No.75
March 12th 2024

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/ NOT SPONSORED**

A Quantum-Safe Roadmap for Telcos

This Briefing is an extract from HardenStance's new report "MWC24: Taking Stock of Telco Security", to be published on March 14th. The quantum safety content that features in this Briefing is exactly the same as features in the broader post-MWC report.

- Quantum safety was well represented at Mobile World Congress this year. It was accorded a status that was proportionate to the risk posed to its telco members.
- Quantum safe strategies should prioritize raising awareness of requirements and challenges, executive buy-in, and an inventory of current cryptographic systems.
- Post Quantum Cryptography algorithms are still quite immature. Those selected by the U.S National Institute for Science and Technology (NIST) are expected to be standardized later this year. China and South Korea are developing their own. Some countries are adopting NIST's algorithms; others are keeping their options open.
- The most pressing requirement for accelerating telco investment roadmaps is direction and timelines from regulators. The EU will publish a recommendation soon.

Assets leveraging contemporary protocols are going to need to be upgraded to PQC algorithms.

Crypto inventories and migration challenges

The threat posed by quantum computers to the integrity of all contemporary encryption standards is years away. And yet at the same time, the threat from Store Now Decrypt Later (SNDL) attacks carried out today is real in the here and now (see the box below).

The migration of an organization's cryptographic assets to quantum safe algorithms will take place over many years. Assets leveraging contemporary protocols such as TLS, HTTPS, SSH and IPsec are going to need to be upgraded to Post Quantum Cryptography (PQC) algorithms. In the interim, or in parallel, hybrid key distribution solutions with pre-shared keys that harden existing encryption standards or borrow from both current and post quantum encryption algorithms and architecture will need to be deployed. This Briefing focuses on the challenge this represents from the perspective of the telecom sector. However, the same core principles also apply to other sectors of industry, especially other industries that fall into the category of critical infrastructure.

The Threat from Store Now Decrypt Later (SNDL) attacks

The threat quantum computers pose to the integrity of contemporary encryption standards is imminent at the same time as it is years away. The years we have left until "Q-Day", when a quantum computer can crack our current systems, is hotly debated. Estimates range from two years to more than twenty.

Nevertheless, rival nation state intelligence agencies are already working on – or executing on – Store Now Decrypt Later (SNDL) attacks, also called Harvest Now Decrypt Later (HNDL) attacks. These involve data being copied – potentially today – and then stored for many years without actually being decrypted. Come Q-Day, decryption of some of that old data, even at that point, will still retain the power to cause a lot of harm. For example, some personal medical data can remain sensitive for many years. From a national security perspective, examples include the layout of missile silos or other military or defence facilities, as well as the conversations of Presidents and Prime Ministers.

A quantum-safe roadmap for telcos is going to be a vast undertaking:

- The scale and variety of cryptographic assets deployed across a telco's IT and telecom infrastructure estates is huge. Most telcos lack visibility into either a substantial or very large subset of those assets. Many, if not most, vendors don't have an inventory of the cryptography in their products and they have "lost" certificates hard coded into software. Telcos often don't know which of their vendors have certificate credentials deployed in their products – or they may know that they use them but they don't know how they use them. Back in 2018, expired Ericsson certificates were the cause of substantial mobile services outages in the UK (O2) and Japan (Softbank).
- The challenge of undertaking a comprehensive asset inventory in a telco isn't just a technical one. It's a human, organizational and political one too. Hands up which head of department wants to cooperate in a crypto asset discovery exercise that might expose vulnerabilities that have left the organization exposed for years? If there is no executive buy-in behind a discovery exercise or audit – and with very few exceptions today, there isn't – what's the motive for supporting it?
- When it comes to prioritizing use cases for cryptographic upgrades, the telco context is unique. Customer data is potentially at its most vulnerable when it's in transit, which makes this a critical priority. But telecom sector regulators are becoming increasingly prescriptive about how telcos defend the network itself against being breached. That makes investment in adequate protection for telco network management interfaces a much higher priority for upgrades than it was in the past.

The most striking example of this sector's relative immaturity is the way the SIKE PQC algorithm was hacked by Belgian researchers.

The development and selection of new PQC algorithms

Post quantum cryptography is a very new discipline. As such, the efficacy, maturity and operability of individual algorithms is still largely unproven. Each algorithm will have to undergo a long process of proving itself in live operations. The most striking example of the sector's relative immaturity is the speed and ease with which the SIKE PQC algorithm was hacked. SIKE was one of a second group of four additional candidate PQC algorithms selected by NIST for post quantum key establishment in the summer of 2022. It was hacked by Belgian researchers within four weeks of NIST selecting it.

More encouragingly, NIST's first group of four algorithms has so far proven resistant to attack. The first of these is CRYSTALS-Kyber for establishing asymmetric (public-private) encryption keys, which are then used to share a symmetric encryption key based on an algorithm such as AES. The other three are CRYSTALS-Dilithium, FALCON and SPHINCS+. These are for digital signatures – for example, when there is a need to verify identities for a digital transaction or remotely sign a document.

The expectation is that these first four will be ratified as standards following the fifth PQC standardization conference in Rockville, MD in the U.S next month (April 10th – 12th). This would then allow for vendors to start embedding the first PQC algorithms into protocols and product from the second half of this year.

Apple is among the early, pre-standardization, adopters of Kyber

Global cloud providers and applications ecosystem leaders have already started adopting pre-standard versions of the NIST algorithms. The week before Mobile World Congress, Apple announced that it has integrated a pre-standard version of the Kyber algorithm into iMessage. This is with effect from iOS 17.4 which was released on March 5th. This forms part of the privacy features arms race between the big messaging players. Apple follows Google Cloud Platform (GCP), Google Chrome, AWS and Cloudflare, all of which have implemented one or more pre-standard versions.

The NIST algorithms are pivotal but there are also other options

According to Annex A, Table 4, of the GSMA's "Post Quantum Cryptography: Guidelines for Telecom Use Cases" (see "More Information" at the end of this Briefing), so far only China and South Korea have formally committed to developing their own PQC algorithms. That said, a number of other countries are still considering other options at the same time as they are considering NIST's algorithms. The European Commission will shortly be publishing a recommendation on European policy (see page 5).

Crypto agility will extend beyond just reducing the cost of swapping out legacy cryptographic primitives to one that drives automated end-to-end cryptographic lifecycle management.

The costs of upgrading will be susbtantial

There will be costs to upgrade to PQC algorithms in software – and significantly higher costs for doing it in hardware. So-called 'crypto agility' is going to become an increasingly important requirement. The requirement here will extend beyond just reducing the cost of swapping out legacy cryptographic primitives to one that drives flexible, automated, end-to-end cryptographic lifecycle management.

There will be all manner of additional capex and opex implications to contend with too. The PQC algorithms will have an impact on CPU consumption, memory, latency and other end to end performance metrics across networks, services and applications. Moreover, each of the new algorithm's impact on performance will be unique. Vendors that have not taken adequate account of the impact of upgrades on the physical and mechanical side of their designs may find themselves having to respin hardware.

Hybrid solutions will form part of the roadmap but aren't yet defined

For now, there doesn't appear to be much agreement as to how "hybrid" solutions should be defined but they are going to be a key part of the roadmap. If precedent is anything to go by, vendors will decide for themselves whether or not to adopt the term, independent of any broader market sentiment.

Vendor solutions for making current crypto more quantum resistant

As well as planning to deploy new PQC algorithms, further hardening of existing encryption standards against quantum threats will also form a part of telecom sector roadmaps. Here are two examples:

- **Nokia**: From its IP/Optical portfolio, Nokia promoted an adapted and layered approach to quantum-safe networks. This uses a physics-based cryptographic offer, enabling IP, MPLS, Ethernet and Optical connectivity. This solution leverages Pre-Shared Keys, symmetric out of band distribution, and AES cipher block encryption techniques to harden engineered connectivity against the quantum threat today. To scale this solution, Nokia promotes its widely deployed, and NATO certified, 1830 SMS (Security Management Server) centralized key management platform. The solution works with Nokia's 1830 family of WDM optical line systems, as well as at L2, L2.5 and L3 with the Nokia 7750 Service Router portfolio.
- **Juniper**: Juniper has completed integration of its vSRX virtual firewall with the new Symmetric Key Agreement Platform (SKA) from Arqit Quantum Inc. Arqit's development of the SKA has been driven by President Biden's White House National Security Memorandum #10 of May 2022. This mandates that U.S government agencies must adopt symmetric key protections for National Security Systems (NSS) to meet the challenge of quantum computing.

  Arqit has found a way of augmenting the symmetric key exchanges in the establishment of IPsec tunnels to make them more quantum resistant. The SKA is designed to be both complimentary to and compliant with IPsec, as well as compliant to National Security Memorandum #10. Juniper supports IPsec across its telecom operator product and services portfolio across fixed and mobile networks, including the MX router series as well as the SRX firewall.

In principle, though, the definition ought to involve the combination of contemporary and PQC algorithms together in such a way that you remain protected come "Q-Day". And if advances in cryptanalysis make it possible to break a PQC algorithm before Q-Day – which is certainly plausible as demonstrated by the vulnerability that was quickly discovered in SIKE– then you remain protected by the contemporary algorithm. This allows PQC algorithms to be phased in gradually - you deploy hybrid on a server, and any client that supports PQC uses both algorithms in hybrid mode, while any older client that doesn't have PQC just uses the classical one. Hence elegant support for hybrid deployments will be a critical component of crypto agility.

Telco trials and supporting cryptographic management software

During Mobile World Congress, HardenStance spoke with Thales and SandboxAQ about their pre-standard PQC deployments with SKT Telecom and Vodafone, as well as with DigiCert and Ericsson, about what they can offer by way of cryptographic management solutions. Profiles of all four companies and their value propositions follow below:

Thales

Through its world leading SIM card business, extensive portfolio of encryption solutions, and dedicated 5G security portfolio, Thales is deeply embedded in the cyber security roadmaps of many of the world's leading telcos.

Softbank has tested the performance of contemporary elliptic curve-based encryption protocols against several pre-standard versions of the NIST algorithms.

Thales is can point to one of the strongest POC proof-points in partnering the telecom sector for quantum safety roadmaps. Last December, the company announced that South Korea's SK Telecom had successfully trialled Thales 5G PQC SIM cards in its 5G SA network. This used a pre-standard version of Kyber. The partners made progress in understanding some of the implications and requirements on the handset side for managing a PQC algorithm's larger key sizes.

The OS upgradeability feature of the Thales 5G SIM has potential to make an important long term contribution to crypto agility. The company reckons 99% of an OS can be upgraded over the air. That includes any crypto algorithms, whether they be contemporary or future PQC algorithms. The Hardware Subscriber Module (HSM) side of Thales, which counts big telecom names among its customers, including Ericsson, is also doing early work on quantum safety. In early trials, Thales has been renewing RSA or other contemporary certificates with PQC certificates. The same types of trials with pre-standard versions of all four of the NIST algorithms are underway with the company's extensive portfolio of high speed encryption products for protecting data in motion.

Thales observes that the banks are currently leading with preparation for the post-quantum era to protect themselves against financially-motivated cyber attacks. Telcos, which are more likely to be targeted by nation state cyber operations, are behind.

SandboxAQ

SandboxAQ is an enterprise SaaS company, which describes itself as providing solutions at the nexus of AI and quantum technology. The company's core team came out of Alphabet Inc. Its Chairman is former Google CEO and Chair, Eric Schmidt. SandboxAQ's Security Suite is a cryptographic management software platform that provides a full range of services for achieving cryptographic agility. Central to its' value proposition is saving time through automated discovery and management of cryptographic assets as well as the remediation of flaws such as obsolete certificates. Across its portfolio, the company partners NVIDIA to simulate quantum mechanics using AI.

The company has already published customer case studies with Vodafone and Softbank. With Softbank, SandboxAQ has tested and compared the performance of contemporary elliptic curve-based encryption protocols against several pre-standard versions of the NIST PQC algorithms. To deliver Quantum Key Distribution (QKD) solutions, SandboxAQ is partnered with EvolutionQ. SandboxAQ promotes the company's BasejumpQDN, a

software layer that manages and secures QKD delivery and optimizes QKD use for efficiency, what it calls 'adaptive network stability', and reduced latency.

DigiCert

DigiCert is one of the world's leading providers of high-assurance TLS/SSL, PKI, IoT and signing solutions. One of the company's core missions at MWC was to reinforce its credentials as an established player and partner as telcos prepare to undertake their migration to PQC cryptography. Its' value proposition comprises three core pillars.

Standards: DigiCert has a deep understanding of the PQC algorithms themselves. It has worked closely with the NIST algorithm selection process and also has a rich pedigree of working with standards organizations like 3GPP on encryption and signing requirements for the telecom sector. DigiCert has deep understanding of how PQC cryptography differs from contemporary standards as well as how different NIST-selected algorithms compare to one another in terms of key sizes and how that impacts telecom networks.

DigiCert leverages AI/ML as part of the process of determining which assets are most and least vulnerable to the quantum threat.

Products: DigiCert has a portfolio of crypto discovery and lifecycle management products. For discovery, the company can deploy its own product or integrate with existing discovery solutions. It leverages AI/ML as part of the process of determining which assets are most and least vulnerable to the quantum threat.

DigiCert is a proven leader in automated lifecycle management and brings that portfolio to bear in the PQC era. The company points to how the cracking of the SIKE PQC algorithm demonstrates how important it is to be able to introduce and replace different algorithms in an organization's infrastructure with minimal disruption – a key component of crypto agility.

Advisory: DigiCert's advisory service brings the human and organizational know-how to help leaders and their teams navigate the many internal challenges of creating and adhering to a quantum-safe roadmap. It can help align people, processes and technology to de-risk that migration plan.

Ericsson Security Manager (ESM)

While it's unlikely to be in any way fully competitive with specialist cryptographic management software platforms, Ericsson does position the Ericsson Security Manager (ESM) as capable of supporting cryptographic inventory for telcos. Among its crypto features, ESM can assure that the right encryption is being applied for each interface, whether it be an internal or external interface.

Regulatory impetus is urgently needed

As was shared in the GSMA's Post Quantum Networks seminar on the Monday of MWC, deliverables generated by the Post Quantum Telco Task Force are already demonstrating the critical importance of telcos collaborating to navigate this challenge. The most recent example of this is the "Post Quantum Cryptography – Guidelines for Telecom Use Cases" report which was released the week before MWC. In the case of 80 – 90% of the use cases identified, the Task Force has identified gaps in 3GPP and other standards that are going to need to be closed in order to align with operator requirements for optimally supporting post quantum cryptography.

Whether it be in terms of identifying and scoping out use cases, sharing best practice on internal organizational change, or generating requirements for vendors, no one telco can be an island. In any one country or region, telcos and their vendors urgently need guidelines and timelines from regulators to help ensure all players are pointing in the same direction, making common assumptions, leveraging the same toolsets, and sharing best practices in the same industry fora. Those charged with driving the necessary change are becoming impatient for regulatory intervention now.

In some cases this may be an excuse for delay but in others it's a genuine recognition of the need for a common regulatory platform from which they can start building out a quantum safe roadmap on the right footing.

The European Commission will publish a recommendation "soon"

The EU Commissioner for the Internal Market, Thierry Breton, gave a surprisingly under-reported speech on the Monday of MWC entitled "Changing the DNA of our Connectivity Infrastructure." HardenStance found his comments singularly confusing, albeit they did at least contain the promise of greater clarity "soon".

According to the European Commission's own transcript of his speech, Commissioner Breton told the Mobile World Congress audience the following:

> *"To safeguard critical applications from the risk of potential attacks, we need to develop strategies to transition to quantum safe digital infrastructure.*
> ***The first step in this direction is developing European post-quantum standards and then deploy them across the whole of Europe**.*
> *We will soon present a recommendation to that effect."*

HardenStance found Commissioner Breton's comments singularly confusing, albeit they did at least contain the promise of greater clarity "soon"

Unfortunately, Commissioner Breton's words can legitimately be interpreted in at least three very different ways:

Possible interpretation #1: *The Commission doesn't want Europe to be reliant on NIST's post quantum algorithms because it doesn't trust that America's National Security Agency (NSA) won't have a backdoor into them*. At this point much of European industry, the telecom sector included, would appear to be assuming the adoption of the NIST algorithms. At this time, there is no evidence of any political mandate for European alternatives (and the Commissioner is nearing the end of his term anyway). It would take a lot of time to develop European alternatives, albeit the UK, Germany, Austria and Switzerland are all strong in cryptography. Such a scenario could conceivably allow for the initial introduction of the NIST algorithms in Europe, while also making the adoption of future European-developed algorithms optional or mandatory. It cannot be ruled out that this literal interpretation of the Commissioner's words may be the correct one.

Possible Interpretation #2: *The EU will soon make a recommendation on post quantum safety but it will be on regulation - not standardization as stated.* This will provide regulatory guidelines that this, that or the other sector of industry must implement quantum safe encryption in a, b, c phases by this, that or the other date (with an implicit or explicit assumption that the NIST algorithms will be embraced).

Misleading language was used because poor speech writers didn't grasp that 'standardization' and 'regulation' are fundamentally different rather than interchangeable. While the first half of this interpretation could be correct, it's very unlikely that the second is. The Commission is surely too well-oiled a bureaucratic machine when it comes to speech writing and checking to make an error of this kind.

Possible Interpretation #3: *As above, the EU will soon make a recommendation on post quantum safety but it will be on regulation - not standardization as stated.* The use of misleading language was deliberate – no more than political hi-jinx by the Commission. It was a dog whistle to fears of deepening dependence on U.S technology with post quantum crypto, albeit with no plan to actually do anything about it.

In this case, the inappropriate use of the term 'standardization' can (sort of) be justified because the European Telecommunications Standards Institute (ETSI) is, of course, developing what genuinely are "European post encryption standards". ETSI, however, is specifying the interfaces that will manage the operation of PQC algorithms in live networks; ETSI isn't specifying the PQC algorithms themselves.

It's good that the Commissioner committed to releasing a recommendation "soon" because European industry is poorly served by the current ambiguity.

Much more to come at MWC 2025

At the end of last year, BT, Fortinet and Arqit Quantum Inc announced the launch of an integrated product for quantum-safe VPN communications using Arqit's Symmetric Key Agreement (SKA). It followed the successful trial of quantum-safe tunnels between three BT sites in London, Exeter and Suffolk.

At MWC the week before last, BT's Chief Network Officer, Greg McCall, gave an interview to Telecom TV in which he said: "I predict that if it's not this year, then next year quantum will be a headline here in the same way that AI is going to be this year." This is a sound prediction. This year it felt as though the touchpaper was lit on the topic of quantum safe networks. Coverage is indeed likely to be greater still next year. ■

More Information on post quantum safety

- **GSMA event recording:** "Third Post Quantum Network Seminar" (MWC 2024)
- **GSMA Guidelines:** "Post Quantum Cryptography: Guidelines for Telecom Use Cases" (February 2024)
- **SandboxAQ**: Softbank Tests PQC Algorithms with SandboxAQ (October 2023)
- **The Ponemon Institute (sponsored by DigiCert):** "Preparing for a Quantum-Safe Future" (October 2023)
- **Nokia:** "Quantum Safe Optical Networking"

More HardenStance events and reports

- **Virtual Event**: Register for HardenStance's two-day "Telecom Threat Intelligence Summit 2024", taking place on June 11th and 12th 2024.
- **Briefing**: "Telco Strategies for Consumer Security" (January 2024)
- **Blog**: After Kyivstar, Which Telco's Next? (January 2024)
- **White Paper**: "Telco Security Takeaways from the NIS2 Directive" (Nov 2023)
- **Report**: "Risk Management in the Telco Spotlight" (September 2023)
- **Briefing**: "Threat Intel in Telecoms (TTIS 2023)" (August 2023)
- **White Paper:** "Aligning Spectrum Policy with Cybersecurity Goals" (May 2023)
- **Briefing** "MWC23: Taking Stock of Telco Security" (March 2023)
- **Briefing**: "Securing IP Services in Router Silicon" (March 2022

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, OASIS, ETSI and TM Forum. HardenStance is also a formally recognized Cyber Threat Alliance 'Champion'. **www.hardenstance.com**.

To receive an email notification whenever HardenStance releases new reports in the public domain, register here (there are only four fields): **Registration Link**.

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness,

noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.