ISARA Radiate™ Quantum-safe Toolkit

Datasheet

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 our curated list of only the most promising algorithms from the NIST Post-Quantum Cryptography (PQC) Standardization process and the Internet Engineering Task Force (IETF)

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 NIST draft 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
- Undergoing NIST standardization (SP 800-208, expected to be completed soon.) IETF has completed specifications under IRTF RFC 8391 and IRTF RFC 8554
- Small public key and comparable performance to ECC-based signature schemes
- Includes ISARA's proprietary approach to state management of the large, stateful private key

Integration tools

- Support for Java using the ISARA Radiate JNI Wrapper to facilitate a seamless integration into solutions written in Java, saving you time and resources

Services & Support

Professional services

Our experienced team of embedded security experts can help you implement 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.

SPECIFICATIONS

ISARA Radiate Quantum-safe Toolkit

Key Features

- Lets you implement 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
- Java API available using the ISARA Radiate JNI Wrapper

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
- RFC-5869
- NIST SP 800-56A Alternative 1 Concatenation
- PBKDF2 (Password-Based Key Derivation Function 2)

Digital signature schemes
- Dilithium
- HSS (Hierarchical Signature Scheme)
- Rainbow
- SPHINCS+
- XMSS (eXtended Merkle Signature Scheme)
- XMSSMT (multi-tree XMSS)

Key agreement schemes
- FrodoDH
- NewHopeDH
- SIDH (Supersingular Isogeny Diffie-Hellman)

Key encapsulation mechanisms
- Classic McEliece
- FrodoKEM
- Kyber
- NTRUPrime
- SIKE (Supersingular Isogeny Key Exchange)

Symmetric cipher
- ChaCha20 symmetric

System Requirements

Recommended
- Android 7.0 (Nougat) or newer (API level 24 or higher)
- FreeBSD 11 or newer (64 bit platforms)
- iOS 10 or newer
- Linux (Ubuntu 18.04 LTS or newer, CentOS 7 or newer; 64 bit platforms)
- macOS 10.14 or newer
- Windows 10 (64 bit platforms)

Minimum
- Android 6.0 (Marshmallow) or newer (API level 23 or higher)
- FreeBSD 11 (64 bit platforms)
- iOS 8.1 or newer
- Linux (Ubuntu 14.04 LTS or newer, Debian 8 or newer; 64 bit platforms)
- macOS 10.10 or newer
- Windows 10 or newer (64 bit platforms)

Supported CPUs by OS
- Android: x86, x86_64, armeabi-v7a, arm64-v8a
- iOS: x86, x86_64, armv7, armv7s, arm64
- Linux: x86_64, core2, sandybridge, skylake, powerpc (32-bit), armv7 (Raspbian 9.4 on Raspberry Pi3)
- macOS: x86_64, core2, sandybridge, skylake
- Windows: x86_64, core2, sandybridge, skylake

Additional architecture-specific builds can also be created on demand; please contact us at quantumsafe@isara.com.

ISARA

Take the next step.

Contact us **quantumsafe@isara.com** to receive a trial toolkit today.

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

Version 2.1 | 03.25.2020