TRUST IN DEVICES AND DATA ENABLES INCREASED ADOPTION OF IoT

- Strong device authentication
- End-to-end data encryption
- Hybrid crypto key for data security
- Automated PKI management
- FIPS 140-2 Level 3 key generation and storage

THE PROBLEM: TRUST AND COMPLIANCE

- Device trust – identity, integrity
- Data trust – security, privacy
- Public key infrastructure (PKI) key management

Today, the adoption of IoT technologies is rapidly increasing as enterprises seek to collect data to automate many business applications. However, trust in the data collected is imperative. If one cannot trust the data, there is no point in collecting, running analytics, and executing decisions based on the data. Data must be protected to ensure its confidentiality and integrity, and its reliability as a decision making tool.

THE CHALLENGE: OPERATIONALIZING TRUST

Maintaining the privacy of sensitive data is paramount in many industries. Increasingly stricter regulations are also making data privacy and security a real concern. IoT security is critical to prevent hacking and data breaches. The first challenge is to have strong mutual authentication and trust between devices and applications. The second challenge is to ensure the sensitive information flows all the way from source to destination, encrypted to meet compliance requirements such as the GDPR and HiPAA among others.

Thales nShield Connect secures the generation and storage of Device Authority KeyScaler™ master and tenant private keys.
DEVICE AUTHORITY AND THALES DELIVER SECURE AND TRUSTED IoT SOLUTIONS

THE SOLUTION: DEVICE AND DATA TRUST FOR IoT

Device Authority’s KeyScaler platform integrated with the Thales nShield Connect hardware security module (HSM), provides high-assurance device authentication, managed end-to-end encryption, and certificate provisioning for a variety of other connected devices. KeyScaler delivers a scalable, device-based authentication service based on the patented Dynamic Device Key Generation (DDKG) technology. The authentication and authorization solution utilizes a challenge-and-response mechanism to query the device hardware to establish a strong root of trust and identity assurance for headless (no visible user interface) 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. The KeyScaler data encryption solution delivers policy-driven, end-to-end crypto services for data flowing through managed devices.

WHY USE THALES nSHIELD HSMs WITH DEVICE AUTHORITY KEYSCLALER PLATFORM?

Encryption keys handled outside the cryptographic boundary of an HSM are significantly more vulnerable to attack, which can lead to compromise of critical keys. HSMs are the only proven and auditable way to secure valuable cryptographic material. nShield Connect secures the generation and storage of the private keys used by the KeyScaler platform within a FIPS 140-2 Level 3 and Common Criteria EAL4+ certified protected environment. Doing so provides the highest level of security and assurance against key compromise and theft.

THALES

Thales eSecurity is the leader in advanced data security solutions and services delivering trust wherever information is created, shared, or stored. Security solutions ensure that critical data is both protected and trusted in any deployment – on-premises, in the cloud, in data centers, or in big data environments – without sacrificing business agility. Security professionals around the globe rely on Thales to confidently accelerate their organization’s digital transformation. Thales eSecurity is part of Thales Group.

DEVICE AUTHORITY

Device Authority is the leading provider of Identity and Access Management (IAM) for the IoT. KeyScaler enables greater trust on devices and the ecosystem, to address the challenges of securing the IoT. The purpose-built solution:

➤ Uses a hybrid crypto model to capitalize on efficiencies of symmetric encryption with the scalability of PKI
➤ Derives the crypto key on the device, and not sent across the network, to significantly reduce the attack surface
➤ Encrypts data without prior knowledge of the destination entity

For more detailed information, please visit 
www.thalesesecurity.com or www.deviceauthority.com