

# Thales and ISARA Corporation

## Using Thales Luna HSMs with quantum-safe security to protect IoT



### The problem

**Quantum computing will break modern cryptography, compromising secure and authenticated software/firmware updates allowing attackers to forge updates**

The onset of large-scale quantum computing will break current public-key cryptography, resulting in widespread vulnerabilities within everything that connects and transacts. This results in a unique problem for long-lived connected devices deployed today which need to remain secure for several years into the quantum age. This is due to the fact that physically embedded roots of trust are used to authenticate software and firmware updates. Without a quantum-safe trust anchor embedded today, they'll need to be recalled and updated resulting in significant financial and logistical burdens. Protecting software updates is just one of the problems to overcome.

### Key benefits

- Deploy high value connected devices (IoT) today with confidence they'll be protected from the quantum threat without requiring costly recalls and physical updates in the future
- Benefit from FIPS 140-2-certified, tamper-resistant hardware security modules (HSMs) to securely create and manage quantum-resistant keys
- Generate digital signatures seamlessly using standardized quantum-safe public key cryptography, specifically stateful hash-based signatures

Simplify the use of stateful hash-based signatures using a unique approach to state management of keys, an industry-wide challenge solved using Thales Luna HSMs



## The challenge

### Protecting connected devices now and in the future using standardized quantum-safe security

While securing connected devices requires a multi-faceted approach, one important measure for robust security is to embed a root of trust which generally requires storing the keys within a tamper-resistant hardware security module (HSM). Today, asymmetric algorithms, such as RSA or ECC, are used for digital signatures which are vulnerable to the quantum threat. Fortunately, quantum-safe replacements exist today but they present new, yet manageable, implementation challenges that need to be considered. Stateful hash-based signatures are quantum-safe, mature and trusted but the private key requires unique state management techniques in order to be securely utilized or deployed.

## The solution

### Tamper-resistant HSM utilizing standardized stateful hash-based signatures for code-signing

The Luna HSM Post Quantum Crypto Functionality Module (FM) utilizes the ISARA Radiate™ Quantum-safe Toolkit and allows for stateful hash-based signatures to be used for code-signing today. This implementation includes mechanisms for key compression that are optimized for either speed or for size to help ensure that the private key is optimally stored and used in an operational environment with different requirements. A crucial feature of any HSM is its ability to handle High Availability (HA) and Disaster Recovery (DR). Mechanisms have been implemented to perform careful private key state management, and provide different private key splitting strategies to enable HA and DR capabilities for stateful hash-based signatures.

## Why use the Luna HSM Post-Quantum FM utilizing ISARA Radiate?

### Key advantages and features include:

- Use future-proof and standardized quantum-safe digital signature algorithms for all your long-lived devices today to ensure you can deliver secure and authenticated software/firmware updates far into the future
- The FM only uses stateful hash-based signatures standardized by the IETF, specifically HSS (Hierarchical Signature System) IETF RFC 8554, and XMSS (eXtended Merkle Signature System) IETF RFC 8391
- Enable quantum-resistant stateful hash-based signatures which are standardized by the IETF and soon to be approved by NIST under FIPS
- Stateful hash-based signatures enable crypto-agility in the face of quantum threats for identity use cases such as document and code signing

## Take the Post-Quantum Risk Assessment

Take our [Post-Quantum Risk Assessment](#) or contact us to learn why it's important to get started, and determine how you can begin preparing for the quantum era with solutions that are available today.

## 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.

For more detailed technical specifications, please visit [cpl.thalesgroup.com](http://cpl.thalesgroup.com) or [www.isara.com](http://www.isara.com)

## About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> [cpl.thalesgroup.com](http://cpl.thalesgroup.com) <    

**Americas** – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax: +1 954 888 6211 • E-mail: [sales@thalessec.com](mailto:sales@thalessec.com)  
**Asia Pacific** – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: [apacsales.cpl@thalesgroup.com](mailto:apacsales.cpl@thalesgroup.com)  
**Europe, Middle East, Africa** – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: [emea.sales@thales-esecurity.com](mailto:emea.sales@thales-esecurity.com)