Luna Credential System

HSM-Secured Identity Credentials

Thales TCT's Luna Credential System introduces a new approach to multi-factor authentication by maintaining user credentials in a centralized 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 certified HSM.

Public Key Infrastructure Basics

- Unique user credentials with private key & digital certificate
- Generally stored on token or smart card

- Password to unlock access to securely-stored credentials

Identity Management Challenges

Robotic Process Automation (RPA)
- Hindered by federal systems built around PKI authentication based on smartcards
- RPA required to use "smartcard logon" for approval to operate in production systems
- OMB Memo M-19-17 policy requires management of digital identities for RPA

Credential Data Protection
- Identity credentials often contain sensitive user and organization information
- Sensitive data can't be put on smartcards that leave a closed area
- Current solution is software credentials

Mobile Workforce with Use of Multiple Devices
- SW-based credentials are less secure than HW-based smartcards & tokens
- Organizations need the elasticity of software-based authentication for their mobile workforce and the disparate variety devices used by workers

Virtual Machine Access to Physical Credential
- Often difficult to connect smartcards to virtual machines
- Multiple virtual machines need to use the same credential

Luna Credential System
New Approach to Multi-Factor Authentication

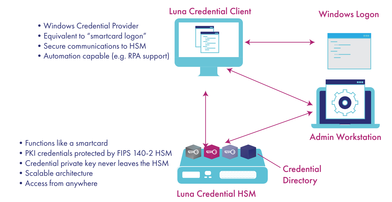
- Maintain user credentials in a centralized hardware device that is securely accessible by endpoints in a distributed network

- Unites familiarity of certificate-based authentication with the security of a FIPS 140-2 certified HSM

- Suited for environments in which endpoints can't use traditional small form-factor token

- Use cases include Windows Logon and authentication to PK-enabled applications and websites

How it Works



- Windows Credential Provider
- Equivalent to "smartcard logon"
- Secure communications to HSM
- Automation capable (e.g. RPA support)

- Functions like a smartcard
- PKI credentials protected by FIPS 140-2 HSM
- Credential private key never leaves the HSM
- Scalable architecture
- Access from anywhere

Luna Credential System Applications

RPA Identity Credentials

RPA robots are required to have digital identities and credentials to operate in production systems.

LCS securely maintains the RPA credentials and provides programmatic interfaces for the robots to utilize the credentials.

User Authentication

Software-based authentication, while not as secure as hardware-based authentication, addresses the proliferation of the mobile workforce and the disparate variety devices used by workers.

LCS provides secure, hardware-based multi-factor PKI authentication with software-like flexibility, scalability, and ease of use.

Credential Data Protection

Identity credentials 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.

LCS stores identity credentials within the confines of a centralized HSM mitigating the risk of accidental loss or intentional compromise of a physical token.

Digital Signatures

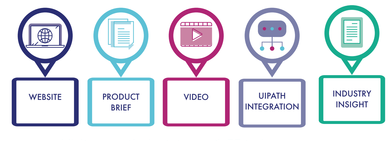
Digital signatures attached to emails and documents verify the identity authenticity of the signer.

LCS leverages the existing integrations between applications and PKI tokens to allow LCS users—either a human user or RPA robots—to digitally sign documents and emails using the key that resides in, and never leaves, the Credential HSM.

Luna Credential System Benefits

Technology Enabler	• Enables the use of new technologies (RPA) in production systems • Supports the use of multi-user and/or RPA Windows workstations
Ease-of-Use	• Seamless user experience for 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 • OMB Memo M-19-17 requirements for the management of digital identities. • DoD Instruction 8520.2 for PK-enabled info systems
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
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

Learn More About Luna Credential System



Visit www.thalestct.com/LCS to learn more

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

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com