ISARA RADIATE
SECURITY SOLUTION SUITE

Version 1.3

WHAT IS THE QUANTUM THREAT?

Within the decade, experts estimate that the first large-scale commercial quantum computer will be available. With it, the next technological revolution will begin. Its immense computing power will allow for amazing advancements in areas such as artificial intelligence and material design.

It'll also break public key encryption standards that are the foundation of trust for all the technology we rely on. If you've used the Internet, you've used encryption that will be broken by a quantum computer in the near future.

"All the public key cryptosystems... must be replaced with quantum safe counterparts."

- National Institute of Standards and Technology (NIST)

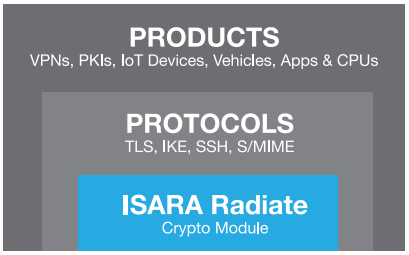
HOW DOES QUANTUM COMPUTING AFFECT YOUR SECURITY?

	CONFIDENTIALITY	ROOTS OF TRUST	IDENTITY MANAGEMENT
PROBLEM	Encryption depends on key establishment to securely share information, which large-scale quantum computers will break. Any information whose confidentiality must persist over time is at risk now to harvest and decrypt attacks.	Hardware and software systems rely on embedded roots of trust to validate that updates are authentic. Malicious updates can wreak havoc by taking control of critical systems like our vehicles, medical devices, and infrastructure.	The threat to PKI-based identity systems will not be realized until a large-scale quantum computer is available. However, the time it takes for a medium to large enterprise to upgrade its PKI and all dependent systems can take several years to a decade.
SOLUTION	ISARA Radiate combines existing mechanisms with multiple leading quantum safe candidates while maintaining current FIPS certification. ISARA's solution protects your data today and in the future ahead of official standards.	In-field updates of IoT devices can range from financially prohibitive to logistically impossible. ISARA Radiate ensures the roots of trust you embed today will be able to protect your software update process.	ISARA pioneered a new crypto-agile PKI identity scheme allowing migration to begin today and completed in a fraction of the time. This seamless modification to encryption protocols provides full forward and backward compatibility making the switch to a quantum safe state easy & cost effective.

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

ISARA RADIATE SECURITY SOLUTION SUITE

The **ISARA Radiate Security Solution Suite** is the first complete solution on the market to offer a high-quality implementation of academic & industry recognized quantum safe algorithms and integration tools built for developers. Our customers gain the ability to integrate critical, quantum safe security measures into their commercial products and networks today.



ISARA optimizes quantum safe algorithms for governments and enterprises, preserving user experience and performance while providing the highest levels of security.

Embrace the quantum revolution, leave behind your security risks.

ABOUT US

ISARA's mission is to build a quantum safe world where all the possibilities and benefits of quantum computing can be realized, with none of the risks.

We specialize in creating class-defining quantum safe cryptography solutions that can be embedded into commercial products today to secure data now and in the future.

Quick Facts:

- Founded in 2015 by global tech experts
- 30+ team members, a third of which are PhD researchers
- Strong IP portfolio
- Global standards leader partnering with ETSI, ITU, IETF
- Solutions covering both hardware and software domains for OEMs

LET'S GET STARTED

Starting your quantum safe transformation is simple.

Visit **www.ISARA.com** or email us at **quantumsafe@ISARA.com** and we'll work with you to create a custom plan.

WHY CHOOSE ISARA?

CLASS-DEFINING CRYPTO

- Rigorous development process resulting in high quality, fully-traceable code that is certification ready
- World-class team of developers, researchers, cryptographers and executive leadership
- Leading global standards development via partnership or chairmanship with key standards setting organizations
- Classic portion of the ISARA Radiate crypto module is undergoing FIPS 140-2 validation

COMPREHENSIVE SUITE

- The ISARA Radiate crypto module provides full coverage across all five areas of academic & industry recognized math suitable for quantum safe algorithm development (hashes, lattices, codes, mutlivariates & isogenies)
- Authentication, key transport and key agreement options are offered to suit all use cases

SEAMLESS MIGRATION

- Well-designed API and optimized implementation for easy integration into existing systems
- Full-range of professional services to achieve quantum readiness
- Crypto-agile through hybrid key establishment and multiple crypto system certificates

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

Follow us: @ISARAcorp @ISARAcorp @ISARA Corporation

Version 2.0 | 29.08.2017