Helping Enterprise customers move easily and securely to IoT

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 Gemalto have integrated KeyScaler’s automated PKI for IoT technology with Gemalto’s FIPS 140-2 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.

IoT Security with automated PKI

Device Authority and Gemalto deliver a seamless integration that expands an organization’s ability to secure PKI keys with the power of SafeNet Luna Network 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 Gemalto’s HSM for all its key protection needs. All operations are performed according to the centralized policy for key and certificate generation, use and renewal. SafeNet Luna HSM also helps to protect KeyScaler platform keys and data. 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
- Reduce risks with high-assurance, FIPS 140-2 HSM for tamper-proof hardware key protection
- Simplified IoT security management

KeyScaler integrated with SafeNet Luna HSM 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.

Together we can help

Many enterprises today need functionality of IoT IAM (Identity and Access Management) with automated PKI capability to meet the IoT security operations requirements for their deployments. Device Identity centric KeyScaler together with SafeNet Luna 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 Luna HSM 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:
1. KeyScaler requests keys to be generated in the SafeNet Luna HSM. If a key pair is generated at the device, this step is not required.
2. Following key generation, a certificate request is initiated.
3. Once the certificate is approved and received by the KeyScaler Platform, the certificate is delivered to the IoT device through the KeyScaler automated process.
4. When a certificate needs to be renewed or rotated, the full process is repeated.

High-Assurance Key Generation and Protection with SafeNet Luna HSMs & SafeNet KeySecure

Organizations that require a high level of assurance can protect their cryptographic keys in FIPS 140-2 Level 2 or 3 certified SafeNet Luna Network HSMs (tamper-resistant, network-attached appliances). Gemalto’s 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.

In addition to securing your cryptographic keys with SafeNet Luna HSMs, SafeNet KeySecure provides organizations with flexible options for secure and centralized key management – deployed in physical, virtualized infrastructure, and public cloud environments. Only Gemalto can deliver key management appliances across FIPS-validated hardware or a virtual appliance with a hardware root of trust using SafeNet Luna HSMs.

KeyScaler Platform

KeyScaler is an innovative platform that delivers:
- Secure device registration and provisioning
- Policy-driven credential delivery and management
- End-to-End device derived cryptography for data in transit and at rest across networks and cloud services

About Gemalto SafeNet Identity and Data Protection Solutions

Gemalto’s portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions from the edge to the core. Gemalto’s SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters.

Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation to protect customer trust in an increasingly digital world.

About Device Authority KeyScaler

Device Authority provides solutions to address the challenges of Identity and Access Management for the Internet of Things (IoT) without human intervention. Our KeyScaler™ platform provides trust for IoT devices and the IoT ecosystem. KeyScaler uses breakthrough technology including Dynamic Device Key Generation (DDKG) and PKI Signature+ that delivers unrivalled simplicity and trust to IoT devices through automated device provisioning, authentication, credential management and policy based end-to-end data privacy/encryption.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com/contact-us
Follow Us: blog.gemalto.com/security