Tomorrow's Cyber Security, Today
IRONCAP

Thales Luna HSM
with Post-Quantum Cryptography

Be Ready for the Post-Quantum World of Cybersecurity

IronCAP™ FM 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 and decryption operations. Users of Thales Luna HSM 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 execute all of 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™ 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.

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.

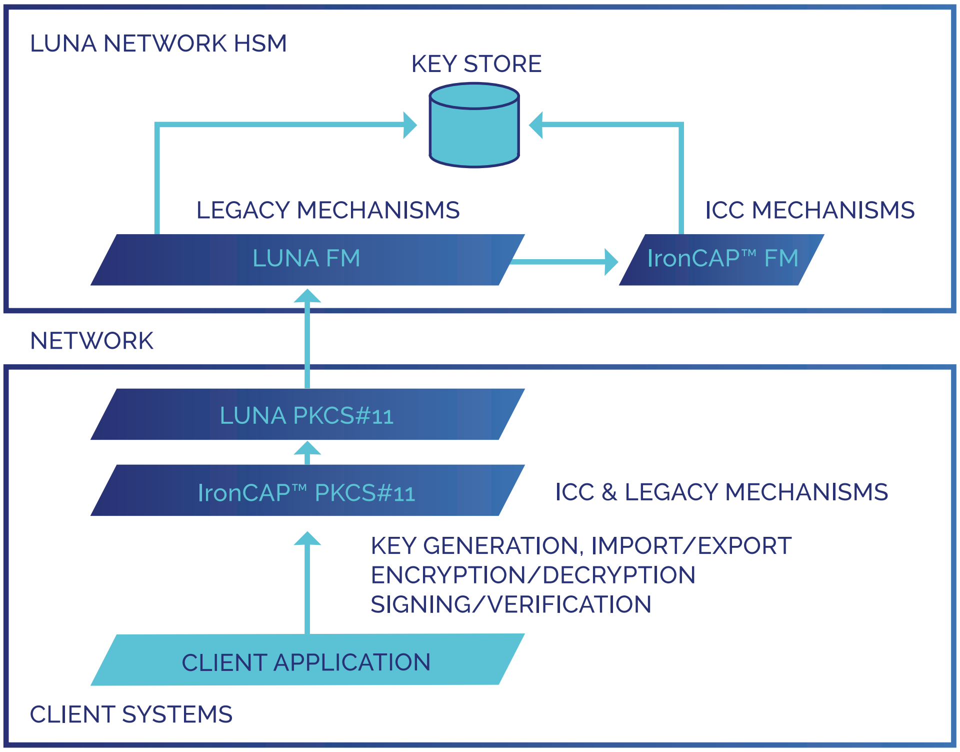
About Thales

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.

01 Communique
789 Don Mills Road
Toronto, ON, M3C 1T5, Canada
1-800-668-2185 | 01com.com

THALES
Building a future we can all trust



LUNA NETWORK HSM

KEY STORE

LEGACY MECHANISMS

ICC MECHANISMS

LUNA FM

IronCAP™ FM

NETWORK

LUNA PKCS#11

IronCAP™ PKCS#11

ICC & LEGACY MECHANISMS

KEY GENERATION, IMPORT/EXPORT
ENCRYPTION/DECRYPTION
SIGNING/VERIFICATION

CLIENT APPLICATION

CLIENT SYSTEMS

VERIFIED SOLUTION
THALES

- Thales Luna HSM users can easily migrate to quantum-safe Signature/Verification and Key Encapsulation Encryption/Decryption
- No hardware changes required. Simply install the IronCAP™ FM into your existing Lune HSM to provide quantum-safe cryptography.
- PKCS#11 compatible – virtually no changes in the application codes
- Backward compatible with traditional crypto (e.g. RSA)

Potential Users of IronCAP™ FM

- Government
- Large telcos
- Commercial banks
- Central banks
- Fintech industry
- Large enterprises