RPA Cryptographic Authentication with Luna Credential System

The Challenge

UiPath is the leading platform for enterprise Robotic Process Automation (RPA). UiPath's Enterprise RPA platform is used to rapidly deploy software robots that emulate and execute repetitive processes, boosting productivity, ensuring compliance and enhancing the experience across back-office and front-office operations. UiPath's solution establishes automated and repeatable workflows that can save organizations thousands of labor hours per year.

UiPath robots can operate in two automation modes: attended and unattended. In attended automation mode, a user or operator launches and maintains involvement in the RPA process with the RPA leveraging the current user's security credentials. In unattended automation mode, the RPA acts autonomously in place of a user or operator leveraging its own security credentials.

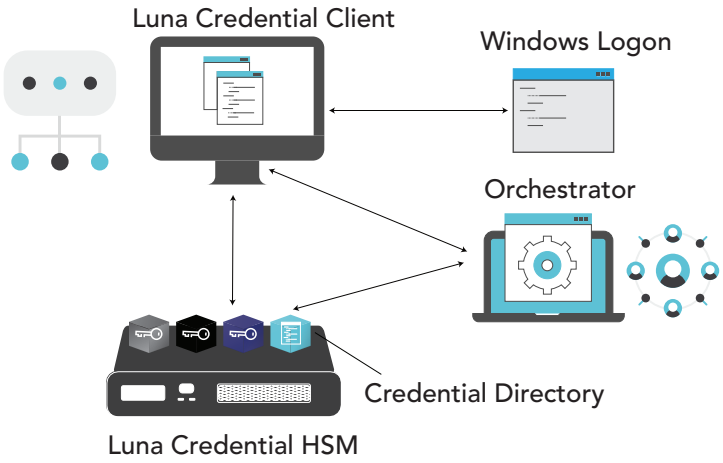
U.S. Federal agencies often require PKI certificate-based authentication to perform Windows Logon and to access public key enabled (PK-enabled) information systems (see DoD Instruction (DoDI) 8520.2). This requires use of a multi-factor authentication token that performs a cryptographic operation using the certificate and keys residing within the token. Traditional multi-factor authentication can introduce roadblocks to new technologies like RPA.

The Office of Management and Budget Memo M-19-17 outlines a policy that requires management of digital identities for non-person entities (NPEs) such as software robots. This means that all robots are required to have individual digital identities and credentials that are managed in the same fashion as traditional user identities. Although robots cannot be issued a physical token, they can utilize multi-factor login capabilities through the use of a centralized, hardware security module-based authentication system.

Luna Credential System

The Luna Credential System (LCS) 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 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.

Robotic Network Login



Luna Credential HSM

Derived from Thales Trusted Cyber Technologies's flagship Luna HSM for Government, 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 supporting 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 non-person entity, 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.

Key Benefits

Ultra-Secure Hardware Platform

- Performs hardware-based key generation
- Private keys always remain in the Luna 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

- Thales Trusted Cyber Technologies 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

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.

Contact Us: For more information, visit www.thalestct.com

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