Trusted Cyber Technologies

Luna Credential System

HSM-Secured Identity Credentials

Certificate-based, multi-factor authentication is a mainstay security technique used by the U.S. Federal Government to ensure the identities of entities within a Public Key Infrastructure (PKI). Two primary components of multi-factor authentication are "what you have" and "what you know." The "what you have" in a PKI consists of a securely stored private key and an associated digital certificate that are the unique user credentials identifying the entity. The "what you know" is a password to unlock access to the securely-stored credentials. When the entity in need of a certified identity is a person, secure storage and distribution of the user credentials is often easily facilitated by utilizing existing technology, such as a secure smart card or USB token. The person assumes physical ownership and responsibility of the token and can use it as needed to access PK-enabled resources. But what if the entity in need of credentials is a non-person entity (NPE), like a device, software robot or some other automation technology? These entities still must have hardware-secured credentials to meet security mandates. Or what if the entity is indeed a person, but token use is not desirable or not an option?

With this in mind, any or all of the following issues may present roadblocks to the use of a multi-factor token for all users in a PKI:

- Policy may dictate that a token cannot be issued to a non-person entity
- The physical security of a token issued to a non-person entity presents a cumbersome, inefficient, or impossible requirement to meet
- Virtual machines are being used which can't access physical tokens
- Multiple physical machines require access to the credentials on a single token
- Hardware-based, multi-factor authentication is needed for human users, but token use is either not feasible or undesirable

Thales Trusted Cyber Technologies (TCT) has filled this troublesome gap in hardware-protected, PKI user credentials with its innovative Luna Credential System.

Luna Credential System

The Luna Credential System (LCS) introduces a new approach to multi-factor authentication by maintaining user credentials in a centralized on-premises or cloud-based hardware device that is securely accessible by endpoints in a distributed network. It unites the familiarity of certificate-based authentication with the security of a FIPS 140-2 Level 3 certified hardware security module (HSM). LCS is a multi-purpose, secure credential system ideally suited for an environment in which the endpoints cannot use a traditional small form-factor token. Composed of the Luna Credential HSM and the Luna Credential Client, LCS supports a number of use cases including Windows Logon and authentication to PK-enabled applications and websites.

Luna Credential HSM

Derived from TCT's flagship Luna T-Series, the Luna Credential HSM generates and protects PKI user credentials within the HSM thereby replacing individual tokens. Credentials never leave the security boundary of the HSM and can only be accessed by authorized endpoints over a secure communication link. The Luna Credential HSM provides a scalable architecture and supports multiple, independent "credential bins." A credential bin is a cryptographically isolated location within the HSM that contains the private key and associated certificate for individual entities. These identity credentials can only be accessed by endpoints when the correct password for the credential bin is provided. An internal credential directory is maintained by the Luna Credential HSM to correspond bins with entities that access the bins via the Luna Credential Client.

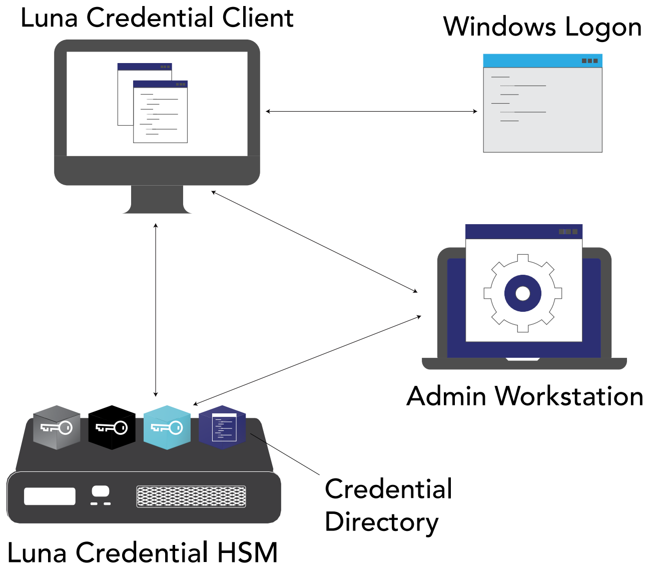
Luna Credential Client

The Luna Credential Client, which is installed on the endpoint machine, provides an equivalent user experience to traditional multi-factor authentication login. During any operation that needs the entity's certificate and corresponding private key, the Luna Credential Client establishes secure communications to the HSM. Utilizing the credential directory onboard the HSM, the client determines the correct credential bin for the given entity and sends the password to the HSM. Once the password is validated, the process on the endpoint system can proceed to utilize the keys and certificates within the entity's specific credential bin. This password may be entered by a human user, or in the case of a NPE, may be supplied by an automated process.

The Luna Credential Client includes a Windows credential provider component that prompts the user for their credential bin password and proceeds to complete the standard Windows Logon using identity credentials residing in the credential HSM. By hooking into the natural authentication flow of Windows systems, the user experience is no different from what users are accustomed to. Additionally, the Luna Credential Client includes an API to allow technology partners with their own credential providers or automated Windows Logon processes to make use of the Luna Credential System.

Luna as a Service Credential System

LCS is also available as a FedRAMP® High authorized cloud service. Thales TCT has partnered with XTec to deliver Luna as a Service Credential System to U.S. Federal Government agencies. Luna as a Service Credential System is provided through XTec's FedRAMP High AuthentX Cloud Software as a Service platform. Customers benefit from XTec's full time maintenance and support for services that reduce overhead and the burden within your agency. AuthentX Cloud is housed across three geographically separated facilities within the U.S.



Use Cases

NPE Identity Credentials

NPEs, such as the software robots used in Robotic Process Automation (RPA), are required to have digital identities and credentials to operate in production systems. LCS securely maintains the NPE credentials and provides programmatic interfaces for the robots to utilize the credentials. A primary use case is when unattended robots use LCS to meet requirements to perform a Windows Logon using identity credentials secured in a FIPS 140-2 certified HSM. LCS also supports unattended or attended robots use of hardware secured identity credentials when the robot is authenticating to a PK-enabled application or web site.

User Authentication

Although traditional password authentication and PKI authentication using software-based credentials are known to be insecure compared to hardware-based smartcards and tokens, these solutions continue to be deployed since organizations need the elasticity of software-based authentication to address the proliferation of the mobile workforce and the disparate variety devices used by workers. LCS provides the best of both solutions by offering secure, hardware-based multi-factor PKI authentication with software-like flexibility, scalability, and ease of use.

Credential Data Protection

Identity credentials often contain sensitive user and organization information. These credentials are left vulnerable when stored on a physical token that can leave the boundaries of a secure environment. With LCS, identity credentials are stored within the confines of a centralized HSM thus mitigating the risk of accidental loss or intentional compromise of a physical token.

Digital Signatures

Digital signatures attached to emails and documents are a well-accepted solution to verify the identity authenticity of the signer. LCS leverages the existing integrations between applications and PKI tokens (or smart cards) to allow LCS users—either a human user or an NPE such as a software robot—to digitally sign documents and emails using the key that resides in, and never leaves, the Credential HSM. Without any changes to the applications or workflows, LCS provides a FIPS 140 certified solution to digitally sign a wide array of Microsoft Office files (documents, spreadsheets, presentations) and emails.

Benefits

Technology Enabler

- Facilitates the use of new technologies, such as Robotic Process Automation, in production systems
- Supports the use of multi-user and/or NPE Windows workstations

Ease-of-Use

- Seamless user experience when performing fundamental tasks like Windows Logon or website login
- Credential HSM integrates with existing network infrastructure

Ultra-Secure Hardware Platform

- Performs hardware-based key generation
- Private keys always remain in Credential HSM
- Multiple layers of security to restrict access to keys and certificates

Compliance

- FIPS 140-2 certified Luna Credential HSM
- Meets OMB Memo M-19-17 requirements for the management of digital identities.
- DoD Instruction 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling
- DoD Instruction 8520.03, Identity Authentication for Information Systems
- Detailed logging and audit tracking of all key utilization, administrator access and policy changes

Scalability

- Provides a scalable architecture to support growing use of devices and automated technologies
- Enables access from anywhere by eliminating the need for a physical token

A Trusted U.S.-Based Source

- TCT develops, sells, manufactures, and supports our core data security solutions solely within the boundaries of the U.S., thus providing a completely trusted U.S. based supply chain

Technical Specifications

- Supported Operating Systems: Windows 10, Windows Server 2016, and Windows Server 2019
- Credential HSM: Refer to Tech Specs of the Thales TCT Luna T-Series Network HSM
- Scalability: The Luna Credential HSM provides a scalable architecture supporting multiple independent "credential bins"

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

For more information, visit www.thalestct.com