ISARA Catalyst™ Agile Digital Certificate Methodology

Simplify Cryptographic Migrations

Avoid the headache of transitioning cryptography within large corporate networks that rely on X.509 certificates

Regardless of the reason for moving from one type of cryptography to another, doing so is a logistically complicated and costly process—especially when you have many different clients needing to connect with a large number of different servers.

Problems with parallel PKI infrastructures

While you may have several options to migrate your systems, you're likely struggling to find one that's cost effective and that maintains interoperability.

For example, some organizations create a parallel public key infrastructure (PKI) that uses the new cryptographic algorithm and use a forklift-upgrade approach to move from the existing PKI to the new one. This duplication requires a significant amount of resources and time, and delays the migration to stronger security measures—creating unnecessary risk.

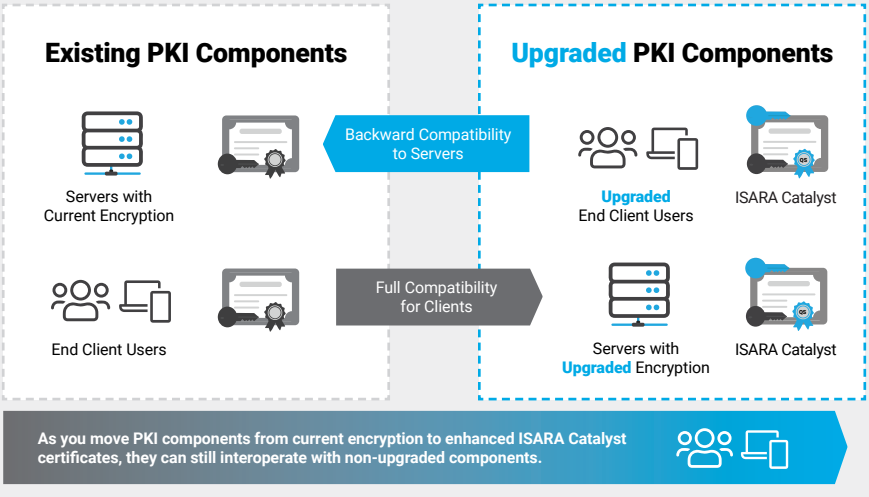
A superior—and smoother—path forward

In contrast, ISARA Catalyst solves this challenge by introducing agility and flexibility into X.509 certificates—enabling two different types of cryptographic algorithms to be used at once without causing compatibility issues with non-upgraded systems.

Benefits of ISARA Catalyst

By utilizing ISARA Catalyst enhanced certificates, transitioning cryptography changes from a logistical challenge to a manageable upgrade, both now and in the future.

- **Gradual migration:** upgrade your most critical, at-risk assets in phases due to backward compatibility with current X.509 certificates, ensuring interoperability
- **Eliminate duplication and management of multiple PKIs:** reduce time, costs and complications associated with transitioning cryptography
- **Protect using the cryptographic algorithms you need to use, faster:** whether you need a faster path to compliance or simply want to transition to stronger or more efficient security
- **Transparent to end users:** those endpoints using the enhanced certificates can still interact with existing systems and vice versa



At-a-Glance

ISARA Catalyst Agile Digital Certificate Methodology gives you the ability to seamlessly migrate complex PKIs and reliant systems in phases by enabling backward compatibility with non-upgraded components.

It's integrated by developers who create and manage identity and access management systems serving enterprise and government.

Methodology Overview: Seamlessly Migrate Complex PKIs and Reliant Systems

ISARA Catalyst creates an enhanced X.509 digital certificate that simultaneously contains two sets of cryptographic subject public keys and issuer signatures while maintaining full backward compatibility with current X.509 formats.

ISARA Catalyst Methodology is:

- **Undergoing integration** into certificate offerings from DigiCert, Sectigo and FutureX
- **Standardized** in Recommendation ITU-T X.509 | ISO/IEC 9594-8 international standard

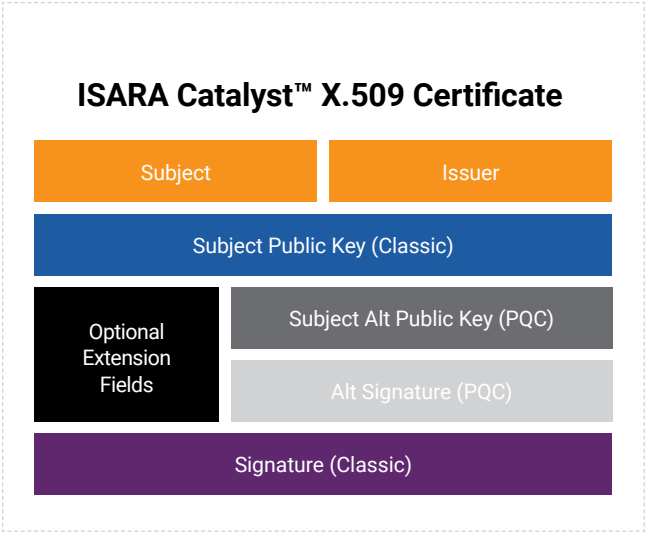
Technical details for developers

Within the certificate layer of the developer's stack, an optional extension is added to X.509 certificates that allows for an alternative subject public key and issuer signature to be added. This alternative public key and signature can be any type of algorithm, whether that be quantum-safe algorithms or currently used ones, such as RSA or ECC.

During certificate issuance, the certificate attributes are signed twice. First, by the new algorithm introduced in the optional extension, and then by the primary algorithm currently in use.

Backward compatibility is possible due to the fact that the subject alternative public key and alternative signature sit within an optional extension, which existing and non-upgraded systems can look past without causing a break in the certificate chain.

ISARA Catalyst Methodology can be used for any cryptographic migration, however it is particularly well-suited to enable the transition from classic cryptography to quantum-safe cryptography (QSC)



Take the next step.

Learn more about **ISARA Catalyst Agile Digital Certificate Methodology** by booking a meeting with our team. Connect with us at **catalyst@isara.com**.

isara.com | +1 877 319 8576
560 Westmount Road North, Waterloo, Ontario, Canada N2L 0A9

© ISARA Corporation. All Rights Reserved.
Version 1.0 | 2021-01-13