Post Quantum Cryptography in Telecom

ITU-T X.509 Day

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

GSMA

GSMA

Join the world's most influential mobile community and access an unrivalled world of practical business benefits.

1,300+
members

Members represent
200+
countries and territories

15,000+
individual experts
engaged through GSMA initiatives and communities

25
operator board members representing nearly
5 billion mobile connections

Have your say on industry-significant developments and challenges and take advantage of high-value networking opportunities with mobile operators and key ecosystem players.

150+
Working Groups and projects
active globally, driving standards and innovation in areas such as roaming

10,000+
active users on Member Gateway
GSMA's Member Extranet allows for collaboration online and in-person year-round

9
GSMA Connected Communities
connecting areas including manufacturing, fintech, mobile AI and IoT with the mobile ecosystem

GSMA Working Group Portfolio

GSMA Working Groups are cooperative networks that bring together industry stakeholders to address shared challenges, enhance interoperability across the telecommunications ecosystem, and support enabling technologies.

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 205)
Standard for Hash-based digital signature scheme

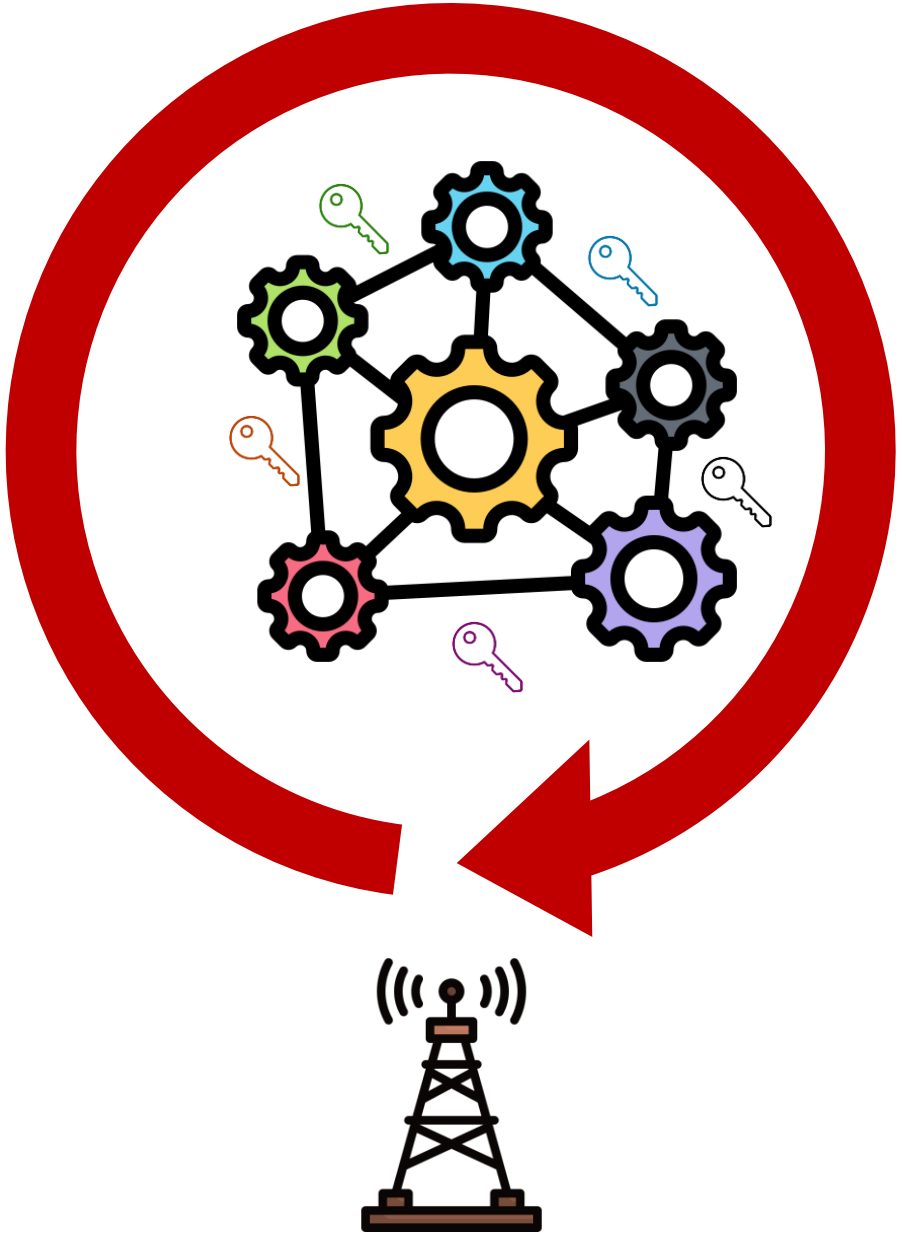
GSMA™

Post Quantum Cryptography – Quantum Computers Attacks

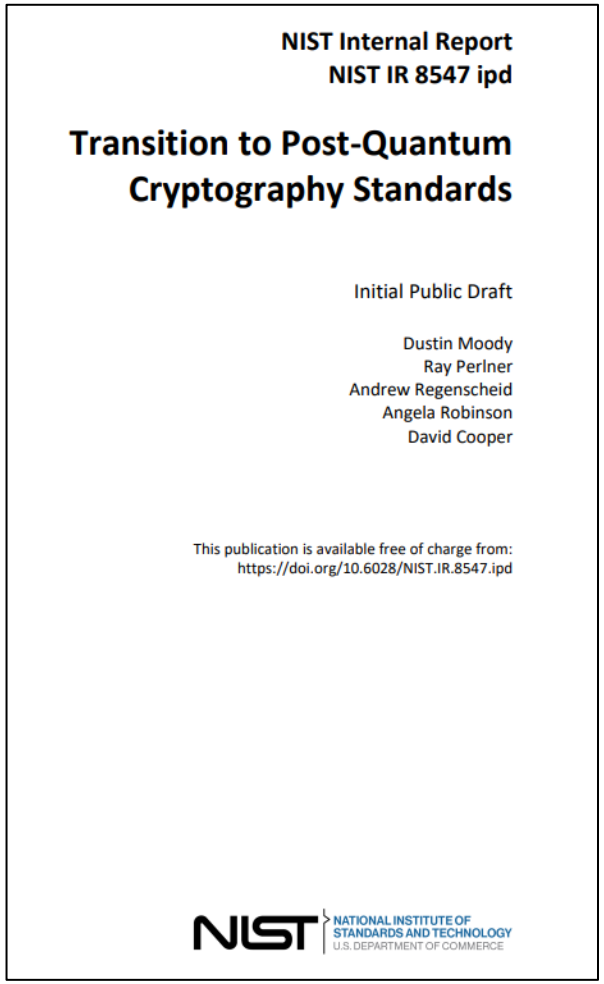
The Question isn't when this Q-Day will arrive

GSMA

Post Quantum Cryptography – Crypto Migration



Post Quantum Cryptography – 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

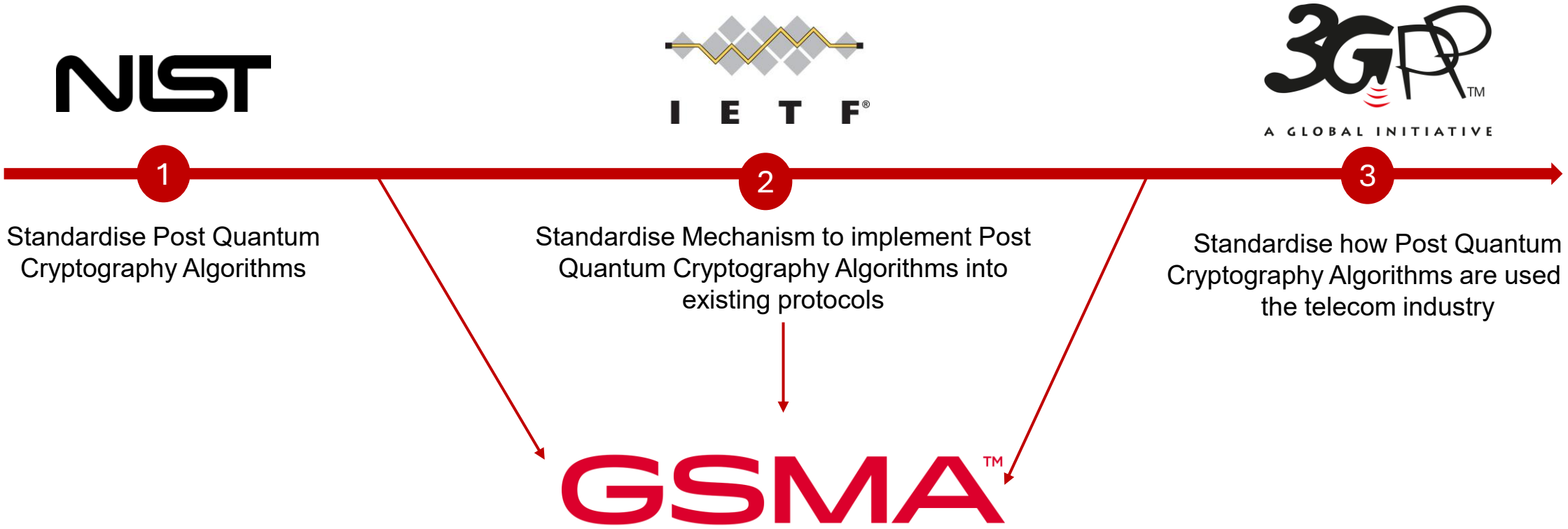
By Dec 2030, High risk use cases transitioned

By Dec 2035, Medium risk use cases transitioned

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

GSMA

Post Quantum Cryptography – GSMA Role



Build awareness of post quantum migration plans

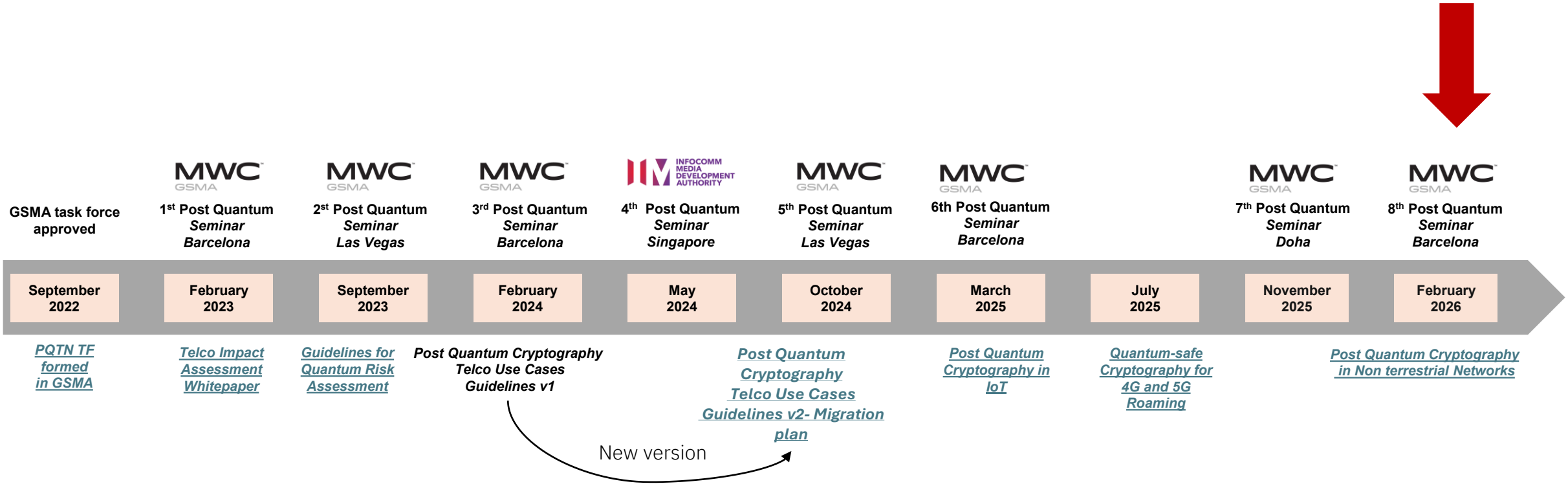
Develop skills on post quantum migration

Identify gaps on the telco industry standards

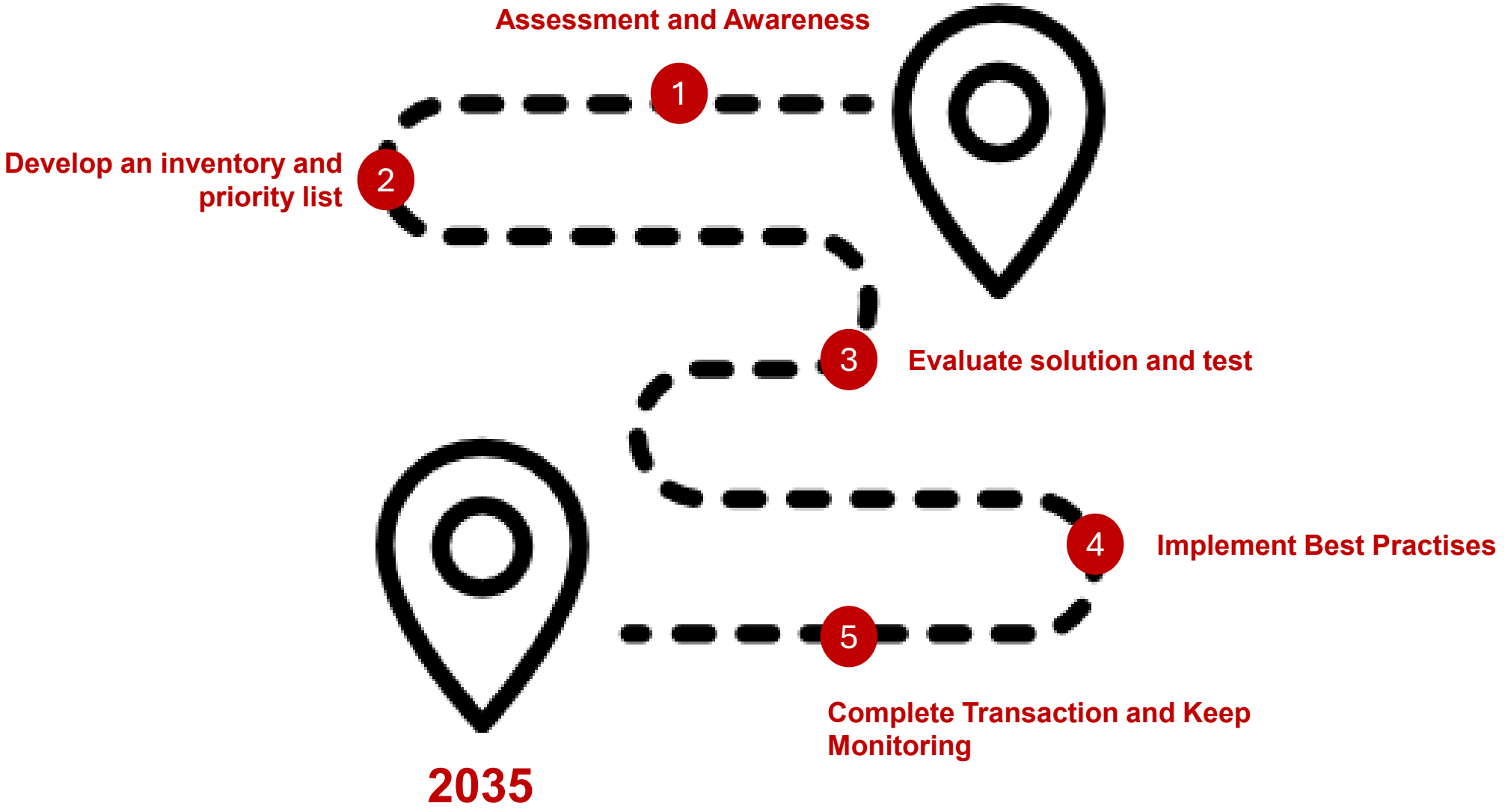
Testing and provide best practice guidelines

GSMA

Post Quantum Cryptography – GSMA Post Quantum Telco Network Taskforce



GSMA Post Quantum Telco Network Taskforce - Crypto Migration Roadmap



GSMA Post Quantum Telco Network Taskforce – Work in progress

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

Practical experience sharing: implementation of a hybrid key exchange mechanism to support migration of IPSec/IKEv2 in the base station connection to the mobile core.

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

GSMA

Join Us!

Lory Thorpe, GSMA PQTN TF Chair
lory.thorpe@ibm.com

Luke Ibbetson, GSMA PQTN TF Vice Chair
luke.ibbetson@vodafone.com

Yolanda Sanz, ysanz@gsma.com