Entrust and Device Authority Deliver Secure and Trusted Solution for IoT in Healthcare

Trust in devices and data enables increased adoption of IoT in healthcare for improved patient care and operational efficiency

HIGHLIGHTS

- 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

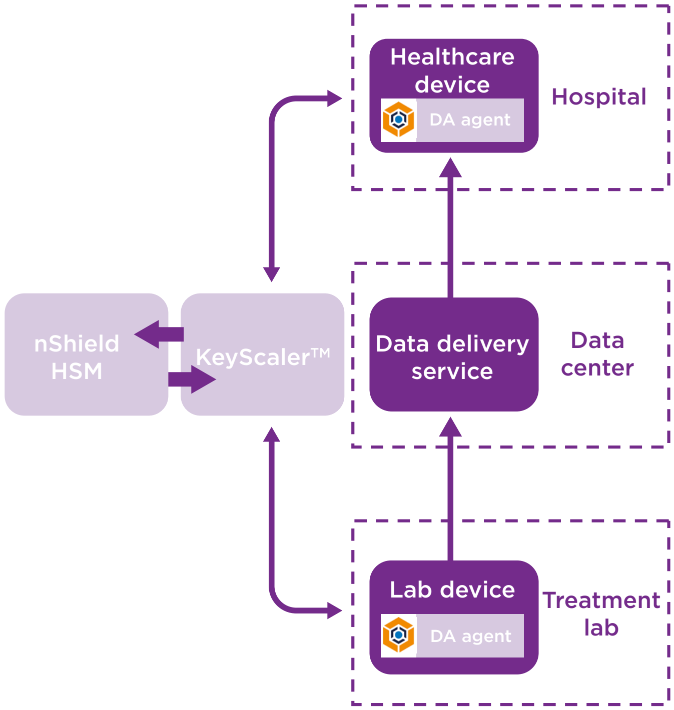
The problem:

Trust and compliance

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

Today, clinicians and healthcare devices generate large amounts of sensitive data, including protected health information (PHI) that needs to be securely delivered to other clinicians, healthcare devices, and applications.

The data needs to be encrypted and only accessible to authorized individuals and devices to deliver patient treatment.



Entrust nShield® Connect HSMs secure the generation and storage of Device Authority KeyScaler™ master and tenant private keys. Entrust nShield can be deployed on-premises or as a service.

DEVICE AUTHORITY
Trust for every Thing

LEARN MORE ABOUT HSM AT ENTRUST.COM

Entrust and Device Authority Integrated Solution

The Challenge:

Operationalizing trust

Maintaining the privacy of patient records and data is paramount in healthcare. If a facility, person, or device collects patient data and exchanges this data over the internet, then data privacy and security is a real concern. Internet of Things (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 HIPAA.

The Solution:

Device and data trust for IoT in healthcare

Device Authority's KeyScaler platform integrated with the Entrust nShield Connect hardware security module (HSM), provides high-assurance device authentication, managed end-to-end encryption, and certificate provisioning for healthcare and 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 Entrust nShield with Device Authority KeyScaler?

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 certified protected environment. Doing so provides the highest level of security and assurance against key compromise and theft. Entrust nShield is available in several form-factors: as an appliance, PCIe, USB, and as a service.

Entrust and Device Authority Integrated Solution

About Entrust HSMs

Entrust nShield HSMs are among the highest-performing, most secure, and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial, and government organizations. Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

About Device Authority

Device Authority provides Identity and Access Management (IAM) solutions 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

Learn more

For more detailed technical specifications, please visit **entrust.com/HSM** or **deviceauthority.com**

To find out more about
Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

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