Post-Quantum

Cryptography Conference

Update from the GSMA
Post Quantum Telco Network Task Force

Lory Thorpe
Quantum Safe Industry Lead at IBM

ENTRUST HID PKI Consortium

Post Quantum Telco Network Task Force

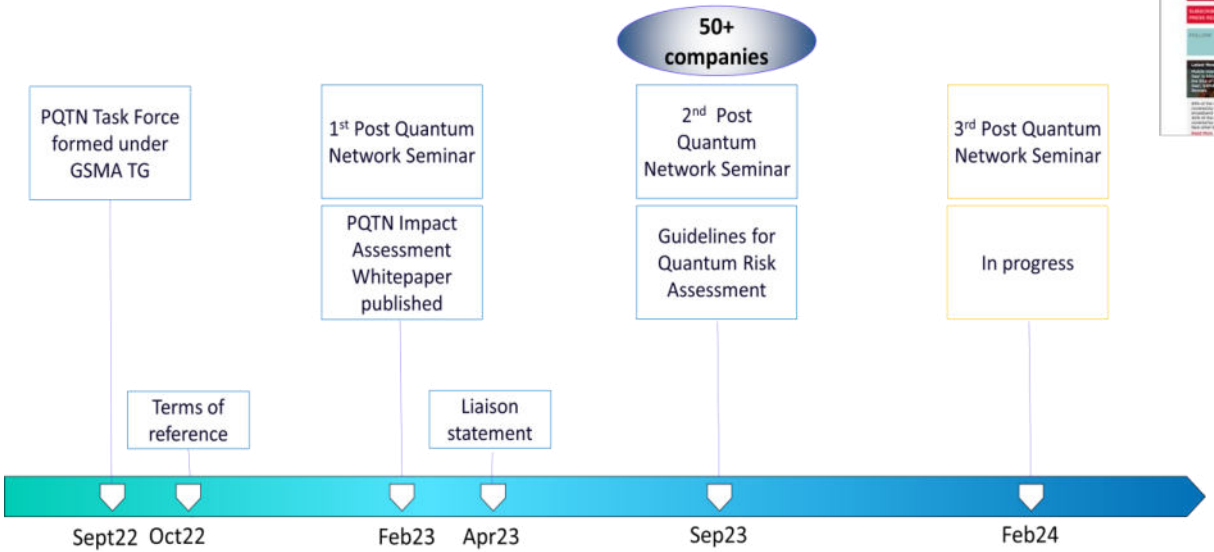
Lory Thorpe, IBM Quantum
Chair PQTN TF

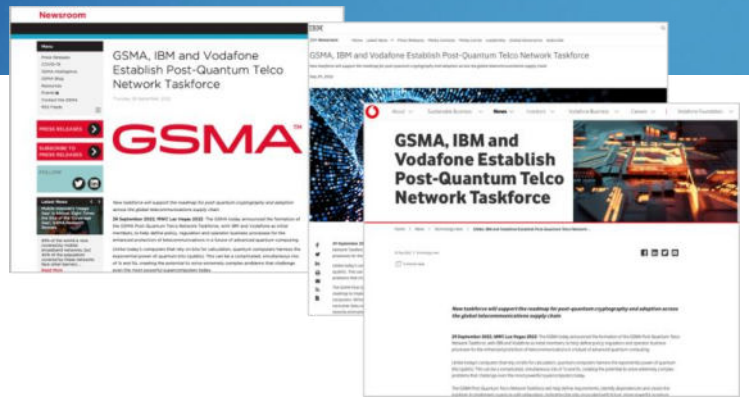
Lory.Thorpe@ibm.com

Agenda

- PQTN TF Timeline
- Why PQTN TF?
- Ongoing Work Items
- Telco Use Cases
- Considerations for the PKI Consortium
- Survey Results

A Timeline of Activities





Post Quantum Telco Network Impact Assessment Whitepaper (Feb 23)

Guidelines for Quantum Risk Management for Telco (Sept 23)

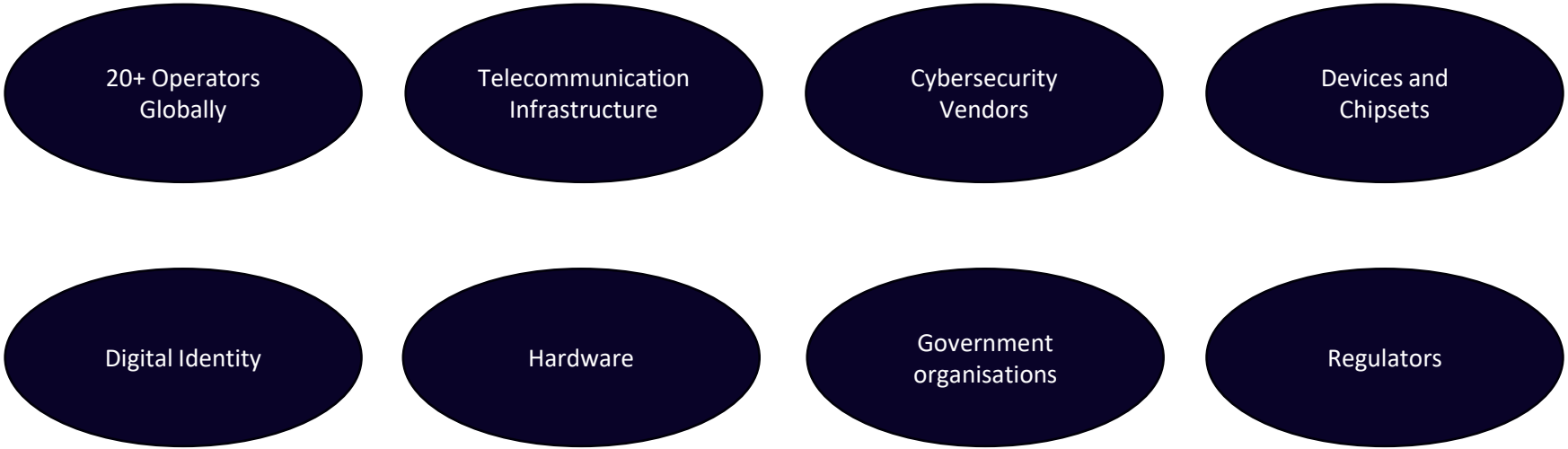
Why PQTN?

Rationale presented to the GSMA Technology Group for the creation of the Task Force in September 22

Problem Statement: The telecom industry has not yet defined the process for adopting **Post-Quantum Cryptography** to secure networks, devices and systems.
Call to action. Define the requirements, identify the dependencies and create a roadmap to implement Quantum-safe telecoms networks.

Who are we?

54 companies are members of the PQTN TF, with a good representation from Operators and the wider ecosystem



Ongoing Work Items

Best practice document	Collaboration	PoCs and Testing experience
Development of **analysis** and **best practice** guidelines for post quantum preparation and migration for Telcos Telco **use case development** **Prioritisation** and **business risk** **PKI** implications	**Education** and **awareness** **Cooperation** and **coordination** with relevant industry bodies, SDOs **Liaise** with **Government** organisations on **policy** and **regulation**, timelines	Proof of Concept **demos** and **showcases** **Test results**, **lessons learnt** and experience sharing, leveraging Task Force and external cooperation

Communication (Post Quantum Network Seminars, ad hoc engagements, etc)

Use cases (Best practice guidelines)

Internal Use Cases
Protection and configuration / management of link between base stations and security gateway
Virtualized network functions (on cloud, on NFV infrastructure)… integrity of the uploaded firmware and VNFs. Authentication of privilege access.
Cloud Infrastructure
Physical SIM
RSP (Remote Sim Provisioning / eSIM), for both M2M (SGP.02), and Consumer Electronics (SGP.22)
Devices and firmware upgrade (linked to code signing and Root of Trust in the device)
Concealment of the Subscriber Public Identifier
Authentication and transport security 4G (MME-S-GW-P-GW)
Authentication and transport security in 5G: Quantum safe TLS between components of 5G core network (Service based architecture)
Quantum safe control plane
Maintaining privacy (GDPR, etc)
Lawful intercept
Billing/charging

External Use Cases
Virtual Private Networks (VPN)
Software defined wide area network (SD-WAN)
Network Operator interworking* (procedures, process, security for interworking between different networks)
Roaming and billing reconciliation
Protecting Critical Devices: Electrical Smart Meters How MNOs could provide Quantum Safe Cyber Security Services for Smart Meters
Prepare automotive for quantum-safe cybersecurity. How could MNO offer crypto-agility services for automotive market

Use case analysis

1. Scope
2. Sensitive data discovery
3. Cryptographic inventory
4. Migration strategy analysis and impact assessment
5. Implementation roadmap (crypto-agility and PQC implementation)
6. Standards impact
7. Stakeholders
8. PKI Implication
9. Legacy impact
10. Actions dependencies

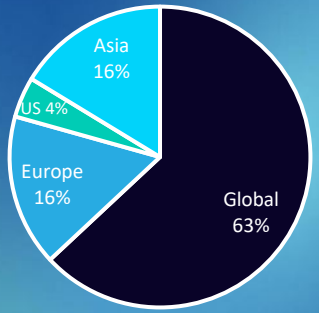
Considerations for the PKI Consortium

We've consolidated an initial list of Telco use cases where we believe post quantum cryptography will have an impact, many of them also rely on PKI.

- How can we leverage synergies between GSMA PQTN and PKI Consortium work?
- Gain better understanding/articulating the benefits and possible dependencies in aligning PKI evolution and Post Quantum activities for the Telcos

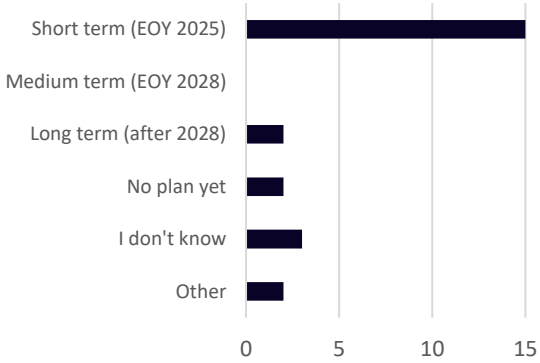
Survey Results

Conducted by PQTN TF to gather insight on risk awareness, timelines, migration plan (Q2 23)

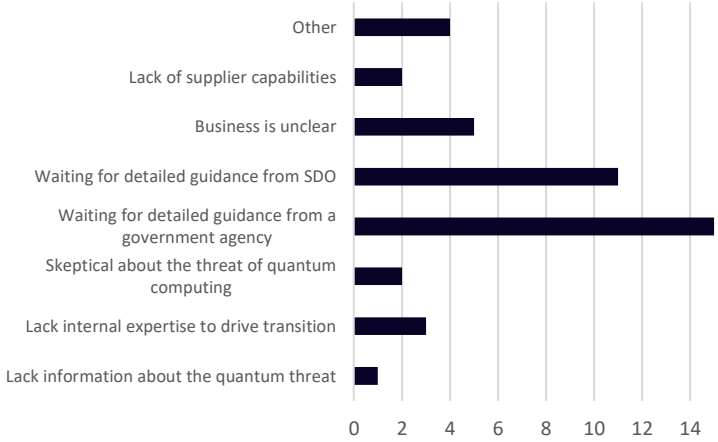


24 responses received (40% operator, 27% Network provider, 13% eSIM/SIM provider, 10% device manufacturer, 3% MVNO, 8% Other)

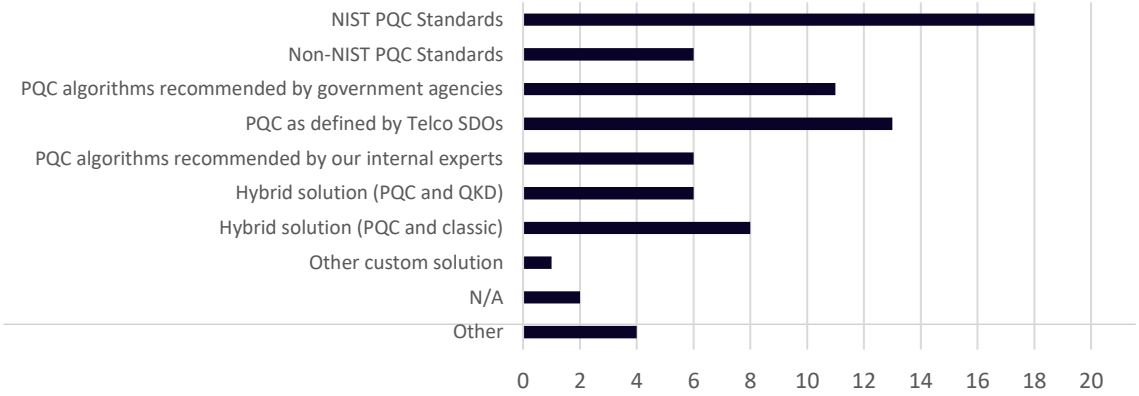
Earliest implementation of Quantum Safe capabilities into your products



What is impacting your plans? (mulitple answers)



Which are you planning to implement? (multiple answers)



Thank you

Post-Quantum

Cryptography Conference

Update from the GSMA
Post Quantum Telco Network Task Force

Lory Thorpe
Quantum Safe Industry Lead at IBM

ENTRUST HID PKI Consortium