thalesgroup.com

THALES

Automated PKI and Data Security Management for IoT with Device Authority's KeyScaler and Thales HSMs

Helping Enterprise customers move easily and securely to IoT and the cloud

The Internet of Things (IoT) presents a huge business opportunity across almost every industry. But to realize that opportunity, enterprise IoT security must become a primary focus. IoT brings new security challenges introduced by the scale and pace of adoption, as well as the physical consequences of compromised security.

Any enterprise class IoT security solution requires a combination of automated Public Key Infrastructure (PKI), high-assurance key storage and management, accompanied by enterprise data security platform integration. It is important to implement the solution as device identity-centric with the modules working in unison, not as isolated modules, to meet data security and compliance (GDPR, HIPAA, PCI-DSS) requirements.

To help manage the security and complexity of the device identity, data security and compliance requirements, Device Authority and Thales have integrated KeyScaler's automated PKI for IoT technology with Thales' cloud-based or on-premises hardware security module (HSM) key protection technology. This integration allows Enterprises who have an existing investment in HSMs and Data Security Platforms to leverage them for automated PKI certificate provisioning, high-assurance device authentication and managed end-to-end encryption at IoT scale.

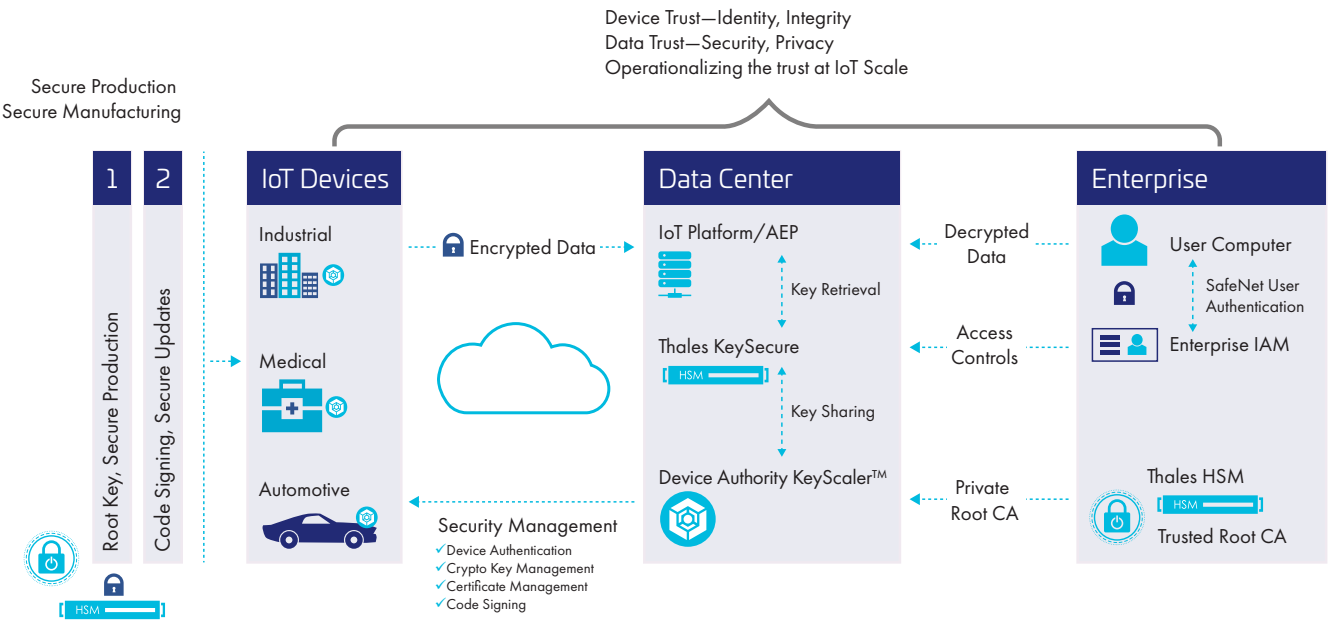
DEVICE AUTHORITY™
Trust for every Thing

IoT Security with automated PKI

Device Authority and Thales deliver a seamless integration that expands an organization's ability to secure PKI keys with the power of SafeNet HSMs to perform cryptographic operations in the most secure environment, no matter where they are deployed or used. Now your organization can automate the full key and certificate lifecycles with SafeNet Luna HSMs; from key generation to certificate provisioning and policy-based lifecycle management.

KeyScaler interfaces to Thales' HSMs for all its key protection needs. All operations are performed according to the centralized policy for key and certificate generation, use and renewal. SafeNet HSM also helps to protect KeyScaler platform keys and data.

Enterprise IoT Solution Blueprint



The integrated solution strengthens Device Trust, Data Trust and availability. KeyScaler extends support for growing numbers of Certificate Authorities (CAs) for solutions that require a public root of trust.

Solution Benefits

- Strong device identity, authentication and encryption
- Hybrid crypto key for data security
- Automated PKI management
- Help meet compliance mandates
- Flexible HSM key protection solutions offer cloud, hybrid/multicloud and on-premises support that fit all deployments and meets the high-availability required for an IoT environment
- Simplified IoT security management
- Firmware Code Signing maintains trust during device manufacturing and field software updates
- Bring Your Own Key (BYOK) for IoT data encryption and privacy

KeyScaler integrated with SafeNet HSMs provides high-assurance device authentication, managed end-to-end encryption, and certificate provisioning for connected IoT devices. After establishing the identity of the device as trusted, KeyScaler then leverages that trust to provide additional security operations, such as issuing a security token that the device can use to authenticate to other IoT platforms, or provisioning a unique device key and certificate. KeyScaler data encryption solution delivers policy-driven, end-to-end crypto services for data flowing through managed devices.

KeyScaler and Thales also allows enterprises to retain control of their own IoT data through the use of Bring Your Own Key (BYOK) technology. KeyScaler uses a public key to encrypt secrets which were used to protect data coming from an IoT device. This means that only the owner of the private key will be able to unlock the secrets and ultimately decrypt the IoT data. Thales provides the HSM functionality required to store the associated private keys. This solution allows enterprises to maintain complete control and access to IoT data and can strengthen their key management and data export practices.

Together we can help

Many enterprises today need functionality of IoT Identity and Access Management (IAM) with automated PKI capability to meet the IoT security operations requirements for their deployments. Device Identity centric KeyScaler together with SafeNet HSMs deliver high assurance:

- Device and Data Security
- Implementing and running security operations at IoT scale
- Meeting compliance requirements and requests

How It Works

KeyScaler uses SafeNet HSMs for securing two important areas in the solution. It uses the HSM for all its operational keys and crypto operations, as well as delivering strong device identity and data protection for IoT devices. KeyScaler automates the provisioning and managing of keys and certificates for IoT devices.

The steps are:

- KeyScaler requests keys to be generated in the SafeNet HSM. If a key pair is generated at the device, this step is not required.
- Following key generation, a certificate request is initiated.
- Once the certificate is approved and received by the KeyScaler Platform, the certificate is delivered to the IoT device through the KeyScaler automated process.
- When a certificate needs to be renewed or rotated, the full process is repeated.

High-Assurance Key Generation and Protection with Thales HSMs & KeySecure

Organizations that require a high level of assurance can protect their cryptographic keys in Thales HSMs. Thales' keys-in-hardware approach ensures your key pairs are securely generated in hardware, and your private key always remains centrally and securely stored, free from rogue administrators and hackers.

Thales offers two FIPS 140-2 Level 3 HSM solutions that can generate and securely store the server keys, providing private key protection.

- SafeNet Data Protection on Demand is a cloud-based 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 a, tamper-resistant hardware appliance, providing high-assurance key protection within an organization's own IT infrastructure

In addition, SafeNet KeySecure provides organizations with flexible options for secure and centralized key management – deployed in physical, virtualized infrastructure, and public cloud environments.

KeyScaler Platform

KeyScaler is an innovative platform that delivers:

- Secure device registration and certificate provisioning
- Policy-driven credential delivery and lifecycle management
- End-to-End device derived cryptography for data in transit and at rest across networks and cloud services

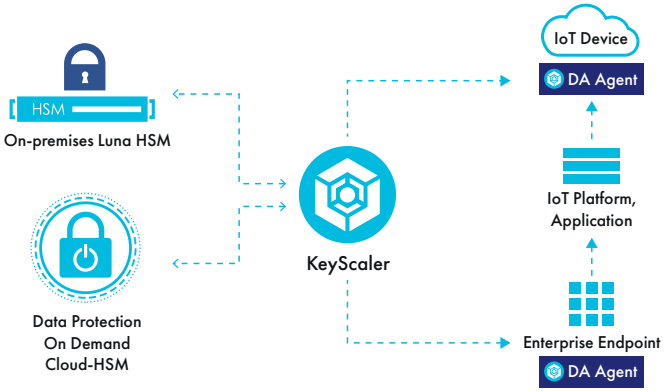
About Device Authority

Device Authority is a global leader in Identity and Access Management (IAM) for the Internet of Things (IoT); focused on medical / healthcare, industrial and smart connected devices. Our KeyScaler™ platform provides trust for IoT devices and the IoT ecosystem, to address the challenges of securing the Internet of Things. KeyScaler uses breakthrough technology including Dynamic Device Key Generation (DDKG) and PKI Signature+ that delivers unrivalled simplicity and trust to IoT devices. This solution delivers automated device provisioning, authentication, credential management and policy based end-to-end data security/ encryption.

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.



> thalesgroup.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • 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