ENTRUST TECHNOLOGY ALLIANCE PROGRAM

DEVICE AUTHORITY

Machine Identity Management for IoT with Device Authority's KeyScaler and Entrust PKI and HSM Solutions

Trust in devices and data enables increased adoption of IoT in Industrial, Automotive and Medical applications for improved cybersecurity and operational efficiency.

A fundamental requirement for IoT use cases is device trust (machine identity, integrity), data trust (security, privacy) and operational trust (OT) and this is best accomplished by leveraging the high assurance security and efficiency of Public Key Infrastructure (PKI) and Hardware Security Modules (HSMs). Machine identity use caes demand automation for data privacy and authenticity at IoT scale in order to meet the diverse cybersecurity and legislative requirements of different industries. IoT Security is critical to help prevent hacking and data breaches.

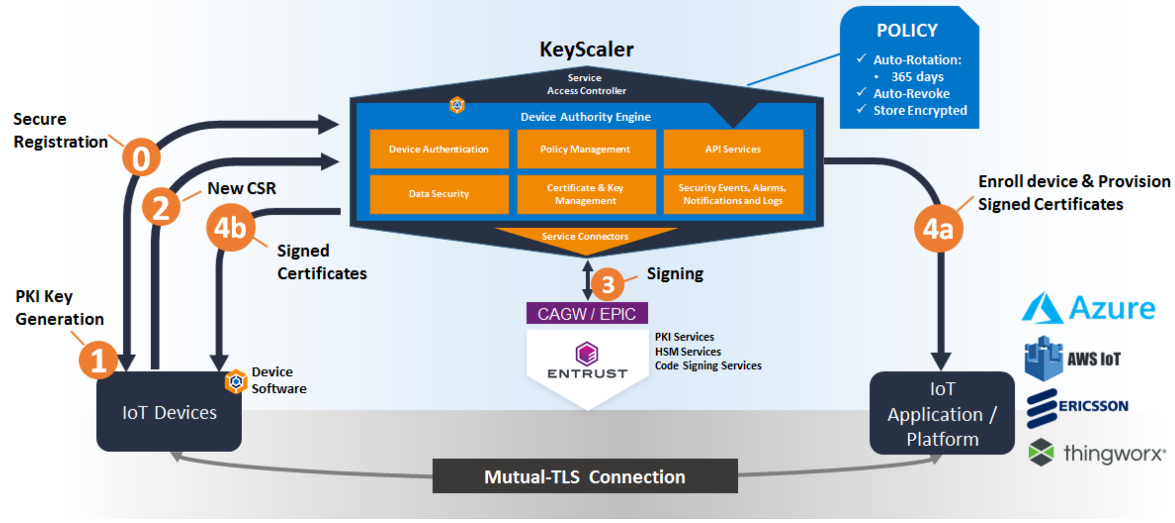
Managing machine identities and secure updates at IoT scale can be challenging throughout the lifetime of a device. Critical IoT applications demand a strong device identity model, real-time authenticity and authorization control, and data privacy controls to protect sensitive data. Industrial, Automative and Medical applications all rely on these fundamental security requirements to maintain trust in their deployments. In the scenario where a device collects patient data and exchanges this data over the internet, data privacy and security is of significant importance. 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, and is encrypted to meet compliance requirements.

THE SOLUTION:

Machine Identity and Key Management through the lifecycle of IoT devices – from manufacturing to decommission – protecting applications and data end-to-end.

Key Benefits

- Saves cost by improving efficiency & removing logistical challenges
- Real time authorization and authentication for IoT devices
- Provides device trust, data trust and automation at IoT Scale
- Machine identity lifecycle management – issuance, renewal & revocation
- Policy driven end to end crypto – PHI data protection
- Flexible architecture to fit most IoT use cases
- Connect and automate security to *any* IoT Cloud App or platform
- Cloud enabled solutions with KSaaS and PKIaaS
- FIPs Compliant PKI and HSM services
- Brownfield deployment options for legacy devices



HOW IT WORKS

Integration of the KeyScaler IoT IAM platform with Entrust PKI and nShield HSM Services provides device trust, data trust and automation at IoT scale. It enables security operations across device attestation/trust, device onboarding, machine identity lifecycle management, certificate signing and crypto operations – and is connected to Entrust FIPs compliant PKI and HSM solutions. By utilizing KeyScaler's pre-built service connectors or flexible integration framework, it automates security operations into *any* cloud application and platform. Components of this solution include:

- KeyScaler IoT Identity Access Management (IAM) Platform
- IoT Device – for verticals such as Industrial, Automotive and Medical (provided by customer)
- IoT Platform or Application – Azure, AWS, ThingWorx etc
- Entrust PKI – scalable cloud based, managed or on premise PKI for public and private certificates
- Entrust FIPs Compliant nShield HSMs

Initial attestation & trust between the device and KeyScaler is established when the device is powered up for the first time. The device "phones home" and attests its identity to the KeyScaler platform through an automated zero touch approach. Upon successful registration, the device will enroll to a group inside the platform, where each group will have tailored policies against it (e.g. PKI provisioning, Crypto key etc). The device will receive its policies and carry them out. For example when it receives a PKI policy, the device will generate a key pair and submit a CSR to KeyScaler. KeyScaler will then reach out to the Entrust PKI and/or HSM (configurable through policy) to request signing of the CSR. On the PKI front, customers can leverage Entrust CA Gateway with the KeyScaler connector to talk to any of the Entrust PKIs, as well as external PKIs like MSFT CA. Once signed, KeyScaler will then send the signed certificate securely to the device, enroll the device to the chosen IoT application, and assign an identity to the enrolled device in the application.

The solution outlined above solves the challenge of manually installing operational certificates in the device at manufacturing, and manual configuration of enrollment records in the applications. It also provides security management capabilities through a devices' lifetime so that customers can manage key rotation, renewal and revocation against policy to meet a robust security posture and meet compliance requirements.

WHY USE KEYSCALER

KeyScaler IoT IAM platform combines secure device onboarding and provisioning with policy-driven crypto and credential management to deliver comprehensive IoT PKI automation at scale. KeyScaler has a tokenized security model to enable IoT security for embedded devices and gateways, as well as any IoT application and platforms, such as Microsoft Azure, PTC ThingWorx and AWS IoT. The platform provides device makers and IoT applications with a turnkey, plug-and-play IoT security suite that is easy to deploy, easy to manage, and provides policy-driven automation for scalability, coupled with an architecture and deployment model which enables small and large enterprises to scale.

About Device Authority

Device Authority is a global leader in identity and access management (IAM) for the Internet of Things (IoT) and focuses on medical/healthcare, industrial, automotive, 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 simplicity and trust to IoT devices. This solution delivers automated device provisioning, authentication, credential management, policy-based end-to-end data security/encryption and secure updates.

deviceauthority.com

DEVICE AUTHORITY

About Entrust

Consumers, citizens, and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services, or logging onto corporate networks. Entrust offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports, and ID cards to the digital realm of authentication, certificates, and secure communications. With more than 2,500 Entrust colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

entrust.com

Learn more at
entrust.com

ENTRUST
TECHNOLOGY ALLIANCE
PROGRAM

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com   entrust.com/contact