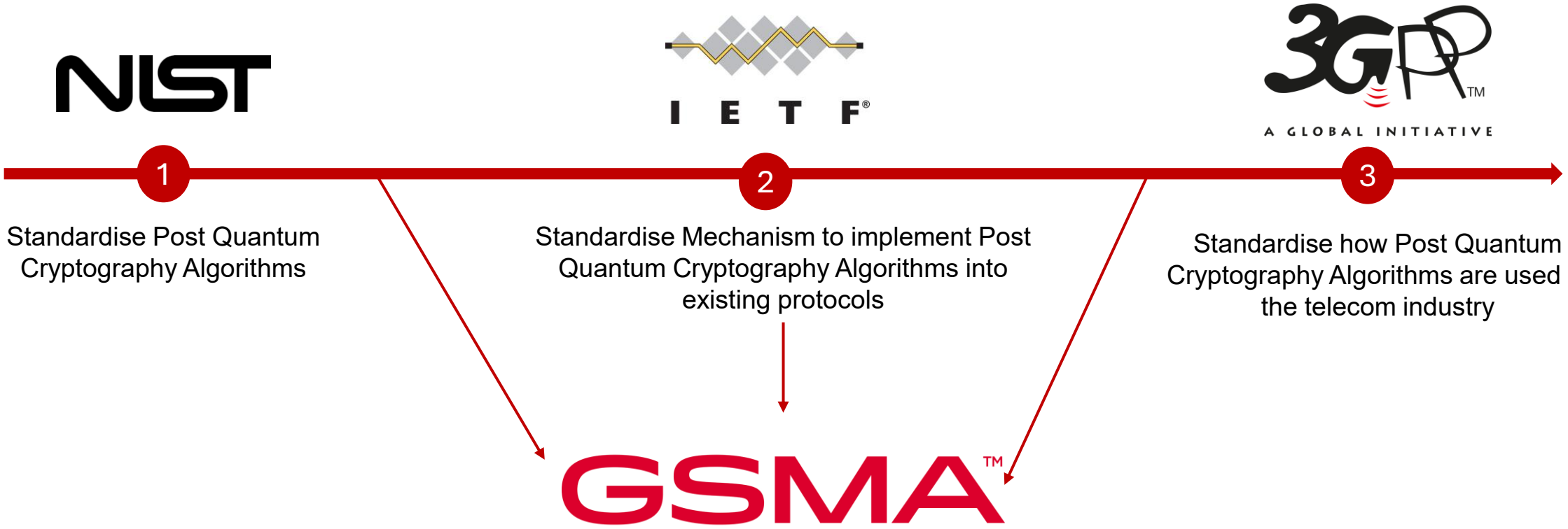
The Question isn't when this Q-Day will arrive

GSMA

Post Quantum Cryptography – Crypto Migration



Post Quantum Cryptography – GSMA Role



Build awareness of post quantum migration plans

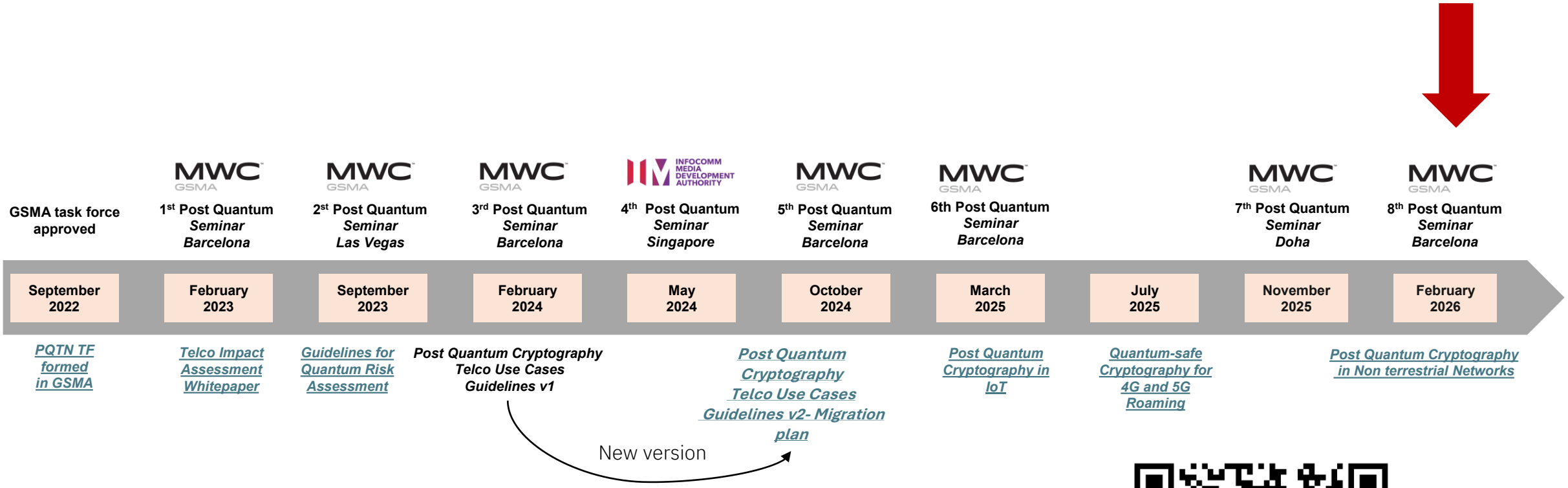
Develop skills on post quantum migration

Identify gaps on the telco industry standards

Testing and provide best practice guidelines

GSMA

Post Quantum Cryptography – GSMA Post Quantum Telco Network Taskforce



GSMA Post Quantum Telco Network Taskforce – Work in progress

GSMA Specifications: PQC Impact Assessment & Roadmap

Assess the existing GSMA specification to determine the impact of post-quantum cryptography (PQC) and identify when the specification could be updated to achieve quantum-safe readiness.

Coming soon!

Cryptography Bill of Material (CBOM) for Telco

Use of CBOM within the telecommunications sector, as it relates to the migration to post quantum cryptography, crypto-agility and ongoing cryptography management. The goal is to provide an analysis around the role of CBOM as part of a comprehensive framework for identifying, managing, and transitioning cryptographic assets to ensure security against threats.

PQC in Automotive (work item in collaboration with 5GAA)

The position paper will detail the security concerns related to classical cryptography and its impact on OEM interests, contextualising the current state of play (including the work already done addressing the MNOs) and the need for the work that 5GAA will do. The position paper is to be shared externally (with both industry stakeholders and policymakers) and will also form the basis of the impact assessment.

Crypto-agility for Telecommunication Networks

Analysis on the implementation of crypto agility in telecommunication networks. The document aims to provide actionable guidelines to support the telecommunication ecosystem in the build/procurement of capabilities, inform emerging standards, provide input to operational considerations.

GSMA

Do not procrastinate. Key advantages

Increased opportunity for testing and refinement

Enhanced assurance in meeting regulatory compliance requirements

Thank you and Join us

MWC GSMA
上海 · SHANGHAI
2026年6月24－26日
24－26 JUNE 2026

GSMA Post Quantum Telco Network Task Force

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

GSMA™