Tomorrow's Cyber Security, Today

IRONCAP

Quantum-Safe Blockchain:

Ahead of the Curve Technology is Here

Be Ready with Quantum-Safe Blockchain

Blockchain has been coined as unbreakable by hackers but new developments in quantum computing are threatening its ultra-secure status. Quantum-Safe Blockchain is available now from Thales Luna with the IronCAP™ FM (functional module). Be ready for future quantum computing threats with this commercially available, seamless integration via industry standards PKCS#11.

Experts proclaim that the fourth industrial revolution is here with recent and rapid advances in quantum computing such as IBM's 1000 qubit Quantum Condor chip. While quantum computing opens up an astonishing new world of computation, the dark side is the quantum threat. This threat is very real as quantum computing renders all current popular encryption methods, such as RSA, elliptic curve, etc. which form the most crucial part in a blockchain, useless. Blockchain depends on the disseminated consensus of trust, achieved through existing hash functions and public-key cryptography. While the chain itself is relatively secure, the endpoints wallets etc. have already been proven "hackable" and quantum methods will expose the chain to fraudsters and thieves.

A quantum computer - harnessing exponential computing power to solve complex problems, is already being embraced by nation states and forward-thinking businesses to solve complex problems. This evolution, from academia and physics principles to commercially available solutions, has already created promise in new drug discovery (e.g. McKinsey's plans to use quantum computing on molecular formations.), deeper and faster analytics for financial trading, efficiency improvements in supply chain management systems and many other exciting and bleeding-edge applications.

The uncertainty over "Y2Q" (Years-to-Quantum) is simply a myth when hackers have already adopted a "steal and harvest" strategy which allows for future decryption when quantum computers have the capacity to do so. Let's also remember that the massive project of quantum-proofing data and systems is a multi-year endeavour.

Now is the time to protect blockchain applications with PQC (Post-Quantum Cryptography)

IronCAP™ crypto engine is a highly effective quantum-safe toolkit that is in lock-step with the NIST recommendation and compatible with the PKCS#11 stack and can facilitate a seamless integration, with virtually no changes in the code of the existing blockchain applications.

Blockchain Technology Architecture and its Security Vulnerability

Blockchain is a decentralized database that can be accessed simultaneously by a significant number of users. This requires a robust computer system with huge storage capacity to manage a substantial volume of data and transactions. It is expected to offer security in each of these blockchain technology layers (specific to security) – application layer, consensus layer, network layer and data layer.

APPLICATION LAYER
CONSENSUS LAYER
NETWORK LAYER
DATA LAYER

THALES

Building a future we can all trust

Each layer is vulnerable to different types of cyber attacks including **privacy leakage, routing attacks, "51%" attacks, Sybil attacks, end-point vulnerabilities, and more.** The network and data layers are most susceptible. The security and privacy of this data is paramount to the integrity of these layers. Digital signatures, hash functions, public keys and private keys are used to validate the transaction before it is added to the blockchain system.

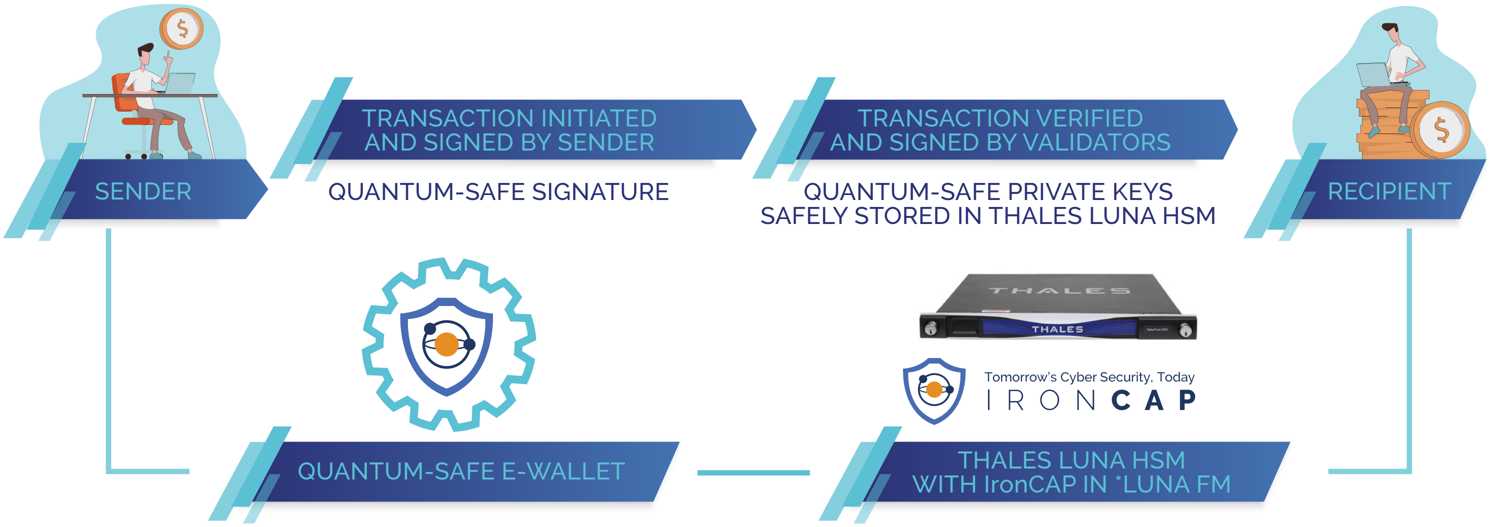
Blockchain and quantum computing are ground-breaking technologies and they bring both advantages and challenges; hence the dilemma. While quantum attacks on the blockchain structure may still be years away, the end-point vulnerability of the blockchain is an immediate threat. Once the (now vulnerable) digital signature is forged, counterfeit transactions can be initiated and validated at-will.

Numerous massive crypto thefts have been reported already - quantum computing has the power to destroy the entire blockchain/trust ecosystem. Now what?

Ahead of the Curve Technology for Quantum-Safe Blockchain is available NOW

Commercially Available

- Seamless integration via industry standards: PKCS11
- Proven Technology (Patent-Protected)
- IronCAP™ technology is protected by its US Patent #11,271,715
- IronCAP™ includes latest NIST approved cryptography
- Industry endorsed and held 2 successful global hackathons in 2019-2021



SENDER

TRANSACTION INITIATED AND SIGNED BY SENDER

QUANTUM-SAFE SIGNATURE

TRANSACTION VERIFIED AND SIGNED BY VALIDATORS

QUANTUM-SAFE PRIVATE KEYS SAFELY STORED IN THALES LUNA HSM

RECIPIENT

QUANTUM-SAFE E-WALLET

THALES LUNA HSM WITH IronCAP IN *LUNA FM

*FUNCTIONALITY MODULE

About 01 Communique

01 Communique is one of the first-to-market, enterprise level cybersecurity providers for the quantum computing era. The Company's cyber security business unit focuses on post-quantum cybersecurity with the development of its IronCAP™ technology, protected in the U.S.A. by its patent #11,271,715. For more information, visit the Company's web site at www.ironcap.ca and www.01com.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.

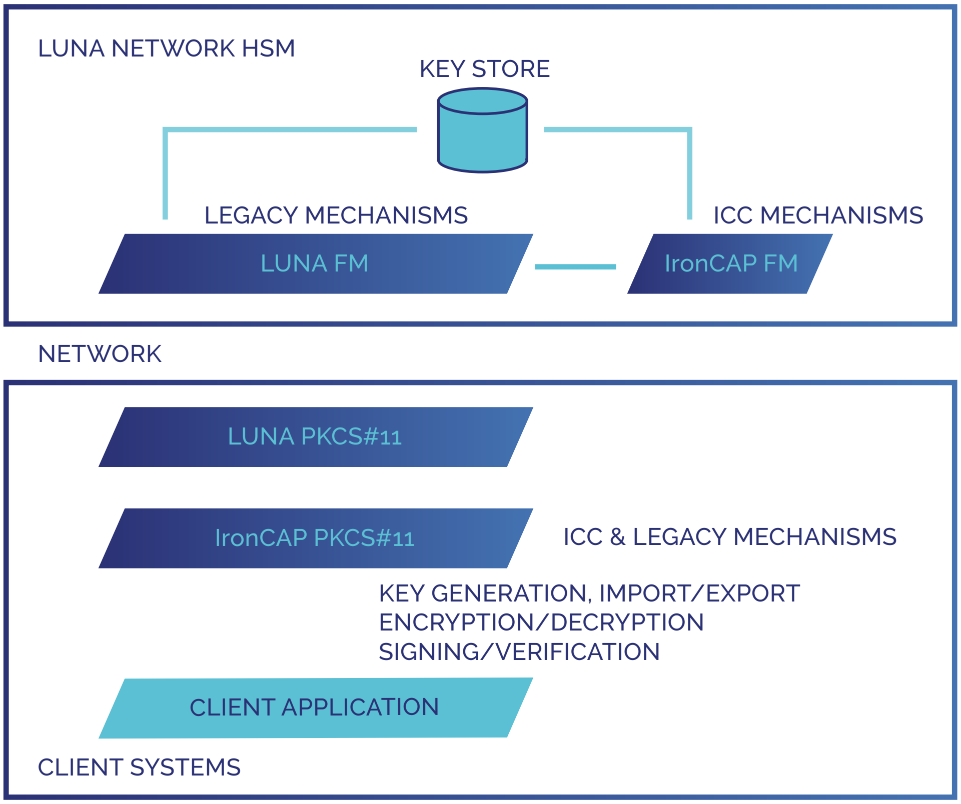
Tomorrow's Cyber Security, Today
IRONCAP

Thales Luna FM and IronCAP™ Integration Description:

IronCAP™ FM (*Functionality Module) for Luna HSM is designed to allow users of Thales Luna HSM, via industry standard of PKCS#11 interface, to seamlessly utilize IronCAP™'s quantum-safe cryptographic functionalities such as key generation, digital signature, signature verification, encryption, decryption, etc. Users of Thales Luna HSMs can take full advantage of the benefits from both worlds allowing Luna HSM's military-grade hardware security to safely store and backup the private key while using IronCAP™ to achieve all the quantum-safety crypto operations.

IronCAP™ for Luna consists of two main components: IronCAP™ FM and IronCAP™ PKCS#11 interface. IronCAP™ FM resides in the Luna Network HSM. It contains the IronCAP™ library for post-quantum cryptography, serving as an extension to legacy cryptography support within the Luna FM. IronCAP™'s PKCS#11 interface resides in the client system. This provides an API to crypto functions: key generation, key import/export, data encryption and decryption, data signing and signature verification for both legacy mechanisms, as well as, post-quantum mechanisms from IronCAP™.

Once the IronCAP™ PKCS#11 interface is installed, all crypto functions will be accessible. Operationally, Luna PKCS#11 works exclusively with Luna-FM. IronCAP™ PKCS#11 interfaces with Luna PKCS#11 to provide post-quantum cryptography support in Luna Network HSM. Current applications utilizing the Luna PKCS#11 can readily use IronCAP™ PKCS#11 for existing mechanisms. For post-quantum mechanisms, it is nothing more than specifying the IronCAP™ mechanism in the API call. A sample client application is provided to illustrate how an application will utilize IronCAP™ PKCS#11 interface to do post-quantum key generation, key import/export into/from Luna Network HSM key store, data encryption and decryption, data signing and signature verification.



VERIFIED SOLUTION
THALES

- Thales Luna HSM users can easily migrate to quantum-safe Signature/Verification and Key Encapsulation Encryption/Decryption

* Luna FM is sold as an add-on component for Luna HSM

- PKCS#11 compatible – virtually no changes in the application codes

- Backward compatible with traditional crypto (e.g. RSA)