ISARA Catalyst™
Agile Digital Certificate Technology

Datasheet

ISARA Catalyst™ Agile Digital Certificate Technology
At-a-Glance

The ISARA Catalyst Agile Digital Certificate Technology is a technique for creating 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. It's integrated by developers who create and manage identity and access management systems serving enterprise and government.

Benefits & Advantages

- Gradual migration – Upgrade your most critical, at-risk assets in phases due to backward compatibility with current X.509 certificates which insures interoperability
- Eliminate duplication and management of multiple public key infrastructure (PKI) – 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

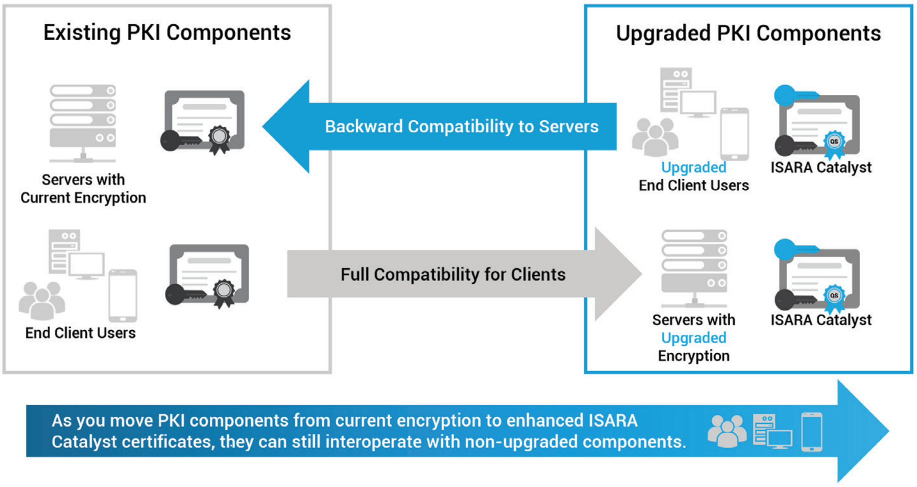
Simplify Cryptographic Migrations with ISARA Catalyst

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, it's a logistically complicated and costly process to do so when you have many different endpoints needing to connect with a large number of different servers. While you may currently have several options to migrate your systems, you're likely struggling to find one that's cost-effective and maintains interoperability. For example, some organizations choose to create a parallel public key infrastructure (PKI) that uses the new cryptographic algorithm and use a forklift-upgrade approach from the existing PKI over to the new one. This requires a significant amount of resources and time due to duplication and delays the migration to stronger security measures for your most at-risk assets.

In contrast, ISARA Catalyst solves this challenge by introducing agility and flexibility into X.509 certificates by enabling two different types of cryptographic algorithms to be used at once without causing compatibility issues with non-upgraded systems. No longer do you need to wait to transition entire certificate chains, you can begin starting with mission-critical servers and devices first based on the risk and business impact they pose. By utilizing ISARA Catalyst enhanced certificates, transitioning cryptography changes from a logistical challenge to a manageable upgrade, both now and in the future.

.


Existing PKI Components
Servers with Current Encryption
End Client Users
Backward Compatibility to Servers
Full Compatibility for Clients
Upgraded PKI Components
Upgraded End Client Users
ISARA Catalyst
Servers with Upgraded Encryption
ISARA Catalyst

As you move PKI components from current encryption to enhanced ISARA Catalyst certificates, they can still interoperate with non-upgraded components.

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

Features

- **Undergoing integration** into DigiCert's certificate offering
- **Where more robust security is needed,** ISARA Catalyst works in conjunction with hardware security modules (HSMs), such as the Thales Luna 7 SafeNet HSM and Utimaco CryptoServer HSM
- **Accepted for standardization** under the Recommendation ITU-T X.509 | ISO/IEC 9594-8 international standard (currently waiting for the next publication cycle)

ISARA Catalyst technology can be used for any cryptographic migration, however its recommended use is for classic to **quantum-safe transitions** due to the urgency of the quantum threat.

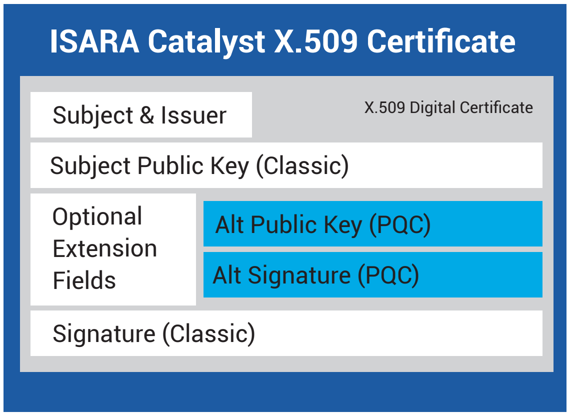
Technical details for developers

Within the certificate layer of the developer's stack, an optional extension is added to X.509 certificates that allows for a second cryptographic key and signature to be added. This secondary 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 cryptographic key in the optional extension is signed twice. First, by the new algorithm introduced in the optional extension, and once by the primary algorithm currently in use.

Backward compatibility is possible due to the fact that the alternative subject 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 X.509 Certificate

X.509 Digital Certificate

Subject & Issuer

Subject Public Key (Classic)

Optional Extension Fields

Alt Public Key (PQC)

Alt Signature (PQC)

Signature (Classic)

Diagram of an X.509 certificate with optional extensions added for "Alt Public Key" and "Alt Signature."

Take the next step.

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

ISARA Corporation, the world's leading provider of agile quantum-safe security solutions, leverages decades of real-world cybersecurity expertise to protect today's computing ecosystems in the quantum age. With our partners, we're clearing the path to quantum-safe security for enterprises and governments by delivering practical, standardized solutions for a seamless migration. Visit www.isara.com.

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

Version 1.0 | 08.06.2019