GSMA

MWC GSMA | DOHA 8 – 10 NOVEMBER 2026

MWC26 Doha Roundtable

The Future of Telco Security: Building Quantum-Safe Networks Across MENA

Agenda:

AI Translation

Timing	Presentation/Demo Title	Presenter	Company
12:30 – 12:45 (15 mins)	Welcome and Introduction **PQC Activities within GSMA**: PQTN TF Update	**Yolanda Sanz**, Head of Working Groups	**GSMA**
12:45 – 13:10 (25 mins)	Crossing the Void Between Manufacturing and Connectivity - Secure connectivity tailored in the factory, built for the quantum future	**John Phelps**, Telecommunications and Secure-Connectivity Subject Matter Expert (SME) **Yasser Alaoui**, Head of Sales MENA	**IDEMIA** **Acceleronix**
13:10 – 13:35 (25 mins)	6G Security & Post-Quantum Cryptography Current Progress and Key Challenges	**Dr. Yan Bo Ti**, Principal Researcher	**Huawei Singapore**
13:35 – 14:00 (25 mins)	Quantum-Safe Telco Networks	**Charbel Sarkis**, Director of Systems Engineering for Telcos and MSSPs	**Fortinet**
14:00 – 14:25 (25 mins)	Current State of PQC in Qatar	**Syed Ahmad Rasool**, Information Security Senior Manager	**Vodafone Qatar**
14:25 – 14:30 pm (5 mins)	Closing	**Yolanda Sanz**, Head of Working Groups	**GSMA**

MWC GSMA | DOHA 8 – 10 NOVEMBER 2026



Welcome and Introduction
PQTN Task Force Updates

Yolanda Sanz
Head of Working Groups, GSMA

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 Threat 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
Standards

ML-KEM

FIPS 203

Standard for Key Establishment

ML-DSA

FIPS 204

Standard for Digital Signature

SLH-DSA

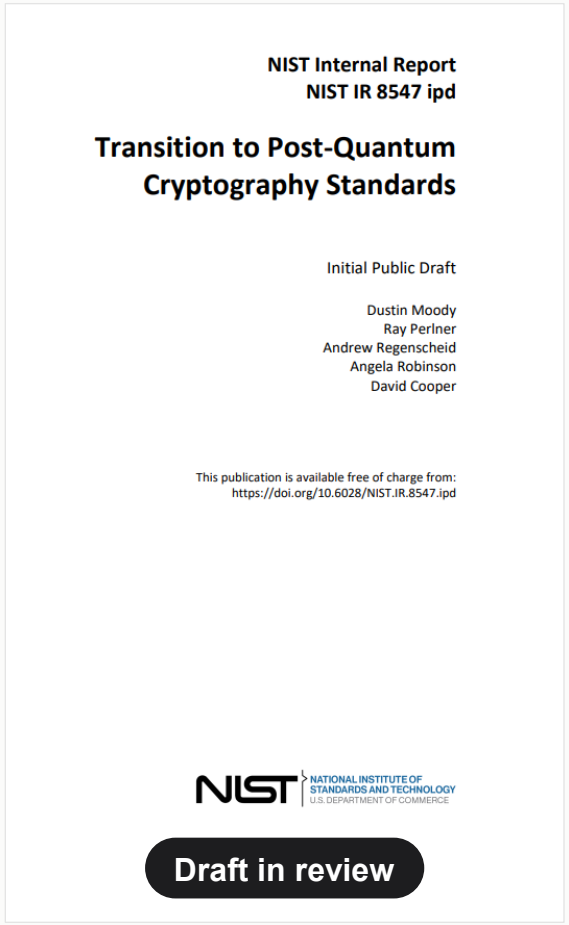
FIPS 205

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

Draft in review

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

DEPRECATED AFTER

2030

112 bits of security strength

DISALLOWED AFTER

2035

112 and ≥ 128 bits of security strength

Applies to ECDSA, EdDSA, RSA signatures and Finite Field DH/MQV, Elliptic Curve DH/MQV, RSA key establishment

GSMA

Post Quantum Cryptography

Necessary (2/2)



CNSA 2.0

By 2027
Migration roadmaps

By 2030
Deprecate RSA, ECC

By 2031
Priority migration

By 2035
Full migration and disallow



CCCS

By April 2026
Quantum Safe roadmap

By 2031
High priority systems migrated

By 2026
Medium priority systems migrated



NCSC

By 2028
Define migration goals

By 2031
Carry out 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





POST QUANTUM CRYPTOGRAPHY

Quantum Computers Attacks

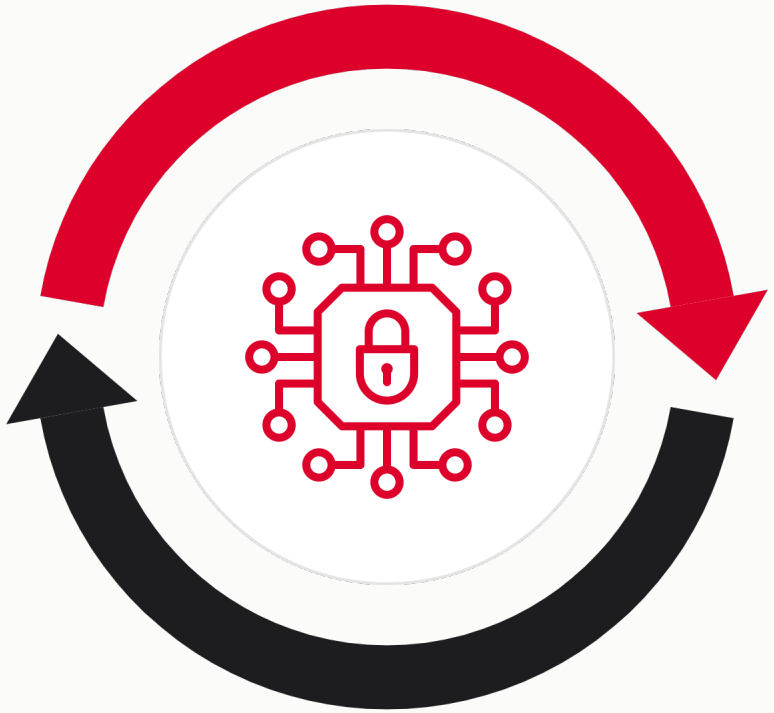
The question isn’t when this Q-Day will arrive

GSMA

GSMA

Post Quantum Cryptography

Crypto Migration



GSMA

Post Quantum Cryptography

GSMA Role

NIST 1

Standardise Post Quantum Cryptography Algorithms

IETF 2

Standardise Mechanism to implement Post Quantum Cryptography Algorithms into existing protocols

3GPP A GLOBAL INITIATIVE 3

Standardise how Post Quantum Cryptography Algorithms are used in the telecom industry

GSMA

- 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

GSMA Post Quantum Telco Network Taskforce - Crypto Migration Roadmap

2035

2030

1

Assessment and Awareness

Raise awareness of quantum risk and assess exposure across the network

2

Develop an inventory and priority list

Catalogue cryptographic assets and rank them by risk and urgency

3

Evaluate solution and test

Evaluate quantum-safe solutions and test them in the lab

4

Implement Best Practices

Roll out best practices and migrate priority systems

5

Complete Transition and Keep Monitoring

Finish the transition and keep monitoring for new threats

GSMA

GSMA Post Quantum Telco Network Taskforce

Resources

01 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!

02 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.

Coming soon!

03 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.

04 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

Post-Quantum Telco Network Taskforce

Post-quantum cryptography milestones, seminars and publications

Scan for all PQTN publications

Sep 2022

Taskforce approved by GSMA

PQTN Taskforce formed

Feb 2023

1st PQ Seminar
Barcelona

Telco Impact Assessment whitepaper

Sep 2023

2nd PQ Seminar
Las Vegas

Guidelines for Quantum Risk Assessment

Feb 2024

3rd PQ Seminar
Barcelona

PQC Telco Use Cases Guidelines v1

May 2024

4th PQ Seminar
Singapore

Oct 2024

5th PQ Seminar
Barcelona

PQC Telco Use Cases v2: Migration plan
New version of v1

Mar 2025

6th PQ Seminar
Barcelona

PQC in IoT

Jul 2025

Quantum-safe Cryptography for 4G & 5G Roaming

Nov 2025

7th PQ Seminar
Doha

Feb 2026

8th PQ Seminar
Barcelona

PQC in Non-Terrestrial Networks

Latest

Oct 2026

NEW · OCTOBER 2026

PQ.08 Post-Quantum Cryptography for Automotive – Impact Assessment

GSMA

GSMA Post Quantum Telco Network Taskforce

Resources

01 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!

02 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.

Coming soon!

03 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.

04 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.

KEY TAKEAWAYS

Do not procrastinate.

Key advantages

01

Increased opportunity for testing and refinement

02

Enhanced assurance in meeting regulatory compliance requirements

GSMA

Thank you and Join us

MWC GSMA | DOHA 8 – 10 NOVEMBER 2026



GET IN TOUCH

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

Scan for all PQTN publications

MWC GSMA | DOHA 8 – 10 NOVEMBER 2026

Crossing the Void Between Manufacturing and Connectivity - Secure connectivity tailored in the factory, built for the quantum future



John Phelps

Telecommunications and Secure-Connectivity Subject Matter Expert (SME)

IDEMIA



Yasser Alaoui

Head of Sales MENA

Acceleronix

AI Translation

IDEMIA
SECURE
TRANSACTIONS

Crossing the Void Between Manufacturing and Connectivity

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



Acceleronix

orange™

IDEMIA SECURE TRANSACTIONS

+

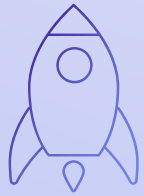
Acceleronix

+

orange™



Global leader in connectivity and security solutions



Acceleronix is a trusted all-in-one IoT partner, delivering scalable, reliable solutions from design to deployment.



Orange is an international telecommunications group that designs and deploys connectivity infrastructure and digital services.

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

Acceleronix

orange™

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

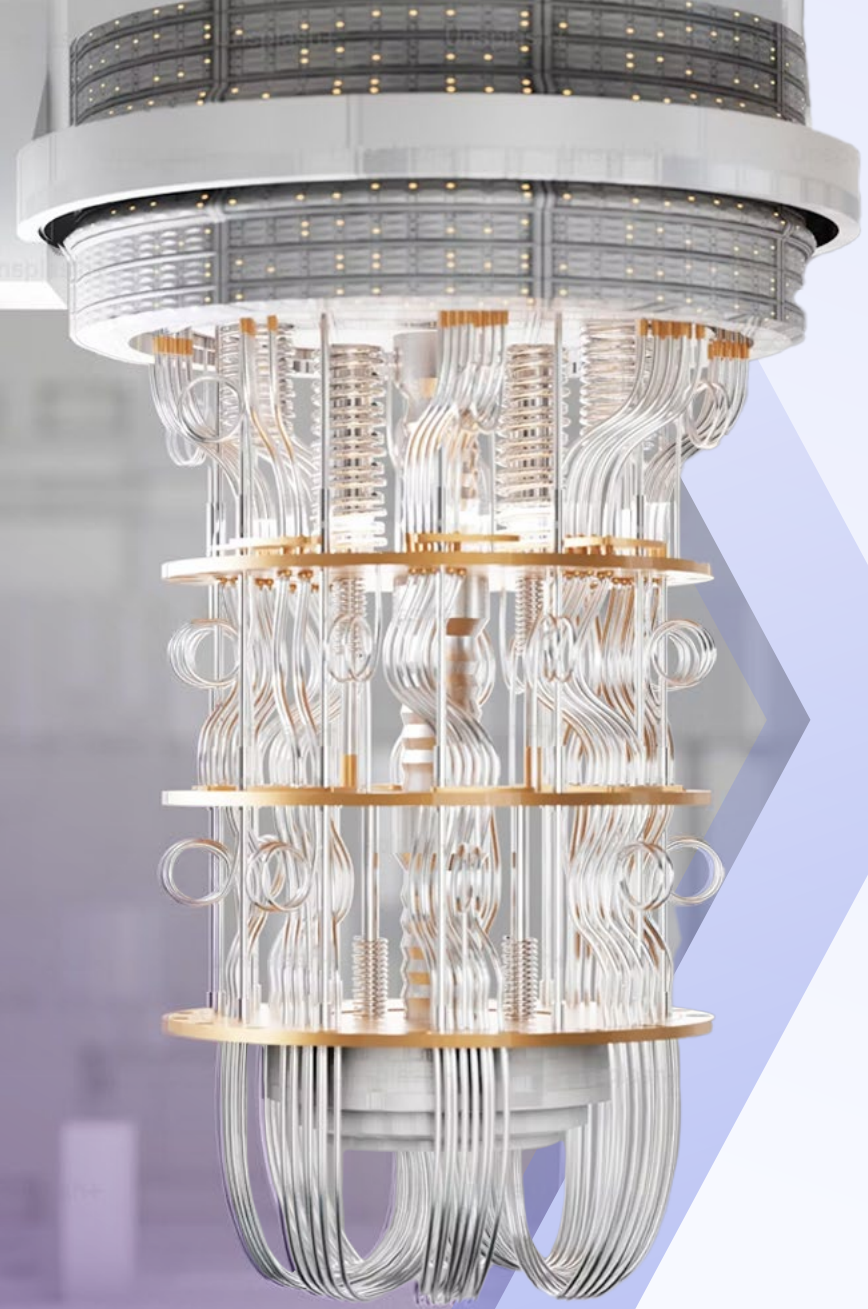
SINGLE GLOBAL SKU

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

Acceleronix

orange™

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

Acceleronix

orange™

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

LONG-TERM CREDENTIAL EXPOSURE

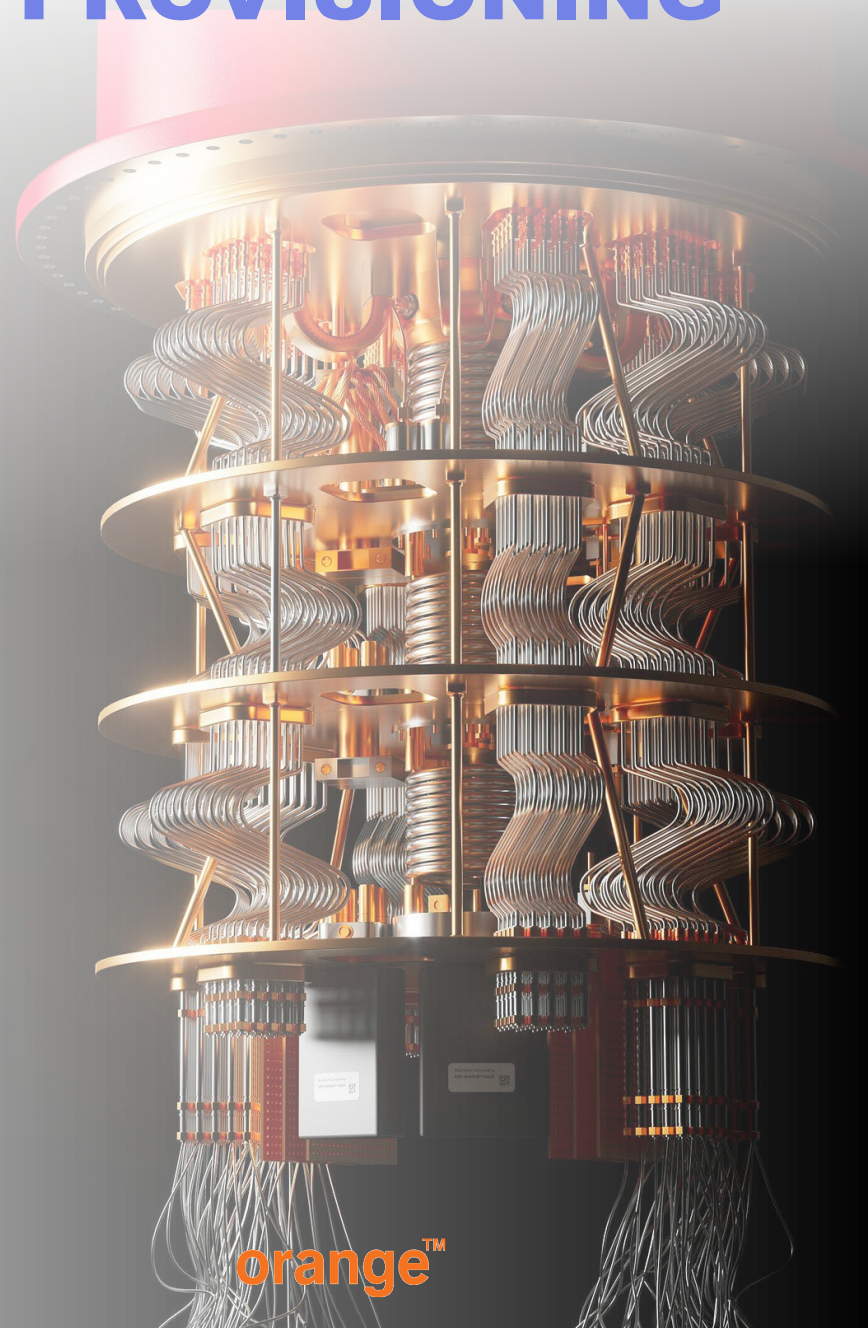
Without quantum-safe protection, IFPP creates deferred confidentiality risk for carrier profile credentials

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

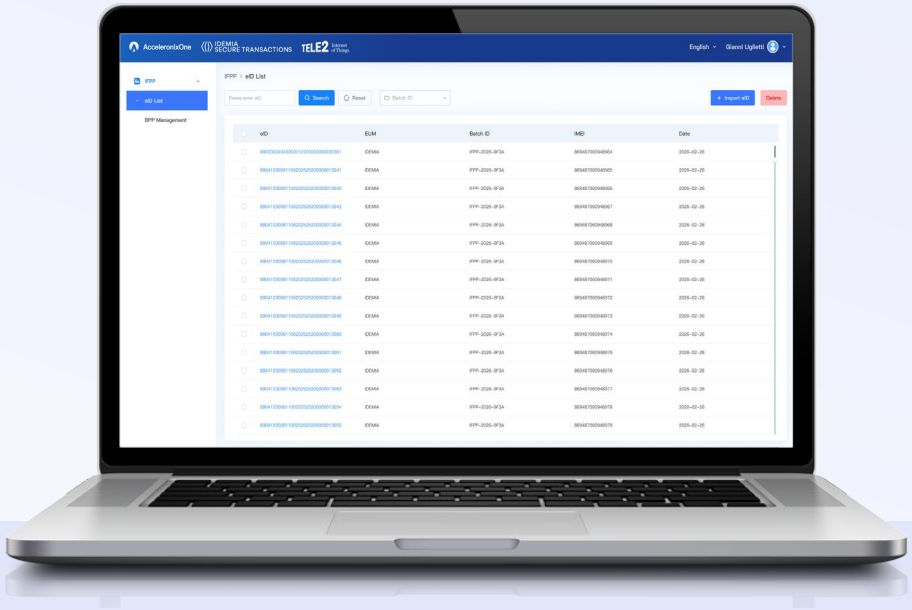


IDEMIA SECURE TRANSACTIONS

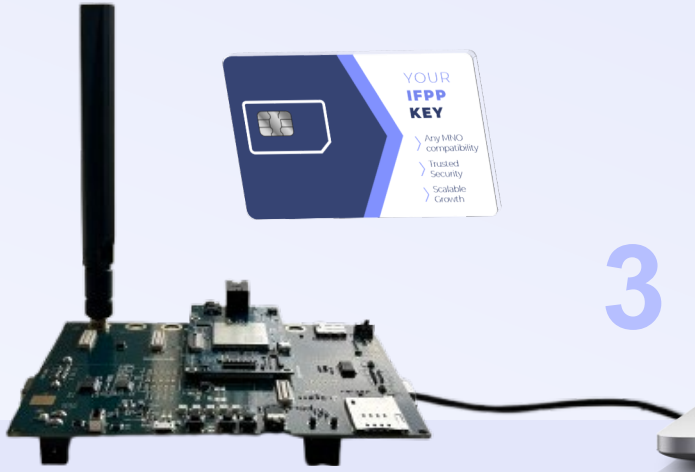
Acceleronix

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

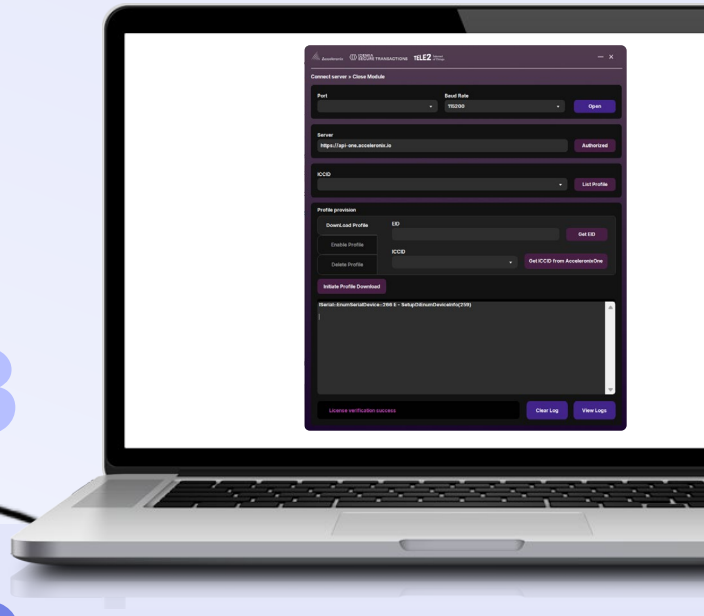
1



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.

CONTACTS

John Phelps
Subject Matter Expert (SME)
IDEMIA

john.phelps@idemia.com

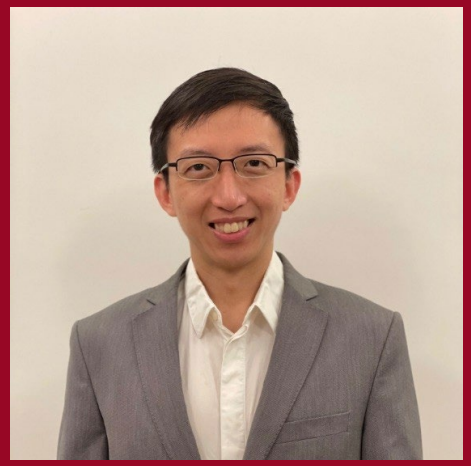
Yasser Alaoui
Reginal Sales MAnager
Quectel / Acceleronix

yasser.alaoui@quectel.com

IDEMIA GROUP

www.idemia.com

MWC GSMA | DOHA 8 – 10 NOVEMBER 2026



6G Security & Post-Quantum Cryptography - Current Progress and Key Challenges

Dr. Yan Bo Ti

Principal Researcher

Huawei Singapore

AI Translation



6G SECURITY & POST-QUANTUM CRYPTOGRAPHY

CURRENT PROGRESS AND KEY CHALLENGES

Yan Bo Ti: Huawei Singapore

OVERVIEW & MOTIVATION FOR PQC IN TELECOM

- Quantum computers running *Shor's algorithm* will break asymmetric schemes (RSA, ECC). Symmetric encryption (AES-256) remains secure against *Grover's algorithm*.
- **"Harvest Now, Decrypt Later" (HNDL)**: Encrypted long-life subscriber data, 5G signaling, and enterprise VPN traffic intercepted today will be retroactively decrypted once Cryptographically Relevant Quantum Computers (CRQCs) arrive.
- Core elements, transport nodes, and embedded SIMs deployed today have **>10 year lifecycles** ⇒ PQC migration an immediate operational requirement.

NIST PQC STANDARDISATION MILESTONES

Standard	Function	Status	Remarks
ML-KEM FIPS 203	Key encapsulation	Finalised in 2024	Primary Lattice-based
ML-DSA FIPS 204	Digital signature	Finalised in 2024	Primary Lattice-based
SLH-DSA FIPS 205	Digital signature	Finalised in 2024	Alternative Hash-based
FN-DSA FIPS 206	Digital signature	In progress	Alternative Lattice-based
HQC-KEM FIPS 207(?)	Key encapsulation	In progress	Alternative Code-based
LMS & XMSS SP800-208	Digital signature	Finalised in 2020	Specifically for software and firmware code-signing

- **Ongoing Evaluation**: Secondary signature standardisation round focusing on non-lattice alternatives to ensure mathematical diversity.

PQC TRANSITION IN 3GPP, GSMA, IETF, ISO/IEC

IETF

- **TLS 1.3**: Hybrid key exchange (ECC+ML-KEM). Moving towards composite signatures in TLS.
- **IPsec/IKEv2**: PQ key encapsulation for standalone and for PQ/T hybrid. Moving towards composite signature in IKEv2.
- **X.509 PKI**: Multi-key/hybrid digital certificates; potential mitigations against large signatures.

ISO/IEC

- Standardised **ML-KEM, LMS/XMSS, FrodoKEM, Classic McEliece**, and standardising **ML-DSA, SLH-DSA**.
- Updates to ISO/IEC 14888 and 18033 series for cryptographic evaluation across critical infrastructure.

3GPP

- **SBA**: PQC-compliant TLS 1.3 for inter-NF (Network Function) signaling.
- **SEPP**: Post-quantum security profiles for N32 inter-operator roaming interfaces.
- **SUCI**: Future-proofing SUCI against quantum decryption.

GSMA

- Established quantum threat baselines, risk governance, and core architectural migration guidelines across the telecom stack.
- Delivered tailored technical specifications for 5G SBA signaling, SUCI, SEPP/N32, IoT ecosystems, NTN, and connected automotive infrastructure.
- Published real-world Proof-of-Concept verification evaluating dual-algorithm hybrid key exchanges

KEY RISKS & OPERATIONAL CHALLENGES IN PQ MIGRATION

Zero-Day Mathematical Risk

- Newly standardised lattice-based schemes lack the decades of rigorous real-world cryptanalysis that classical RSA/ECC have undergone.
- Code-based schemes share similarities with lattice-based schemes.
- Hash-based schemes are generally believed to be safer, but performance is inadequate.

Performance overheads

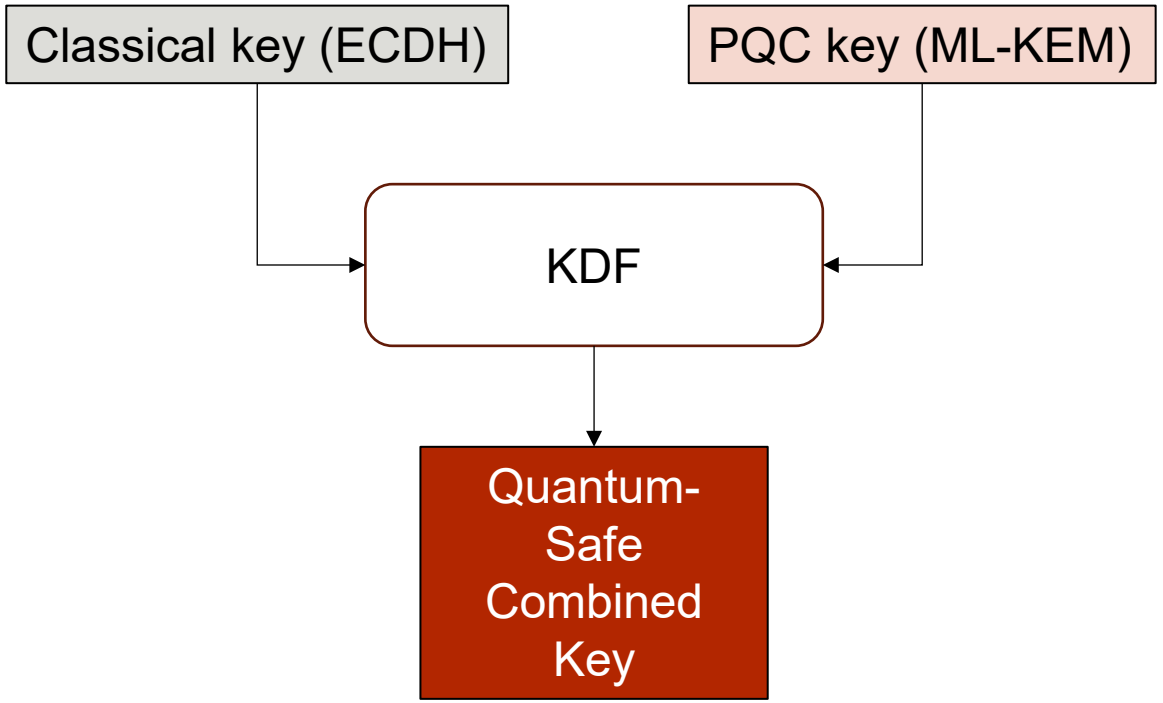
- **Key Size Expansion**: Larger public keys and ciphertexts risk IP packet fragmentation and buffer overflows.
- **Handshake Latency**: Computational overhead during session establishment impacts real-time voice, control plane signaling, and URLLC services.

Legacy Compatibility

- Upgrading multi-vendor carrier environments without breaking backward compatibility or inter-operator roaming.

MITIGATION STRATEGY 1: ALGORITHM COMBINERS

- **Mechanism:** Combining a classical algorithm with a PQ scheme via a Key Derivation Function (KDF):
  $$K_{final} = KDF(K_{classical} \parallel K_{PQC})$$
- **Fail-Safe Security:** Security remains even if one component scheme is broken.
- **Regulatory Compliance:** Satisfies existing mandates for classical ECC while fulfilling emerging PQ requirements.



MITIGATION STRATEGY 2: ARCHITECTURAL CRYPTO-AGILITY

- Software and hardware architectures designed to swap cryptographic algorithms via configuration/software updates without physical hardware replacement.
- **Examples of domain-specific application:**
  - Transport/Backhaul: Hardware abstraction in MACsec/IPsec processors for dynamic key exchange.
  - 5G/6G Core: Modular microservice crypto-libraries with dynamic policy configuration.
  - eSIM/Smart Cards: Over-the-Air (OTA) crypto-applet management for constrained devices.
- **Automated Asset Inventory:** Continuous visibility into cryptographic assets (algorithms, key lengths, certificates) across the network.

PRAGMATIC MIGRATION ROADMAP FOR OPERATORS

Discovery	Automated inventory of all classical asymmetric cryptography across all domains.
Combiners	Implement dual-algorithm key exchange on high-risk links (roaming, backhaul, sovereign cloud connectors).
Cryptoagile PQC	Adopt standardised native PQC algorithms and automated policy management across all network functions.

Attachments – Reference

Comparison of standardised PQC schemes

KEM	Security level	Public key size	Ciphertext size	Combined size
ML-KEM-512	1	800	768	1,568
ML-KEM-768	3	1,184	1,088	2,272
ML-KEM-1024	5	1,568	1,568	3,136
HQC-KEM-1	1	2,241*	4,433*	6,674*
HQC-KEM-3	3	4,514*	8,978*	13,492*
HQC-KEM-5	5	7,237*	14,421*	21,658*
FrodoKEM-640	1	9,616	9,720	19,336
FrodoKEM-976	3	15,632	15,744	31,376
FrodoKEM-1344	5	21,520	21,632	43,152
Classic-McEliece-460896f	1	524,160	156	524,316
Classic-McEliece-6688128f	3	1,044,992	208	1,045,200
Classic-McEliece-8192128f	5	1,357,824	240	1,358,064

Attachments – Reference

Comparison of standardised PQC schemes

DSA	Security level	Public key size	Signature size	Combined size
ECDSA-P256	1	65	72	137
ECDSA-P384	3	97	104	201
ECDSA-P521	5	133	139	272
ML-DSA-44	1	1,312	2,420	3,732
ML-DSA-65	3	1,952	3,309	5,261
ML-DSA-87	5	2,592	4,627	7,219
FN-DSA-512	1	897	666	1,563
FN-DSA-1024	5	1,793	1,280	3,073
SLH-DSA-128s	1	32	7,856	7,888
SLH-DSA-192s	3	48	16,224	16,272
SLH-DSA-256s	5	64	29,792	29,856

MWC GSMA

DOHA
8 – 10 NOVEMBER 2026



Charbel Sarkis

Director of Systems Engineering for Telcos and MSSPs

Fortinet

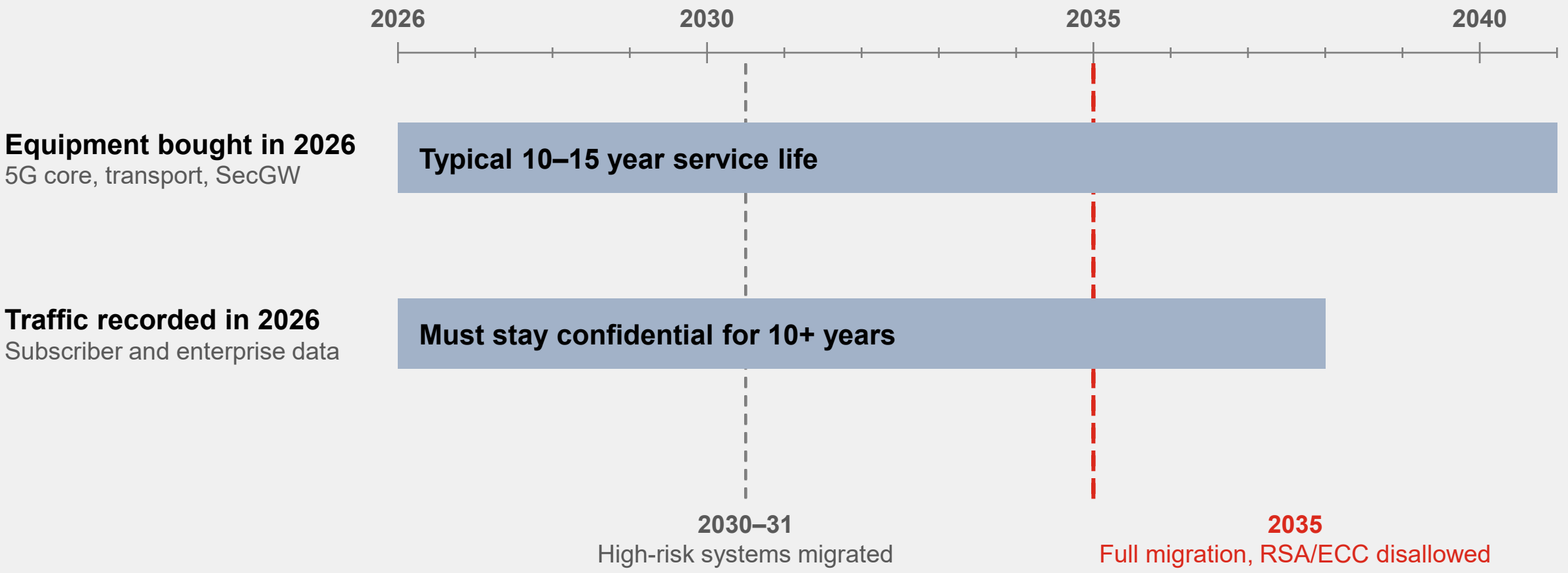
AI Translation

Quantum-Safe Telco Networks

Start with what you can see, protect what lives longest

Charbel Sarkis
Director, Systems Engineering for Telcos and MSSPs

Today's network and traffic outlive the 2035 deadline



Anything protected with classical key exchange today can be recorded now and decrypted later.

Deadlines: NSA CNSA 2.0, UK NCSC and EU NIS Cooperation Group roadmaps, as summarised by GSMA PQTN. Service-life and data-lifetime spans are illustrative.

© Fortinet Inc. All Rights Reserved.

Classical key exchange protects every telco interface today

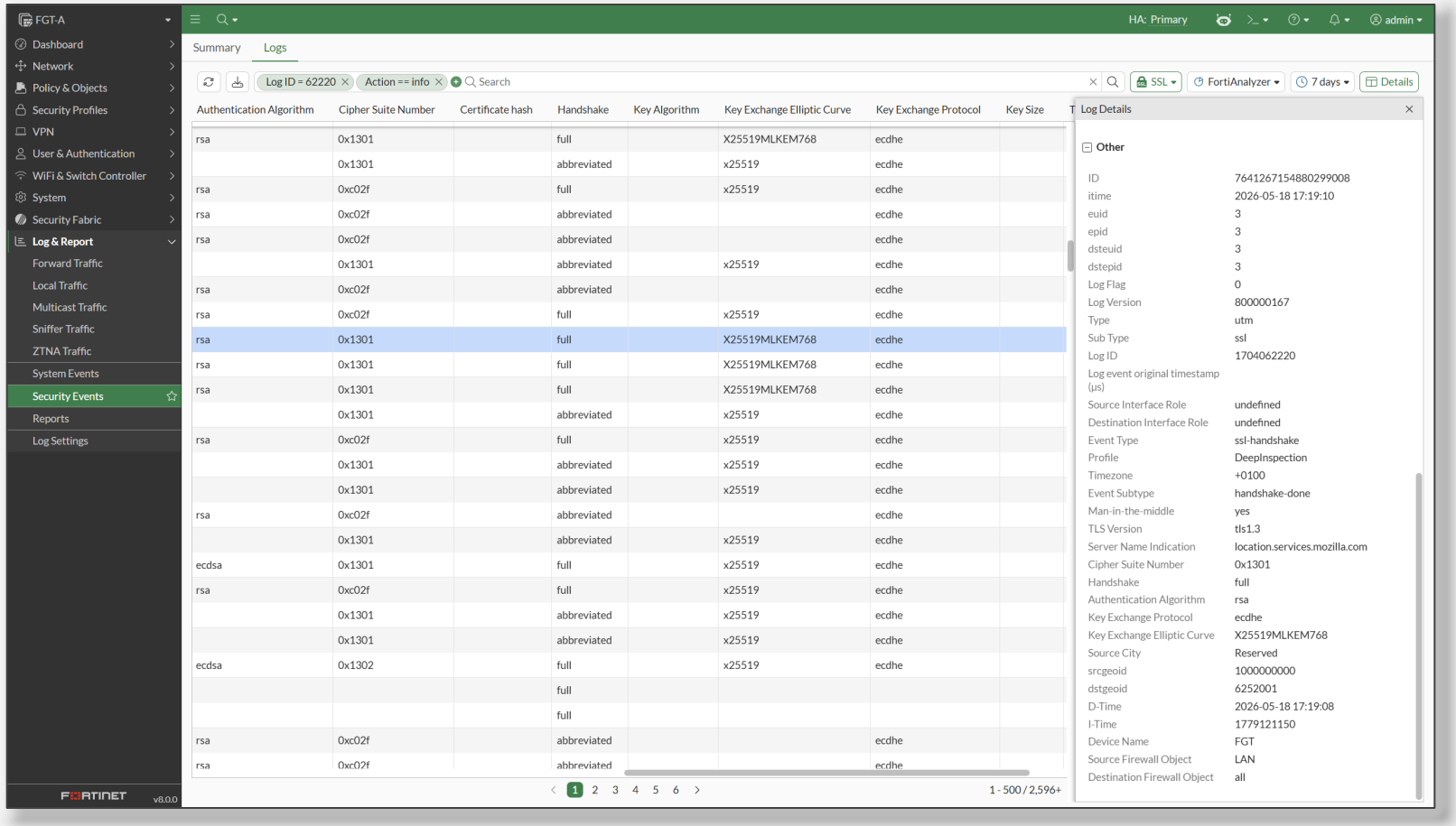
Devices & eSIM	RAN backhaul	Mobile core	Roaming / IPX	Internet & VPN
• eSIM profile delivery (ECC) • SUCI subscriber privacy • Device TLS to apps	• IPsec / IKEv2 from gNB to security gateway • MACsec on transport	• TLS 1.3 between network functions • HTTPS service APIs	• TLS on N32 (SEPP) • IPsec over IPX / GRX	• TLS at Gi / N6 • Enterprise IPsec VPN and SD-WAN • ZTNA access
Outside firewall view	**SecGW**	**Internal segmentation**	**Roaming firewall**	**Gi/N6 firewall, VPN**

Management plane: SSH, HTTPS, SNMPv3 and syslog over TLS to every element. PKI and HSMs sign it all.

Firewalls already sit on four of these five domains, which makes them the first discovery point.

© Fortinet Inc. All Rights Reserved.

Your firewalls already log which sessions use PQC



FortiGate SSL handshake log, FortiOS 8.0: one row per session

What every session log shows

- **Key exchange:** hybrid X25519MLKEM768 or classical x25519
- TLS version and cipher suite
- Server name and certificate algorithm (RSA, ECDSA)

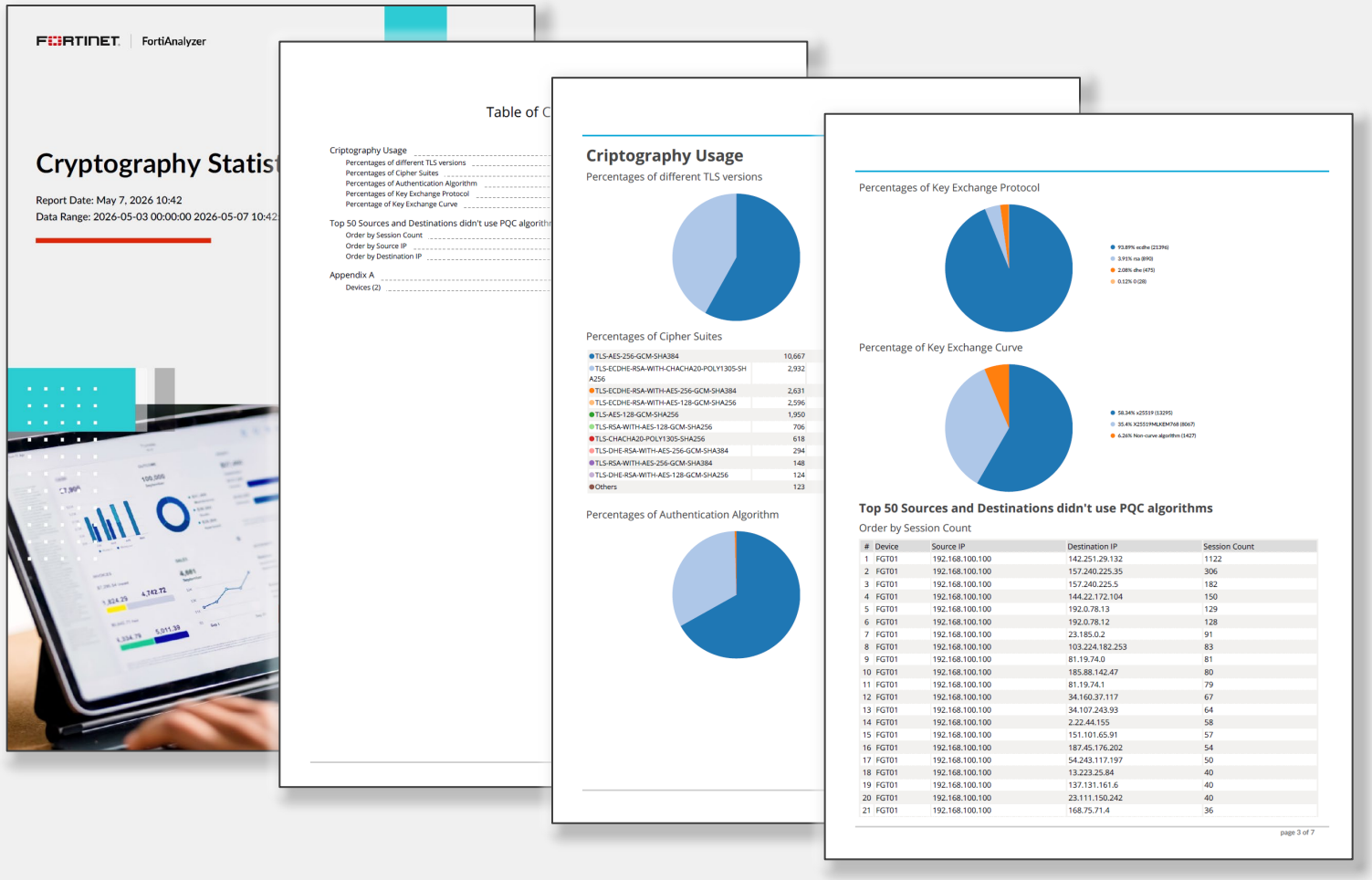
What it cannot see

- Crypto inside applications, code and stored data
- Traffic that never crosses a firewall
- Keys held in HSMs and PKI

Requires SSL handshake logging in the inspection profile. Combine with code scanning and CBOM tooling for a full cryptographic inventory.

© Fortinet Inc. All Rights Reserved.

Reporting turns firewall logs into a migration baseline



FortiAnalyzer Cryptography Statistics report, built from FortiGate SSL logs

1 Baseline

Share of sessions using hybrid PQC key exchange, per domain

2 Worklist

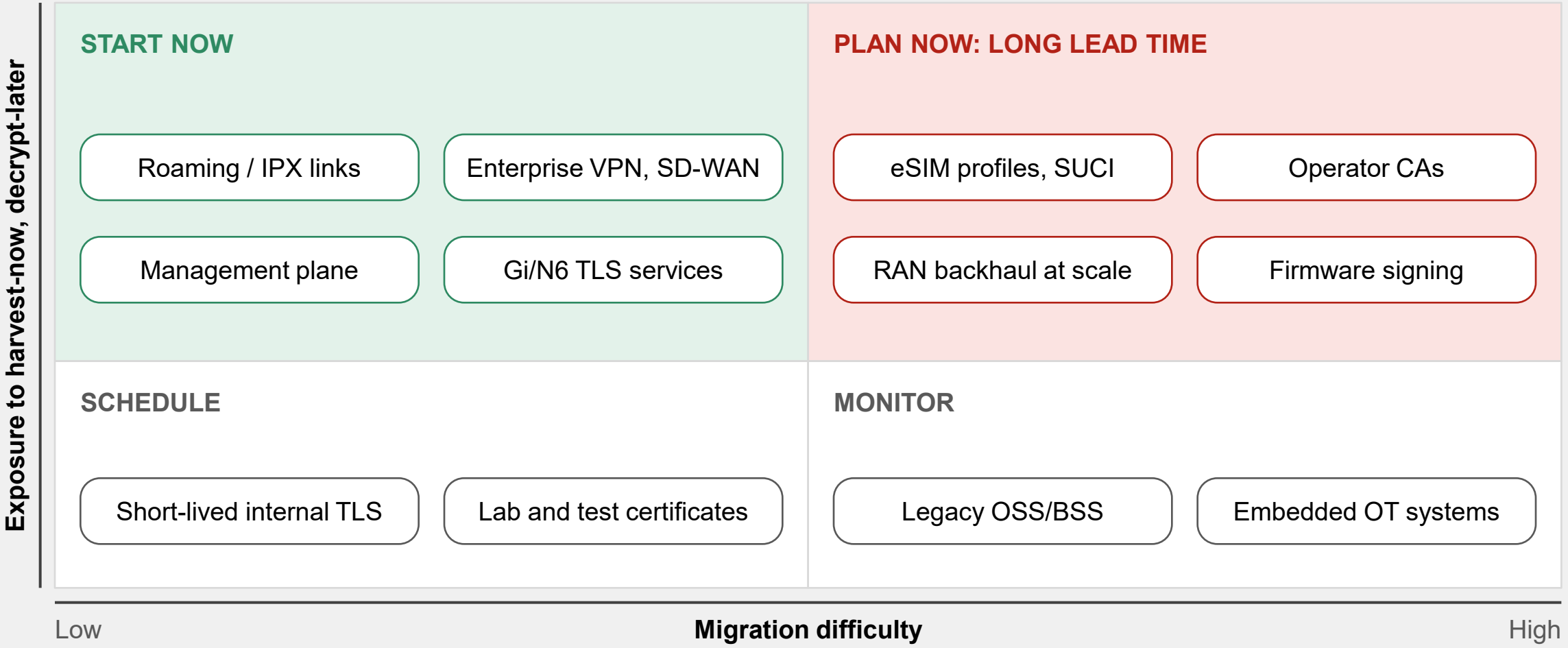
Top sources and destinations still on classical crypto

3 Evidence

The same report every month shows progress to the board and regulator

© Fortinet Inc. All Rights Reserved.

Start where exposure is high and migration is easy

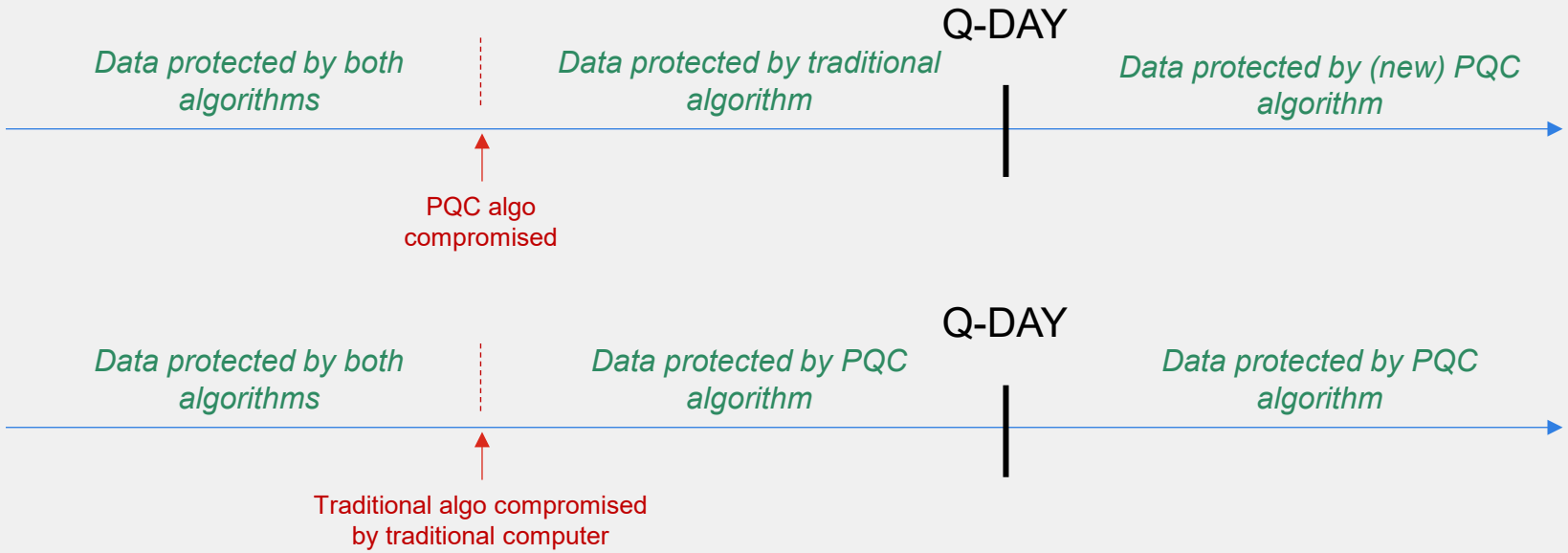


Exposure: how long the data must stay confidential and how easily it can be intercepted. Difficulty: vendor dependency, scale and operational risk. Placement is illustrative; each operator's own report sets it.

© Fortinet Inc. All Rights Reserved.

Hybrid key exchange hedges both quantum and PQC risk

- Two unknowns:
  - When will Q-Day happen?
  - Will a flaw be found in the new PQC algorithms first?
- Hybrid combines classical ECDH with ML-KEM: an attacker must break both
  - TLS 1.3: X25519MLKEM768. IKEv2: ECDH plus ML-KEM additional key exchange (RFC 9370)



© Fortinet Inc. All Rights Reserved.

Hybrid key exchange runs today on TLS and IPsec

Protocol	Where it runs	Hybrid / PQC key exchange	PQC signatures
TLS 1.3	Gi/N6 inspection, service APIs, management access	**X25519MLKEM768** Management GUI, agentless VPN (7.6.5) SSL deep inspection, VIP (8.0)	ML-DSA on management GUI (7.6.5) Public web certificates remain RSA / ECDSA
IPsec / IKEv2	RAN backhaul SecGW, roaming, enterprise VPN	**ML-KEM, RFC 9370** ECDH + ML-KEM (7.6.1) QKD hybrid (7.6.3), PPK RFC 8784	**ML-DSA and SLH-DSA (8.0)** Peers must support it too
PKI and keys	Operator CAs, firmware signing, key custody	**FortiHSM: ML-KEM** Via PKCS#11	**FortiHSM: ML-DSA** FIPS 140-3 validation pending

© Fortinet Inc. All Rights Reserved.

Four places to switch on hybrid first



Roaming and interconnect

WHY

Subscriber and signalling data crosses partner networks you do not control.

HOW

Hybrid IKEv2 on IPX tunnels; log PQC use on N32 TLS.



RAN backhaul

WHY

Every subscriber session rides these tunnels to the core.

HOW

ML-KEM IKEv2 on the FortiGate SecGW; pilot one cluster first.



Management plane

WHY

A decrypted admin session hands over control of the network.

HOW

X25519MLKEM768 on management access; PQC IKEv2 for OAM tunnels.



Managed enterprise VPN

WHY

Government and banking customers are asking for quantum-safe services.

HOW

Sell hybrid IPsec and SD-WAN as a premium managed service.

© Fortinet Inc. All Rights Reserved.

Test four things before hybrid goes into production

1	**Packet size**	ML-KEM-768 adds about 2.3 KB to each handshake. Check MTU and fragmentation on IKE, N32 and Gi/N6 paths.
2	**Throughput**	Measure tunnel setup rate at SecGW scale, and added latency for voice and signalling.
3	**Interoperability**	Test against each roaming partner, gNB vendor and client stack before enforcing hybrid.
4	**Fallback and rollback**	Decide when classical fallback is allowed, log every fallback, and keep a rollback plan per maintenance window.

© Fortinet Inc. All Rights Reserved.

The next 12 months: discover, report, pilot

Discover Months 0–3

- Turn on SSL handshake logging on Gi/N6, roaming and management firewalls
- Upgrade FortiOS where hybrid is needed

Report Months 3–6

- Build a per-domain PQC baseline in FortiAnalyzer
- Rank links on the exposure and difficulty matrix
- Align targets with the national roadmap

Pilot Months 6–12

- Hybrid on one roaming link, one backhaul cluster and the management plane
- Run the four pre-production tests
- Launch a quantum-safe managed VPN offer

Every step runs on firewalls and logging the operator already has in place.

© Fortinet Inc. All Rights Reserved.


FORTINET

MWC GSMA | DOHA 8 – 10 NOVEMBER 2026



Current State of PQC in Qatar

Syed Ahmad Rasool

Information Security Senior Manager

Vodafone Qatar

AI Translation

Current State of PQC in Qatar

MWC Doha
November 2026

Draft

Agenda

01 **Qatar PQC developments**

Recent milestones and industry consultations

02 **Quantum-safe ecosystem**

Research paper perspective and proposed roles

03 **National strategy**

NCSA strategic pillars and sector priorities

04 **Telecom exposure and impact**

Cryptographic interfaces, vulnerabilities and business risks

05 **Strategy and target state**

Migration priorities, policy guidance and vendor readiness

Qatar PQC Timeline – Significant Events from the last meet



NOV 2025

MWC Doha

PQC Briefing

MAY 2026

CRA

Call for Status on PQC

OCT 2026

1st PQC Link

Qatar Established 1st PQC Link

- At HBKU Research Lab

Now

CRA & HBKU

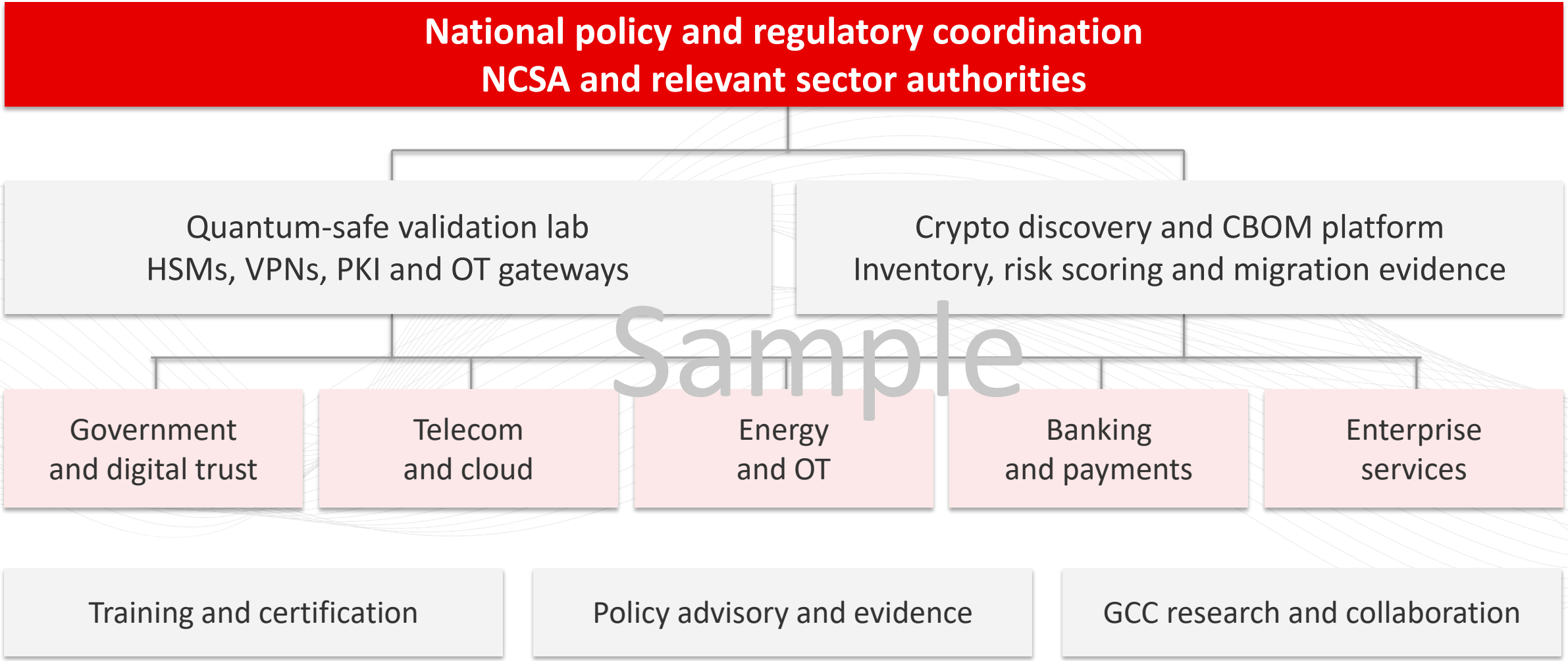
PQC Framework Industry Consultation

NCSA Qatar

Consultation for National Quantum Safe Strategy

Sample

Qatar Quantum-Safe Ecosystem: Research Paper



Sample

Source: PQC - QA.pdf, Al-Khwarizmi Tech Lab, June 2026, Adapted from report.

Conceptual ecosystem proposed in research. Roles and partnerships require agreement.

NCSA Quantum-Safe Strategy: Strategic Pillars – WIP

Qatar National Quantum-Safe Strategy – Work in Progress

Pillars frame the sector's current-state assessment

A **Cryptographic Governance and Policy**

Qatari policy requirements, compliance verification and quantum-safe procurement.

B **Awareness and Communications**

Quantum-threat awareness at all levels and channels to coordinate plans.

C **Participants and Influences**

Stakeholders, national trust services and international partners shaping timelines.

D **Supply Chain**

Critical suppliers' quantum-safe plans, upgrade vs. replace, long-life OT contracts.

E **Infrastructure, Applications, Operations**

OT constraints, expertise, patch windows and performance baselines.

F **Knowledge of Assets Impacted by Cryptography**

Cryptographic inventories, dependencies and long-lived protected data.

G **Cryptographic and Quantum-Safe Technologies**

Tracking standards, CRQC timelines, certificate changes and skills.

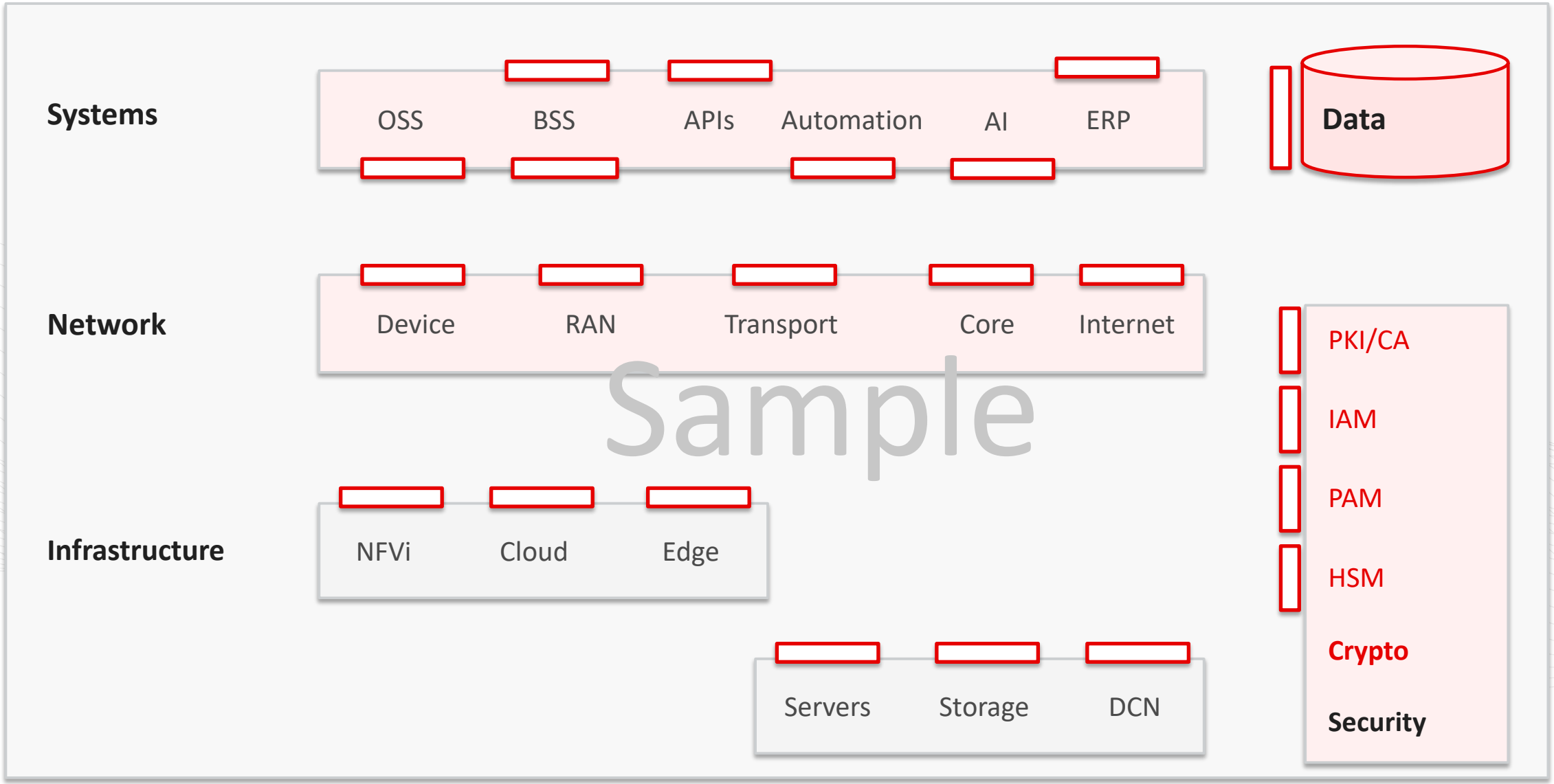
Why it matters

Telecommunications is named critical national infrastructure

Sample

Source: NCSA, Qatar National Quantum-Safe Strategy Workshop Questions.

Interfaces where Cryptography is used in Telecoms



Areas Vulnerable to Attacks

Domain	Confidentiality	Identification	Integrity	Non-Repudiation
Device	Secure user-to-network registration	Identify the user (IMSI) and device (IMEI) to the network.	Critical software (RF baseband) is unaltered	Emergency call origin
SIM/eSIM	Secure user-to-network communication against casual eavesdropping	Identify the user. (The root of trust for user identity).	Data on SIM is unmodified.	Call origin and billing
Network	Secure network signalling	Limit access to network functions to privileged users	Network Function software is not modified	Control plane and routing changes
Systems (OSS)	Secure network topology and configuration	Limit access to management plane to privileged users	Network configuration is not modified	Origin of critical network changes
Systems (BSS)	Keep subscriber account data and call records confidential	Limit access to subscriber data	Ensure subscriber call records cannot be altered	Inter-operator transactions (roaming, unbundled orders) cannot be revoked
ERP	Ensure employee, Financial records are confidential	Limit access to unannounced financial results	Ensure financial records (ledger) are not altered	Payments cannot be revoked
Infrastructure (Cloud)	Ensure data-at-rest is confidential	Limit access to cloud control plane to privileged users	Ensure workloads and configuration are not modified	Origin of workload deployment and updates

Sample

Threat Impact

Quantum Threat	Business Risk	Drivers & New Services
Asymmetric Cryptography at Risk • Shor's algorithm enables exponential speedup in factoring large integers and solving discrete log problems • RSA, elliptic curve, and Diffie-Hellman key exchanges are all vulnerable **Symmetric Protocols Impacted** • Grover's algorithm provides quadratic speedup for attacking block ciphers and hash functions • Mitigation possible through increased key sizes (e.g., AES-256) **Timing and Migration Urgency** • The arrival date of a cryptographically relevant quantum computer remains uncertain • Store Now, Decrypt Later attacks may already be underway	**Store Now, Decrypt Later** • Adversaries harvesting encrypted data today for future quantum decryption • Threatens data with long-lived confidentiality needs: IP, state secrets, bio-data **Code-Signing and Digital Signatures** • Vulnerable algorithms undermine service authentication and software update integrity **Rewriting History** • Compromised signature algorithms threaten audit records, contracts, and call records **Key Management Attacks** • Symmetric keys stored with vulnerable wrappers become exposed	**Network Security** • Quantum threat is an intrinsic driver requiring risk assessments across all cryptographic applications • Covers crypto libraries, PKI, HSMs, networking equipment, and telecom architectures **New Revenue Opportunities** • Quantum-Safe VPNs, SD-WAN, IoT connectivity, satellite links, and cloud storage • Monetisation window during multi-year migration period **Business Verticals** • Financial services: BIS, DTCC, and Banque de France actively testing PQC • Public sector: Government mandates driving operator compliance timelines

Sample

Strategy & Target State

Strategy	Primary Domains	Critical Path
• **Hybrid first:** Use ML-KEM-768 + ECDH in approved TLS 1.3 and SSH contexts. Prefer Curve25519. • **Risk-based migration:** High-priority assets: indicative 2030–2031 or to be realigned with national strategy. Medium/low-risk assets: nominally 2035. • **Crypto-agility:** Enable algorithm changes and secure fallback without reducing security or causing downtime. • **PKI and key custody:** Plan signature migration, maintain key lifecycle controls and engage vendors.	• **TLS / digital services:** Enable and prefer TLS 1.3. Prefer X25519MLKEM768 for hybrid key exchange. • **SSH / management:** Prefer mlkem768x25519-sha256. Other options must follow the standard. • **IPsec / PKI / QKD:** PQC for IPsec, PQC signatures and QKD are under evaluation. • **Radio access:** Algorithm selection follows the separate Radio Access Security Standard.	• **Discover:** Inventory vulnerable algorithms, protocols, certificates and system dependencies. • **Prioritise:** Assess confidentiality lifetime, system criticality and upgrade constraints. • **Validate and govern:** Test approved TLS/SSH hybrids and fallback. Obtain executive approval and assign operational ownership.

Sample

Vendor Readiness (What we need)

- Vendor commitments: approved ML-KEM-768 hybrid profiles for TLS 1.3 / SSH, with tested product versions.
- Roadmaps only for signatures and IPsec PQC. Escalate urgent needs to the Cryptography Standard owner.
- Require trusted implementations, interoperability evidence and throughput / latency impact assessments.
- **Production readiness:** secure fallback, rollback, maintenance windows and documented key-management procedures.



Together we can

GSMA™