ISARA manages the complexity of cryptographic transitions and creates a clear path to quantum-safe security

Quantum computers will deliver tremendous benefits, but they will also be able to break the cryptography underlying public key infrastructure (PKI).

This capability makes quantum computers an enormous threat to enterprises and connected device manufacturers—who increasingly use PKI for authentication and encryption—and has CISOs and CIOs looking for solutions.

Act today to protect your tomorrow

The National Institute of Standards and Technology (NIST) is still in the process of standardizing quantum-safe cryptographic algorithms, but that doesn't mean you have to wait to start managing the quantum risk.

There are already solutions available to bridge the gap between classical and quantum-safe encryption—and there are real reasons to take action today:

- The shift to quantum-safe algorithms will be the largest and most complex cryptographic migration in history—getting started now offers significant advantages
- Systems, products and platforms being designed today that will still be in use a decade or more from now need to be quantum-safe
- Motivated threat actors are already harvesting valuable secrets protected by today's classical cryptography—to decrypt with quantum computers in the future

Manage crypto-risk. Become quantum-ready

We provide crypto-agile technologies and quantum-safe cryptography to enable a seamless, practical and cost-effective transition to quantum-safe cryptographic standards.

We can help you with:

- **Integrating crypto-agility** into large and complex PKIs
- **Protecting against attacks** targeting classically encrypted sensitive data
- **Future-proof code-signing** for long-lived IoT devices
- **Gaining hands-on experience** with quantum-safe cryptography and solutions

Why **ISARA**

ISARA is the world's leading provider of crypto-agile and quantum-safe security solutions.

We have particular expertise in building practical cryptographic systems for the constraints of real-world operational environments.

Our high-performance, standards-based quantum-safe cryptography and integration tools are ready to help you test and deploy robust solutions for the quantum world.

When trust matters, leading organizations trust **ISARA**

BlackBerry digicert FUTUREX
THALES utimaco VENAFI

About **ISARA**

Since our founding in 2015, we have played a leading role in developing and commercializing real solutions to manage quantum risk.

Our **Home**

We're headquartered in Waterloo, Ontario—just steps from the renowned University of Waterloo and its world-famous Institute for Quantum Computing (IQC).

Our **Team**

Our team is composed of some of the most inquisitive and ingenious minds in the cryptography and cybersecurity industry, with years of experience at companies including BlackBerry, Certicom, Oracle and McAfee.

We're fortunate to be led by accomplished security leaders, several of whom are responsible for establishing the BlackBerry platform as the most secure in the world.

Our **Approach**

We educate and validate within industry and government through meaningful quantum-safe proof of concept projects.

We partner with security providers to deliver quantum-safe and crypto-agile solutions.

Our **Contributions**

We're leading global standards efforts—with ETSI, ITU-T, IETF, X9, and more—to help ensure interoperable, lasting security solutions.

In fact, we were a lead contributor in developing an important international quantum-safe standard with ITU-T—introducing multiple public-key algorithm certificates within X.509.

Unique **Solutions**

We offer a range of products and programs to help organizations become quantum-ready.

ISARA Radiate™ Quantum-Safe Toolkit

A high-performance, lightweight, standards-based quantum-safe software development kit which allows you to test quantum-safe cryptography and integrate it into your commercial products

ISARA Catalyst™ Agile Digital Certificate

A standards-compliant X.509 digital certificate extension which can be introduced into existing systems to enable a seamless migration to quantum-safe security

ISARA Quantum Readiness Program for Enterprise

A comprehensive program to equip your information and cryptography teams with actionable know-how and practical experience through education sessions, workshops and hands-on training

Ready to get started?

Contact us at **quantumsafe@isara.com** to learn more about crypto-agility and quantum-safe security.

ISARA

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

Version 1.0 | 2020-05-05