thalescpl.com

THALES

Securing Identities Where and When Needed

Large-Scale Identity and Certificate Management with SafeNet and Keyfactor

The Internet of Things (IoT) presents a huge business opportunity across almost every industry. But IoT also brings with it large scale, complex deployments that can cause security management challenges. As the scale of IoT deployments increase, the complexity of certificate lifecycle management increases. As the number of device grows, companies need the ability to quickly and securely store and manage an expanding number of keys and certificates. As IoT devices are deployed and dispersed across the globe, an organization must be able to secure communications and to protect the data in motion to and from these devices.

The Solution – Securing & Managing Deployed IoT Security Systems

A strong, enterprise class, IoT security solution requires a combination of automated Public Key Infrastructure (PKI) certificate provisioning, firmware code signing, high-assurance key storage, and a powerful management system that simplifies certificate lifecycles while meeting data security and compliance requirements. Keyfactor and Thales bring together a solution of proven PKI and Key Storage solutions for both on-premises and in the cloud, combined with key lifecycle management systems to ease certificate deployments that handle the large scale and widely dispersed needs of IoT.

Thales has the depth of encryption and access management offerings to meet the needs of any deployment. With our Cloud 1st strategy we developed our HSM on Demand service, utilizing our deep industry experience and extends it to the cloud. And to protect applications and devices at the access point, Thales offers SafeNet Trusted Access, a cloud-based access management and authentication service. In addition to our industry-leading on-premises Luna HSM product line, Thales has partnered with Keyfactor to complete a flexible and powerful IoT offering.

- SafeNet Data Protection on Demand is a cloud based hardware security module (HSM) as a service that can be deployed within minutes and no need for specialized hardware or associated skills.
- SafeNet Luna HSMs store, protect and manage sensitive cryptographic keys on-premises in FIPS 140-2 Level 3, tamper-resistant hardware appliances, providing high-assurance key protection within an organization's own IT infrastructure
- Keyfactor Control enables device identity through a unique combination of certificate lifecycles management and automation at IoT scale and across all aspects of IoT ecosystem.
- SafeNet Trusted Access ensures secures identities and ensures secure access to devices and applications with a broad range of authentication methods.

Thales Use Cases for IoT:

1. Certificate Key issuance and management
2. Device Manufacturing Identity Provisioning PKI key issuance
3. Device and User Authentication during updates
4. Development and Update Code Signing
5. SSL/TLS Communication Private Key storage and management
6. Data at rest and data in motion security with advanced encryption entropy

Key Features

- Thales' SafeNet family of HSM solutions, either SafeNet Data Protection On Demand or Luna HSM, provide flexibility for cloud-based, hybrid/multi-cloud or on-premises root of trust protection and management of encryption keys.
- Keyfactor Control offers certificate lifecycle management that discovers, tracks and manages all credentials as well as providing code signing solutions for all classes of IoT devices, including embedded headless devices.
- SafeNet Trusted Access offers a broad range of authentication methods and adaptive access policies that evaluate risk conditions and validates users by enforcing the appropriate level of authentication where needed, ensuring the right people have access under the right conditions.

Solution Benefits

Many enterprises today need functionality of IoT with automated PKI capability and comprehensive certificate lifecycle management to meet the IoT security operation requirements of their deployments. The combination of Keyfactor Control, with Thales's SafeNet Luna HSM and the HSMoD service from SafeNet Data Protection On Demand provides:

Flexible HSM key protection solutions offer cloud, hybrid/multi-cloud and on-premises support that fit all deployments and meets the high-availability required for an IoT environment

- Device Identity Provisioning PKI key issuance during manufacturing establishes known device validation for its deployed lifecycle
- Device and user authentication assures identity before lifecycle events are performed
- Development Code Signing establishes strong, secure trust before device deployment
- Firmware Code Signing maintains trust during field software updates
- Automatic certificate discovery, inventory and issuance workflow reduces costs. Business continuity by avoiding certificate expirations that could cause expensive system outages
- SSL/TLS Private Key storage and management maintains secure communications during data exchanges with IoT devices. Offloading TLS/SSL operations increases system optimization
- Advanced encryption entropy ensure sensitive data at rest or in motion is secured

- MFA and User Validation make certain the right people have access at the right time to data stored on-premises or in the cloud

Thales's Value to IoT

Establishing Root of Trust to secure Identities and Communications throughout the IoT ecosystem

- Deployment flexibility with hardware- and cloud-based HSM solutions
- Device Manufacturing Identity Provisioning PKI key issuance
- Device and user authentication during updates
- Development and Updates Code Signing
- Certificate Key issuance and management
- SSL/TLS Communication Private Key storage and management
- Data at rest or in motion security with advanced encryption entropy
- Access management secures apps with policy-based authentication

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.

About Keyfactor

Keyfactor™, formerly Certified Security Solutions (CSS), is a leading provider of secure digital identity management solutions that enables organizations to confirm authenticity, and ensure the right things are interacting in the right ways in our connected world.

From an enterprise managing millions of devices and applications that affect people's lives every day, to a manufacturer aiming to ensure its product will function safely throughout its lifecycle, Keyfactor empowers global enterprises with the freedom to master every digital identity. Its clients are the most innovative brands in the industries where trust and reliability matter most.

> thalescpl.com <

Americas – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com