SOLUTION BRIEF

Using hybrid certificates with quantum-safe security to enable simplified cryptographic migrations

Together We Can Help

The DigiCert hybrid certificate solutions and ISARA quantum-safe security solutions work together to simplify complex PKI and reliant systems migrations by enabling you to achieve the following:

Solution benefits:

- Get ahead of the quantum threat by future proofing your organization today in a way that will not disrupt your current operations, reduce switching costs and ensure you can switch seamlessly to new algorithms in the future.
- With hybrid certificates from DigiCert, that use the ISARA Catalyst™ Agile Digital Certificate Technology, you can continue relying on a single certificate that is capable of authenticating to current, non-upgraded systems as well as upgraded quantum-safe systems without any user involvement or disruption.

The problem and challenge: quantum computing will break modern cryptography, the foundational security measure used in digital certificates

Large-scale quantum computing will break current public key cryptography algorithms, such as RSA and ECC, causing widespread vulnerabilities within everything that connects. These algorithms are used in digital signatures to establish trust and security over insecure networks and are fundamental to public key infrastructure (PKI). However, switching out algorithms within PKI and reliant systems is complicated and time consuming. The interdependent nature of the systems that rely PKI for authentication makes transitioning to new algorithms challenging with high IT management costs. Duplication of the PKI may be required. This is due to current digital certificates only using one public key algorithm, causing interoperability issues should specific components be updated to new algorithms before others. Also, the PKI must be fully transitioned to quantum-safe security before the rest of the dependant systems can be secured. Today it can take a large organization several years to over a decade to completely transition to a new algorithm. Time that security-conscious organizations don't have before a large-scale quantum computer exists.

> *" By 2021, organizations with crypto-agility plans in place will* ***suffer 60% fewer cryptographically*** *related security breaches and application failures than organizations without a plan. "*
>
> - Gartner, Better Safe Than Sorry: Preparing for Crypto-Agility, Refreshed August 2019, Published March 2017

The solution: Create an agile and future-proof PKI using hybrid certificates with quantum-safe cryptography

DigiCert and ISARA are industry-leading innovators uniquely positioned to quantum-proof your organization's PKI in a completely backward compatible and crypto-agile way. The combined solution of hybrid certificates and quantum-safe cryptography enables organizations to protect their mission-critical assets today as part of a phased or gradual migration approach due to backward compatibility with current X.509 certificates.

Solution Benefits:

- Simplify PKI and reliant systems migrations by integrating crypto-agility and flexibility into your existing systems.
- Protect mission-critical assets today without impacting interoperability with non-upgraded components and systems.
- Deploy quantum-safe roots of trust (trust anchors) today ahead of the quantum threat.
- Achieve continued compliance with X.509 standards (hybrid certificate approach is accepted for standardization under the Recommendation ITU-T X.509 | ISO/IEC 9594-8 international standard (currently waiting for the next publication cycle)
- Reduce PKI and reliant systems migrations costs, no system or credential duplication is required when using hybrid certificates.
- Start issuing entity certificates as reliant systems get upgraded.

About ISARA Corporation

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.

About DigiCert

DigiCert is the world's premier provider of high-assurance digital certificates—providing trusted SSL, private and managed PKI deployments, and device certificates for the emerging IoT market. Since our founding almost fifteen years ago, we've been driven by the idea of finding a better way. A better way to provide authentication on the internet. A better way to tailor solutions to our customer's needs. Now, we've added Symantec's experience and talent to our legacy of innovation to find a better way to lead the industry forward, and build greater trust in identity and digital interactions.

ISARA Agile Quantum-safe Security Solutions

ISARA Corporation is the world's leading provider of agile quantum-safe security solutions. ISARA's tools and technologies, such as the ISARA Radiate™ Quantum-safe Toolkit for developers and the ISARA Catalyst™ Agile Digital Certificate Technology, integrate and augment DigiCert's certificate solutions to enable hybrid certificates and enhanced security using quantum-safe algorithms today. ISARA's solutions and technologies are built using a standards-based approach for interoperability – the quantum-safe cryptographic library aligns to the NIST Post-Quantum Cryptography Project and the ISARA-developed hybrid certificate approach is accepted for standardization under the Recommendation ITU-T X.509 | ISO/IEC 9594-8 international standard.

DigiCert Certificates

DigiCert is the world's premier provider of high-assurance digital certificates—providing trusted SSL, private and managed PKI deployments and device certificates for the emerging IoT market. DigiCert's TLS solutions provide the world's largest organizations with the security they need to protect their business, brand, and customers through our innovative enterprise PKI management platform. DigiCert's solutions are backed by the most extensive collection of global experts with offices and data centers around the world who are focused on bringing the most advanced PKI solutions to our customers. DigiCert is proud to partner with ISARA to bring their Radiate solution to a global audience to through their Quantum-safe Toolkit to help start preparing the world today for the quantum tomorrow.

Start protecting with agile quantum-safe security today.

From proof of concept to deployment.

Contact us at **quantumsafe@isara.com** to get started.