

ISARA Radiate™ Quantum-safe Toolkit

Datasheet — v3.1

Overview

The ISARA Radiate™ Quantum-safe Toolkit is a **high-performance, lightweight, standards-based quantum-safe software development kit**, built for developers who want to test and integrate next-generation post-quantum cryptography into their commercial products.

Developers choose ISARA Radiate because of the professional tools and documentation, timely product releases and updates, and thorough testing. All backed by our team of embedded security experts available to assist you with your questions and custom integration needs. License our optimized, proprietary implementation of NIST PQC candidate algorithms with confidence knowing it is free from copyleft licensed code, reducing your risk of accidentally exposing your intellectual property to the public domain.

Key Benefits

Standards-based

- Confidently begin testing and integrating using the algorithms selected for standardization by NIST through the Post-Quantum Cryptography (PQC) Standardization process

Accelerate time to market

- Give your development team the freedom to focus on product innovation and leave the implementation of quantum-safe cryptography to us
- Test how quantum-safe cryptography fits into your products today and be ready to deploy commercially faster than your competitors once the final algorithm standards are available

Developer-friendly

- Intuitive APIs allow you to quickly leverage the quantum-safe library, written in highly portable C99 for various platforms and architectures
- Exhaustively tested, thoroughly documented, with sample code provided

HSS & XMSS: Production-ready for roots of trust and code-signing

- Stateful hash-based signatures, Hierarchical Signature Scheme (HSS) and eXtended Merkle Signature Scheme (XMSS), are well trusted to be used today for specific use cases
- Approved for government use by NIST SP 800-208, and specified in IRTF RFC 8391 and IRTF RFC 8554
- Small public keys and comparable performance to ECC-based signature schemes
- Includes ISARA's proprietary approach to state management of the large, stateful private key

Services & Support

Professional services
Our experienced team of embedded security experts can help you integrate quantum-safe security into your products as a professional services project.

Developer support
We offer a variety of different support packages to suit your specific needs.

Product updates
We regularly update the toolkit to align with the NIST PQC Standardization Process and to provide improvements and optimizations. Receive the latest version backed by developer support with a commercial license agreement.

© 2024 ISARA Corporation. All Rights Reserved.

SPECIFICATIONS

ISARA Radiate Quantum-safe Toolkit

Key Features

- Enables you to integrate high-performance, standards-based quantum-safe cryptographic algorithms into commercial products
- Free from copyleft licensed code found in open source libraries, reducing your risk of accidentally exposing your intellectual property to the public domain
- API designed to easily plug in your SHA2, SHA3 or RNG implementations for better performance or hardware support considerations
- Developed by our team of embedded security experts with extensive experience implementing cryptography for real-world applications
- Professional documentation, sample code, and developer support available

Languages

- ISARA Radiate is written in highly portable C99 for various platforms and architectures

Supported Algorithms

Hash algorithms
SHA2 (Secure Hash Algorithm 2; 256 bit, 384 bit and 512 bit)
SHA3 (Secure Hash Algorithm 3; 256 bit and 512 bit)

Message authentication codes
HMAC (Hash-based Message Authentication Code)
Poly1305

Random number generators
HMAC-DRBG (HMAC Deterministic Random Bit Generator)

Key derivation functions
HKDF (HMAC-based Extract-and-Expand Key Derivation Function)
NIST SP 800-56A Alternative 1 Concatenation
PBKDF2 (Password-Based Key Derivation Function 2)

Digital signature schemes
CRYSTALS-Dilithium
HSS (Hierarchical Signature Scheme)
SPHINCS+
XMSS (eXtended Merkle Signature Scheme)

Key encapsulation mechanisms
Classic McEliece
CRYSTALS-Kyber

Symmetric encryption
ChaCha20

System Requirements

Recommended
Linux (Ubuntu 20.04 LTS or newer, Debian 11 or newer; 64-bit platforms)
macOS 11 or newer (64-bit Intel)
Windows 10 or newer (64-bit platforms)

Minimum
Linux (Ubuntu 18.04 LTS or newer, Debian 9 or newer; 64-bit platforms)
macOS 10.14 or newer (64-bit Intel)
Windows 10 or newer (64-bit platforms)

Supported CPUs by OS
Linux: x86_64, skylake
macOS: x86_64, skylake
Windows: x86_64, skylake

Additional architecture-specific builds can be created upon request; please contact us at quantumsafe@isara.com for more information.

ISARA

Take the next step.

Contact us **quantumsafe@isara.com** to level up your cryptography.

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

© 2024 ISARA Corporation. All Rights Reserved.
Version 3.1 | 04.2024