Enabling Quantum-Safe Migration with **Crypto-Agile Certificates**

ISARA Corporation

Table of Contents

1 Public Key Infrastructure (PKI)

Over the past few decades, many organizations and governments have made substantial investments to deploy public key infrastructure (PKI) systems. These systems provide the essential elements required to secure their networks, devices, communications and even physical facilities access. With the availability of large-scale quantum computers within the next eight to 15 years, these investments need to be protected by migrating to quantum-safe versions of cryptographic primitives.

2 The Quantum Threat to Cybersecurity

There are a number of risk vectors that malicious attackers can exploit. With cryptography being used ubiquitously in our systems, we identified three areas that highlight the need for urgent action today:

- **Harvest & Decrypt**: communications can be harvested today and decrypted later using a large-scale quantum computer
- **Roots of Trust**: public keys based on classic cryptography which are embedded in long-lived devices (such as connected vehicles, critical infrastructure and military equipment) cannot be trusted to authenticate software updates after a large-scale quantum computer arrives
- **Crypto Agility in PKI**: organizations and governments rely on complex PKIs to support information and communication technology (ICT) systems that often require several years to a decade to migrate.

To determine the negative impact to your organization, you'll need to consider the probability of attack for each particular area. In this whitepaper, we focus on attacks on PKIs.

Attacks on PKIs are much more cost effective *for an attacker* than harvest and decrypt. When deploying harvest and decrypt, the attacker must run Shor's algorithm for *each* communication session, where the algorithm may need to be executed a number of times on a stream of sessions to fully obtain what is desired. After all that effort, an attacker receives past information, which depending on its type (i.e. state or military secrets) can be of significant value but not as a matter of course.

Now, when attacking a PKI system, only a single instance of Shor's algorithm is needed. Note that the public key of the root certificate authority (CA) is known to everyone *by design*. Therefore, virtually no effort is required to obtain such a public key. With the public key of the root CA in hand, running Shor's algorithm only once is enough to obtain the root CA's private key. And once root CA's private key is obtained, the attacker can produce just about any digital certificate for *any* entity, existing or new. Since certificate issuance is typically an off-line process, it is extremely difficult to detect the malicious issuance of a false or impersonating certificate. In essence, the attack is nearly undetectable while the root CA's public key is trusted.

This is an incredibly powerful attack that can be perpetrated by adversaries with access to a large-scale quantum computer. This means that if the PKI is used for access control, the attacker can obtain access to any classified information. And if the PKI is used for financial transactions, the attacker can steal any amount of money since fraudulent transactions will appear to execute legitimately.

3 Migrating to a Quantum-Safe PKI

The solution then must be to migrate to a quantum-safe version of a PKI as soon as possible. What options exist? There are fundamentally two approaches, stateful and stateless digital signature schemes. A review of the approaches and their readiness for deployment follow.

3.1 Choosing Quantum-Safe Digital Signatures

Stateful hash-based signature schemes are well-studied and the most trusted quantum-safe options currently available to use in low frequency signing operations. For example, code signing and certificate signing both represent ideal use cases. Organizations should begin migrating immediately to quantum-safe CA certificate, starting with root certificates, as the process of migrating is exceedingly time consuming and logistically difficult.

The two accepted stateful hash-based signature schemes are Leighton-Micali Signatures (LMS) and eXtended Merkle Signature Scheme (XMSS). These schemes have unique properties. From a performance perspective, they are several times faster than elliptic curves on the same hardware specs, however they have a very large private key with a state that needs to be managed after every signing operation.

Their specifications are in process of being finalized by the Internet Engineering Task Force (IETF). The National Institute of Standards and Technology (NIST) is expected to standardize their use shortly once their specification is complete – long before their Post-Quantum Cryptography Standardization process is completed (it was initiated in November of 2017).

For entity authentication in protocols such as TLS and IKE, a stateless signature scheme is better suited, as there is no state to manage and an unlimited number of signatures can be created. There are a number of leading candidates emerging including Dilithium, Rainbow and SPHINCS. However, the final specifications and definitions for these schemes is still a work in progress as part of NIST's Post-Quantum Cryptography Standardization process. It is expected that a number of changes will be applied to these algorithms (and others may be added) during the standardization period.

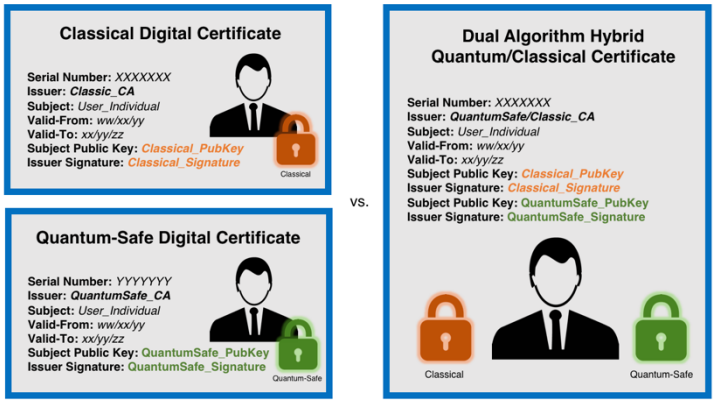
3.2 Challenges when Migrating to Quantum-Safe PKI

Aside from the algorithm selection and standardization outlined above, there are significant additional concerns which organizations must take into account to plan a transition to a quantum-safe PKI.

1. Duplicating the existing classical PKI with a parallel quantum-safe version is required in order to migrate organizations' ICT systems and users. This is an incredibly expensive, resource intensive, and cumbersome (to users and administrators) proposition.
2. With both a classical PKI and a quantum-safe PKI in place, transitioning users, systems and services in stages is logistically extremely challenging as legacy and upgraded systems must continue to interoperate.
    a. Will systems need to be modified/replaced/duplicated to support backwards compatibility?
    b. Will applications require updates/changes to support backwards compatibility?
3. Maintaining service levels for users, services and systems while minimizing downtime will be critical for this transition to be a success.
    a. Can end users tolerate and correctly use multiple sets of certificates?

Taken as a whole, these concerns must be addressed, and their impact minimized for an orderly and efficient migration to quantum-safe cryptography to be possible. In other words, a solution that provides cryptographic agility, or crypto-agility, is required.

4 ISARA's Crypto-Agile Solution



ISARA has pioneered a new method of creating a compound or hybrid digital certificate that contains both classical public key and signature, and quantum-safe counterparts together. A good analogy for this technology would be a dual jurisdiction passport, that contains the identity of a single individual certified as authentic by two countries. The key to such a construct is ensuring that this crypto-agile digital certificate would in fact be accepted as legitimate when obtaining authorization to enter either country, with no extra effort or training required by either the passport holder or the border control officers.

In a nutshell, this is exactly what crypto-agile digital certificates provide.

4.1 Detailed Technical Description

The current universally adopted design for X.509 digital certificates used in PKI's are standardized to employ a single cryptographic algorithm, making duplication of a PKI system the *only* means by which multiple algorithms can be supported. ISARA's crypto-agile certificate technology creates the ability to support two cryptographic algorithms within a single X.509 certificate in such a way that it is fully compatible with systems that are unaware of the second cryptographic algorithm. This allows for the existing PKI to be upgraded with the ability to issue new crypto-agile certificates without the duplication of resources.

A crypto-agile certificate allows for backward compatibility between systems that only recognize classical algorithms and those that are upgraded to recognize quantum-safe algorithms. In this case an updated system can communicate with a legacy one using crypto-agile certificates, as the legacy system will only process the classical cryptographic primitives and ignore the quantum-safe equivalents without any modification. This makes migration of these dependent systems in phases not only possible but practical as the complexity of staged migrations is *greatly reduced* since backwards compatibility is maintained.

Users will not need to manage multiple sets of certificates during the migration process, to them their crypto-agile certificate is all they need to access the systems and services they require. The support burden on the IT team is greatly reduced as a result.

4.2 Defined in Key Global Standards

ISARA's crypto-agile certificate contribution to the International Telecommunications Union (ITU) X.509 specification has been approved and will part of the updated standard release later this year. Together with collaborators from Cisco Systems and Entrust Datacard ISARA submitted an Internet Draft to IETF outlining the new X.509 certificate format.

4.3 Ready to use Today

To summarize, crypto-agility is the key to effective management of the migration of Information and Communication Technology (ICT) systems from legacy to quantum-safe systems. The tools to do this cost-effectively and efficiently are now available with ISARA's crypto-agile certificate technology. The time to start your quantum-safe migration is now.

5 About ISARA Corporation

ISARA Corporation is a cybersecurity company specializing in creating production-ready quantum-safe solutions for today's computing ecosystems. We enable OEMs to achieve a seamless migration to next-generation security measures by embedding our optimized quantum-safe algorithms and unique crypto-agile technology.

Experts estimate that within the next eight to fifteen years, currently used public key cryptography is expected to be broken by a large-scale quantum computer *forcing a complete migration to quantum-safe cryptography (QSC)*. Migrating to QSC is a long-term project, therefore NIST advises starting early.

The ISARA Radiate™ Security Solution Suite is the only complete solution on the market to offer a production-ready implementation suite of quantum-safe algorithms and integration tools built for developers. By embedding the ISARA Radiate cryptographic library, OEMs can create quantum-safe commercial products and systems today while maintaining performance and interoperability. Our unique crypto-agile technologies enable OEMs to seamlessly integrate our quantum-safe algorithms into their existing systems while maintaining backward compatibility. Learn more about ISARA Radiate at www.isara.com/isara-radiate/.