thalescpl.com

THALES

Upgrading Existing Security Systems to Agile Quantum-Safe with SafeNet Luna HSMs and SafeNet High Speed Encryptors

White Paper

Contents

Background

This solution brief will focus on the use of SafeNet Luna Hardware Security Modules, SafeNet High Speed Encryptors, and ISARA's quantum-safe solutions to enable the most seamless, trustworthy and cost-effective method of transitioning to quantum-safe security while maintaining backward compatibility with existing systems. The challenges and solutions outlined below will show how this is possible without compromising current National Institute of Standards in Technology (NIST) approved algorithms.

In 2015, the National Security Agency (NSA) issued a statement declaring, "For those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, we recommend not making a significant expenditure at this point, but instead to prepare for the upcoming quantum resistant algorithm transition."[1] The motivation for this statement is the impending arrival of large-scale quantum computers powerful enough to pose a threat to today's encryption. It is no longer a question of "if," but "when" this level of cryptographically-relevant quantum computing will be available.

There are various opinions ranging from 4 to 14 years[2] from academics, quantum computer developers and industry players for when we will see a large-scale cryptographically-relevant quantum computer in the hands of a nation-state. It is undisputed however that, the race to introduce large-scale quantum computers is on. Several recent bills proposed by the United States Congress to include the recently passed National Quantum Initiative Act (NQIA) are designed to ensure that the United States and her allies are the first to achieve quantum computing. However, other nation-states have invested heavily with national strategies to capture first-mover advantage in the introduction of useful quantum computers. They have also invested in other quantum technologies for offensive and defensive commercial and national security purposes.

For defense purposes and risk mitigation to critical infrastructure, Thales and ISARA believe government and commercial organizations should plan to have protection in place in their security systems to defend from any potential quantum computer attacks no later than 2023. The Five Eyes (FVEY) intelligence agencies believe that encrypted data is currently being harvested and stored by adversarial nation-states. Although this data remains secured with NIST-approved Suite B algorithms today, an attacker with a large-scale quantum computer will possess the ability to break this encryption, rendering the data completely vulnerable. This is known as "harvest and decrypt". Therefore, data requiring secrecy beyond 2023 is already at serious risk of compromise.

Fig 1. Crypto Agility for IoT / Digital Transformation

1 NSA IAD [Online]. Available: https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

2 M. Mosca, "Cybersecurity in an era with quantum computers: will we be ready?" [Online]. Available: https://eprint.iacr.org/2015/1075.pdf and L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner and D. Smith-Tone, "Report on Post-Quantum Cryptography," April 2016. [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/8105/final

Government policy dictates that Government agencies and departments rely on direction from the NSA and NIST on which encryption algorithms can be safely used to secure systems, both classified and unclassified. Today, Suite B is the approved set of algorithms permitted to encrypt data and systems. For the future, NIST is evaluating several possible quantum-safe algorithms to protect Government systems.

Their evaluation is expected to take five years or more to complete. It will take an additional three to five years for Original Equipment Manufacturers (OEMs) to move forward with implementing the approved quantum-safe algorithms into their systems and hardware/software solutions. Implementation of these new quantum-safe products will add additional years to the process. This opens critical systems to significant risk prior to transition work starting.

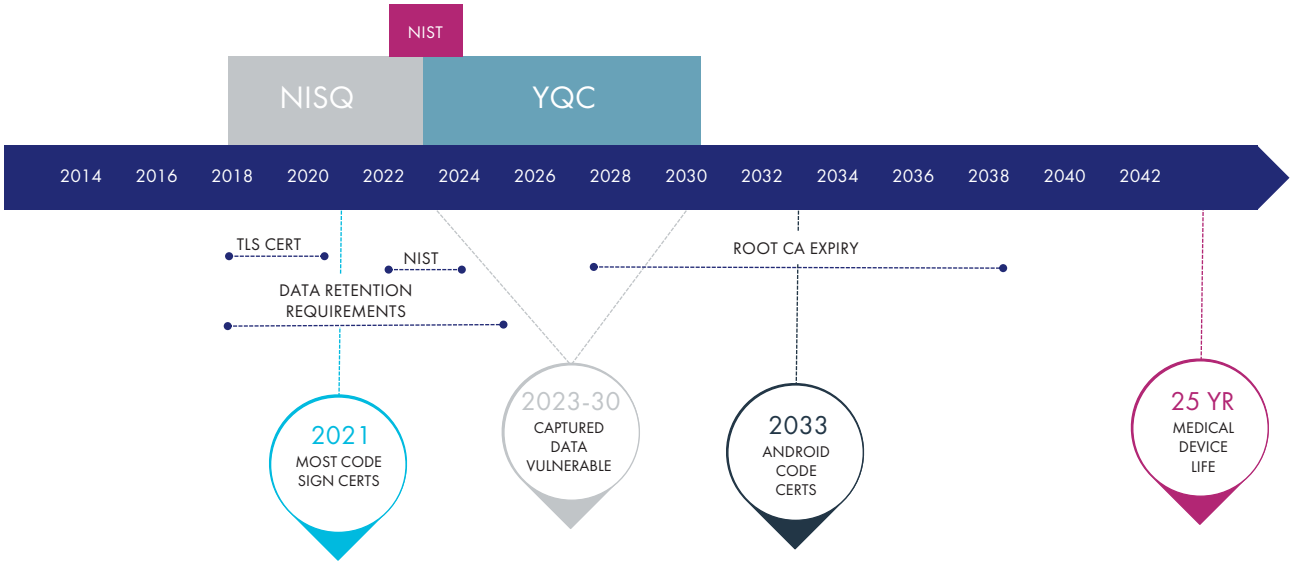

Fig. 2 Data Protection Quantum Timescale

Past experience has proven that updating encryption within Government systems and commercial organizations is a costly, logistically challenging and a time-consuming process. It is our belief that waiting for NIST's next approved suite of quantum-safe algorithms is not practical, since it will leave organizations vulnerable to potential quantum computing attacks and will not allow enough time to address this threat before it materializes. Agile cryptographic design and hybrid encryption solutions will be critical to bridge the gap between the time it will take to upgrade embedded cryptography and NIST publishing their algorithmic recommendations. It is critical that government and commercial organizations begin to address this transition now through identification of vulnerable cryptography, prioritizing high-risk components and commencing the necessary testing and proof of concept work.

Challenge #1 - Public Key Infrastructure (PKI) Migration to Quantum-Safe

The asymmetric algorithms upon which Public Key Infrastructures (PKIs) are based, will need to be made quantum-safe before they are susceptible to total compromise by a large-scale quantum computer. Even though the threat to PKI will not be realized in the immediate term, the time required to upgrade PKIs and all dependent systems will likely take a decade or more. Migrating this environment in time will be a challenge.

In examining this migration, a seamless and cost-effective solution must consider some of the following properties:

- What is the impact to the end user? This includes both the user experience and the client hardware used.
- What is the computing load it places on the server infrastructure?
- What is the impact to the continuity of operations/backwards compatibility within PKI?
- What is the impact to the security of the system?
- How easy is the management of this transition? (e.g. resources required - time)
- What is the cost of making this transition?

There are limited solutions to consider. A logical starting point would be to wait until all systems were quantum-ready and then upgrading or switching them all to a quantum-safe state over a set period of time. This path will also require NIST-approved quantum-safe encryption schemes to complete. Examining the success criteria mentioned above, aside from some basic training, this option has very low impact on end-users who come to work one day and begin using a new system.

By upgrading or replacing systems, there is little to no additional load placed on the existing infrastructure, but this option requires a high degree of administrative planning, testing, quality assurance and possible rollback if something fails. The risk of this option is the time it takes to complete the update or replacement. By waiting until all systems are ready to be upgraded, you greatly increase the window of exposure to threats like harvest and decrypt, subversion of the roots of trust or possibly a quantum computer attack from a nation-state.

A second solution could be to create a duplicate quantum-safe version of existing infrastructure and devise a method to move to this new PKI. (Fig.3) This approach would require NIST-approved quantum-safe encryption schemes to complete. It would also result in negative results for many of the criteria mentioned above. From an impact perspective, there would be a high reliance on end-users to choose correct certificates to use depending on which parts of the infrastructure have been upgraded. The load and costs on the server infrastructure could be doubled with the management of two systems and two certificates. The resulting effect on quality assurance and seamless operations would be considerable.

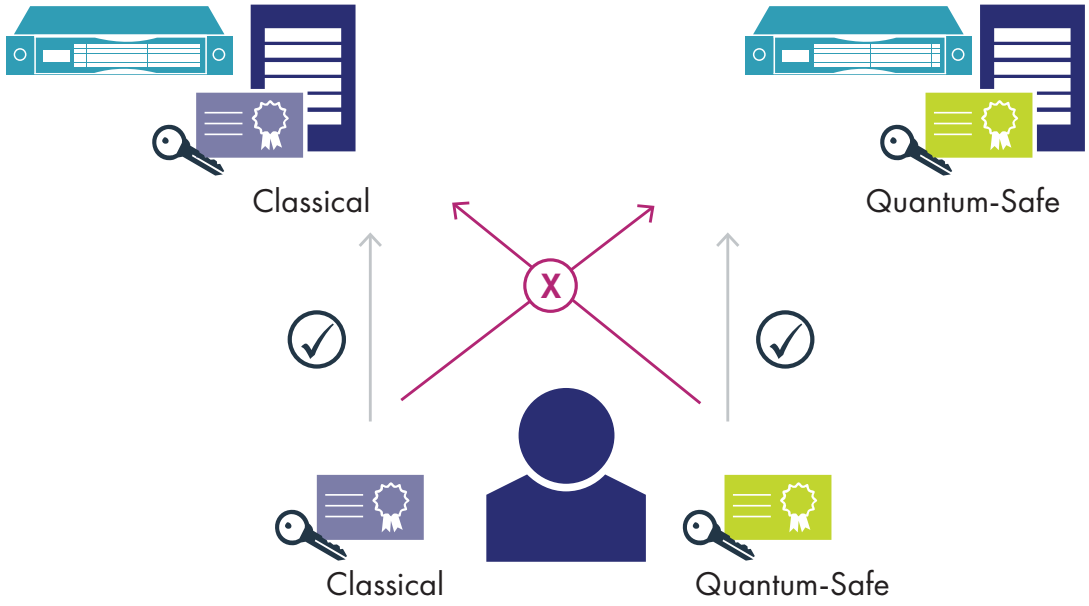

Fig.3 Duplicate Quantum-safe PKI in Addition to Existing Infrastructure

Recommended Solution

We believe the most effective method of migrating PKIs from classical to quantum-safe algorithms is to utilize a crypto-agile approach using ISARA Catalyst™ Agile Digital Certificate Technology. The essence of ISARA Catalyst is the enablement of a single digital identity where both classical and quantum-safe algorithms are able to co-exist (Fig. 4). This approach allows for transition work to begin today, while maintaining your FIPS 140-2 validation.

Taking an industry leading approach, ISARA Catalyst enables the insertion of a quantum-safe public key and issuer signature into the existing certificate while maintaining backwards compatibility with your existing installation. If we consider the current protocol, both classical and quantum-safe algorithms connected to one single identity could reside in a single certificate on a newly issued Common Access Card (CAC) as part of the 3-year renewal program. By utilizing ISARA Catalyst, the underlying infrastructure can be upgraded in phases, allowing for existing and upgraded quantum-safe systems to interoperate seamlessly using only one CAC without any action required by end-users or modifications to the existing systems.

From an impact perspective, the crypto-agility built into this approach makes it entirely seamless to end-users. There are no parallel instances required in the infrastructure making the impact on computing load very low. ISARA Catalyst provides the administrators maximum flexibility since crypto-agile credentials offer full backward compatibility. The ability to upgrade in phases allows the most critical or vulnerable portions of the PKI to be addressed first. In addition, this crypto-agile approach can be deployed utilizing existing systems and infrastructure.

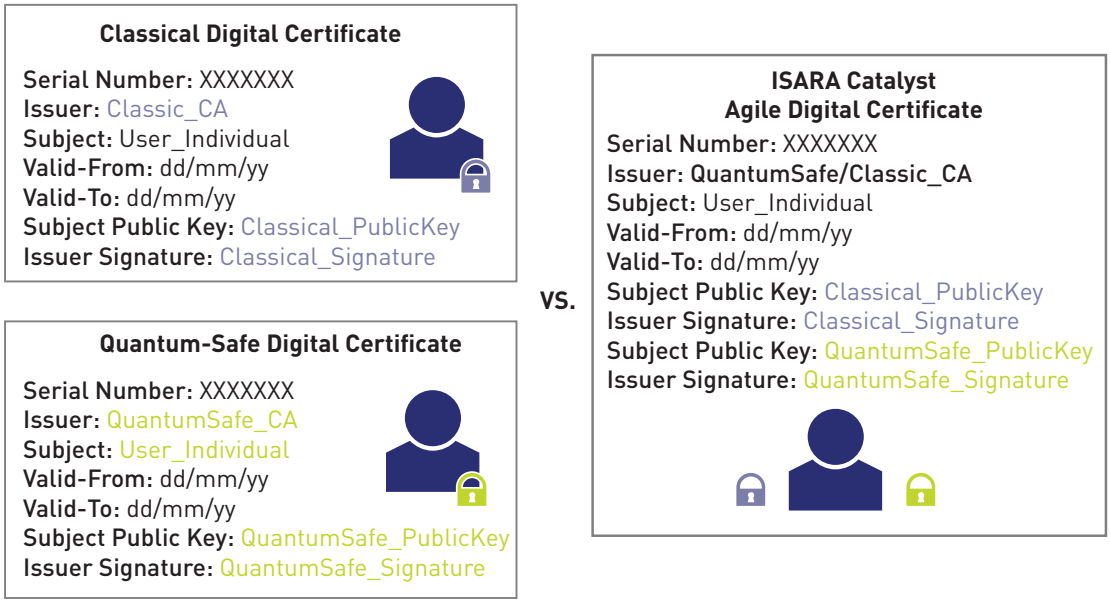

Fig.4 Comparing a Duplication of Certificates with ISARA Catalyst™ Agile Digital Certificate Technology

Challenge #2 - Future-Proofing the Security of Connected Devices

Before public key cryptography can be used for authentication in connected devices, there is an important initial setup that is performed. A trusted root public key is embedded in a system before it leaves the manufacturing facility, with the ID issuance being secured via code signing. Over their lifetime, systems rely on this root public key to authenticate software/firmware over-the-air (SOTA/FOTA) updates to ensure they are coming from a trusted source without modification. When the embedded root public key is compromised, a manual operation is required to inject a new root public key into the system. This operation needs to be performed onsite to guarantee security. This is often logistically challenging (e.g. satellites, deployed military equipment) or financially prohibitive (e.g. millions of low-cost devices) to perform.

Recommended Solution

Stateful Hash-based signatures are ready to be used for code and certificate signing today. There are two candidates (HSS and XMSS) that the Internet Engineering Task Force (IETF) is standardizing and NIST will approve in the near future for limited use.[3] These schemes have a small public key, reasonable signature sizes and are very fast. They are perfectly suitable for devices with limited computational capability. ISARA and Thales have partnered to create a space- and speed-optimized implementation of stateful Hash-based signatures ready for production. Protecting and managing encryption keys in SafeNet Luna Hardware Security Modules (HSMs) ensures those keys are safely stored in a high-assurance, tamper-proof, FIPS 140-2-validated hardware appliance. Furthermore, SafeNet Luna HSMs enable you to update cryptographic algorithms in-field, providing you with the crypto agility to quickly react to cryptographic threats by implementing alternative methods of encryption. Together, Thales and ISARA have the technology to secure code and certificate signing with quantum-safe algorithms today.

Challenge #3 - Future-Proofing the Security of Communications

Today we use separate types of cryptographic algorithms. There are symmetric algorithms, which use the same secret key for encryption and decryption, and asymmetric algorithms (or public-key algorithms), which are used to securely establish a shared secret key even if an adversary is monitoring the communication channel. The security industry, with the support of standards agencies, is confident that this process secures sensitive data and protects it from prying eyes.

Once an adversarial nation-state has access to a large-scale quantum computer, they will have the ability to break current public key cryptography using Shor's quantum algorithm. Shor's algorithm running on a sufficiently-powered quantum computer would allow an adversary to break the key establishment part of the communication protocol, unmask the symmetric encryption key and read the exchanged data in clear text. If this encrypted data is stolen today and stored until a sufficiently-powered quantum computer is available, the secure data will be accessible. If this data has a secrecy obligation beyond the introduction of large-scale quantum computing, then it is at risk today.

3 "FAQs," [Online]. Available: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/faqs.

There are no practical modifications of the current public-key algorithms that would be resistant to an attack by an adversary having access to a large-scale quantum computer. The most practical solution is to change the math. Not taking action today and waiting for NIST to approve next generation encryption standards puts system at high risk.

Recommended Solution

While there are no quantum-safe key agreement or key transport algorithms that have been standardized thus far, our recommended approach is to use a hybrid key establishment solution, with key material protected by a SafeNet Luna HSM. A hybrid solution would combine multiple key establishment mechanisms in a way where this new mechanism has the combined security advantages of each individual component. NIST recently approved this approach stating, "Assuming one of the components of the hybrid mode in question is a NIST-approved cryptographic primitive, such hybrid modes can be approved for use for key establishment or digital signatures."[4] For example, by merging a quantum-safe algorithm like Kyber with a classical algorithm such as Elliptic Curve Diffie-Hellman (ECDH), we can create a new key agreement that is as strong as its strongest component. That is, in the unlikely event that the chosen companion quantum-safe algorithm is shown to be vulnerable to either a classical or a quantum attack during the standardization process, the hybrid scheme will still be as strong as ECDH.

Furthermore, there are multiple areas of quantum-safe cryptography in development that apply radically different areas of math. These algorithms rely on different security assumptions and different mathematically hard problems. As a result, it is highly unlikely that two of the most promising quantum-safe algorithm candidates will be shown to be vulnerable in the future. Thus, merging two quantum-safe key agreement algorithms (based on different underlying mathematical problems), with a classical algorithm like ECDH, would result in a cryptographic algorithm that is undoubtedly secure against both classical and quantum attacks.

For link-level encryption of data centres another possible technique is to leverage Quantum Key Distribution (QKD) between the two endpoints. QKD allows for two nodes to agree on a shared key known only to them. While current QKD technology is limited to point-to-point connections or the use of a trusted node, this can be a powerful tool in protecting against attackers eavesdropping and recording transmissions today. Thales' quantum-powered CN8000 SafeNet High Speed Encryptor (HSE) enables multi-link encryption of Layer 2 Network Ethernet traffic, providing 100 Gbps of total encrypted bandwidth, with no overhead and minimal latency.

Thales' security solution contains multiple options for key agreement and key transport based on different mathematical problems. Using ISARA-implemented algorithms in combination with currently used classical algorithms, we can mitigate the harvest and decrypt threat today in TLS, IKEv2, S/MIME, Signal and other protocols.

Conclusion

The threat to public key cryptography from quantum computers is now a matter of "when", not "if". The industry has a limited amount of time to upgrade and protect systems that are vulnerable today, to authenticate applications that are sustained through SOTA updates and to transition complex infrastructure to ensure authentication and confidentiality of user identification. It's generally accepted that Government data is under threat today, but we have a high level of confidence in the security we use to protect that data. However, protected information that is stolen or copied at some point in the near future becomes clear text in the hands of an adversarial nation-state possessing a large-scale quantum computer. This is a critical vulnerability for information that requires a secrecy obligation beyond 10 years and requires action today. A hybrid approach utilizing both classical and quantum-safe algorithms can solve this challenge.

Securing the roots of trust with future-proof algorithms stored in a SafeNet Luna HSM ensures that vehicles, infrastructure and other connected devices remain secured when they are updated with authenticated software code. The use of HSMs for stateful Hash-based signature schemes is a mature and effective way to ensure long-term security. In the case of PKI migration, there are limited options available to successfully migrate the current cryptography embedded in the infrastructure, to cryptography that is protected from future quantum computer attacks. ISARA Catalyst technology provides the ability to support multiple algorithm certificates under one identification to make a phased and backwards compatible transition possible. Lower costs, manageable logistics and minimal complications all add up to a successful and seamless migration strategy resulting in continuity of operations throughout the process.

ISARA's team of researchers includes multiple PhDs in quantum computing and mathematics. Coupled with professional developers, crypto agility, and the strength of Thales' Cloud Protection & Licensing (CPL) suite of products, together we are able to spearhead the industry in developing quantum-safe tools and solutions and address the threat to encryption posed by large-scale quantum computers.

Contact us to learn how you can get started with protecting yourself in the post-quantum era.

3 & 4 "FAQs," [Online]. Available: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/faqs.

About Thales Cloud Protection & Licensing

Today's enterprises depend on the cloud, data and software in order to make decisive decisions. That's why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive information and software wherever it is created, shared or stored – from the cloud and data centers to devices and across networks. Our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, and create more value from their software in devices and services used by millions of consumers every day.

About ISARA Corporation

ISARA Corporation is a cybersecurity company specializing in creating production-ready quantum-safe solutions for today's computing ecosystems. We provide our partners with agile quantum-safe technologies to enable a seamless, cost-effective and faster migration for their solutions. As a commercial solution provider within a rich academic and research ecosystem, ISARA is part of a collaborative effort to raise awareness of quantum threats, and design and implement quantum-safe solutions that will work globally.

ISARA was founded in 2015 and is headquartered in Waterloo, Ontario, Canada, with an office in Silicon Valley, California. Our team has grown to over 40 employees, many with years of experience in technology and security companies, including BlackBerry, Certicom, Oracle, and McAfee, and academic and research institutions, including the Institute for Quantum Computing (IQC) and the Perimeter Institute. We actively collaborate with academic and standards institutions to conduct joint research and raise awareness of the quantum threat. We are a proud part of 'Quantum Valley' in Waterloo Region, a rich collaborative environment between academic and industry focused on accelerating the development of quantum computing and related technologies.

THALES

Americas
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211 | E-mail: sales@thalesesec.com

Asia Pacific – Thales Transport & Security (HK) Ltd
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 8141 | E-mail: asia.sales@thales-esecurity.com

Europe, Middle East, Africa
Meadow View House, Long Crendon,
Aylesbury, Buckinghamshire HP18 9EQ
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> thalescpl.com <