UiPath™

THALES
Building a future we can all trust

Securing UiPath Credential Stores with Thales Trusted Cyber Technologies' Luna Vault

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.

Central to the management of UiPath Robots is Orchestrator, a web application responsible for provisioning, scheduling, monitoring, and deploying the Robots. All Robots, whether attended or unattended, communicate with Orchestrator to get all the information necessary for their operation, including credentials and workflow assets. By default, these credentials and assets are stored in a software database on the Orchestrator server in "Credential Stores" that are created by Orchestrator administrators. A quick glance at cyber security news is all it takes to know that storing sensitive data in software is not the most secure way to protect data.

The Solution

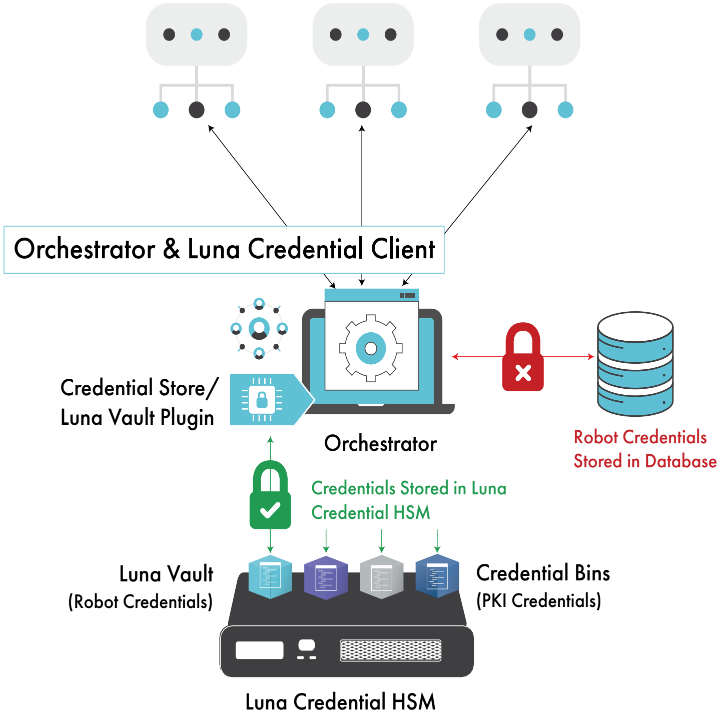
Thales Trusted Cyber Technologies' (TCT) Luna Vault

Knowing that some customers, like agencies of the U.S. Federal Government, have more stringent security requirements for the storage of sensitive data, UiPath implemented support for third-party Credential Store plugins that allow for enhanced security solutions for these Credential Stores. In response to U.S. Federal Government needs, Thales TCT created a Luna Vault Plugin as part of its Luna Credential System RPA security solution that enables its Luna Credential Hardware Security Module (HSM) to be used to provide hardware-based, FIPS 140-2 Level 3 security for Credential Stores.

The Luna Vault Plugin is an installation option in the Luna Credential Client software component of the Luna Credential System. In order to protect UiPath Credential Stores, the Luna Credential Client software is installed on the Orchestrator server and facilitates secure communication with HSM. Once the Luna Vault Plugin is installed and configured, an Orchestrator administrator is able to create a new Credential Store and specify a Luna Vault on the HSM as the target storage location. Both Robot Credentials and Assets can be specified for storage in the resulting Luna Vault.

The Luna Credential HSM and Client are part of Thales TCT's Luna Credential System that can also provide hardware storage of PKI credentials for Robots using Windows Logon. The Luna Vault Plugin can be used as a standalone feature providing hardware storage for an Orchestrator Credential Store, or it can be used in conjunction with the Windows Logon feature to also enhance security of the high-level Robot password (Credential Bin password).

Whether used as a standalone feature or an add-on feature, the Luna Vault provides the peace of mind knowing sensitive data-at-rest is being stored within the safe confines of a hardware security module.


Orchestrator & Luna Credential Client
Credential Store/ Luna Vault Plugin
Orchestrator
Robot Credentials Stored in Database
Credentials Stored in Luna Credential HSM
Luna Vault (Robot Credentials)
Credential Bins (PKI Credentials)
Luna Credential HSM

About the Luna Credential System

The Thales TCT Luna Credential System is comprised of the Luna Credential HSM, which is derived from Thales TCT's flagship Luna Network HSM, and the Luna Credential Client Software. The Luna Credential Client is specialized Luna Client software that is installed on the Orchestrator server and/or the endpoint Robot machines, depending on use case. The client also includes the Luna Vault Plugin as a selectable option upon installation on the Orchestrator server.

Key Benefits

Ultra-Secure Hardware Platform

- Hardware-based protection of Orchestrator Credential Stores
- Multiple layers of security to restrict access to the Credential Stores

Compliance

- FIPS 140-2 Level 3 validated 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.

For more information, visit www.thalestct.com