nCipher
AN ENTRUST DATACARD COMPANY

www.ncipher.com

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

- 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

DEVICE AUTHORITY
Trust for every Thing

Device Authority and nCipher deliver secure and trusted solution for IoT in healthcare

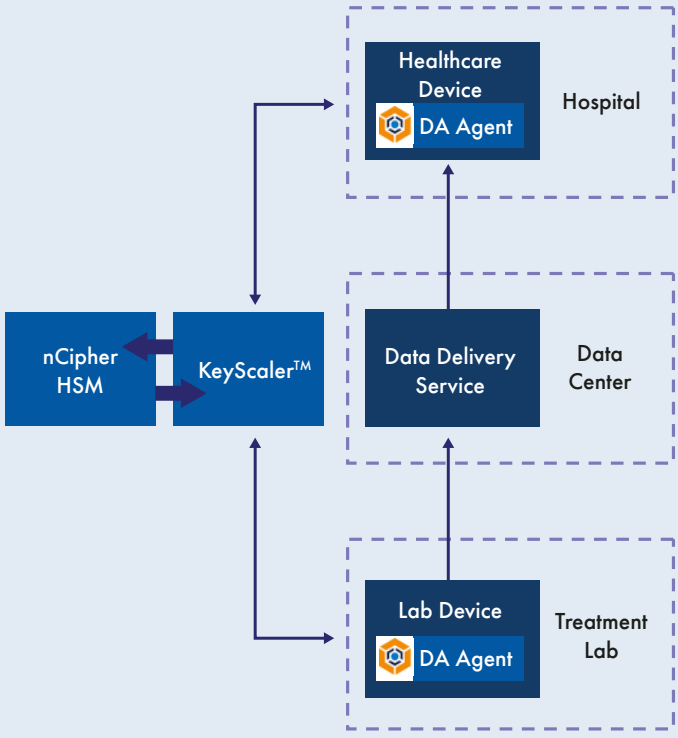
THE PROBLEM: TRUST AND COMPLIANCE

- 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 patient 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.

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. 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.



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

Device Authority and nCipher deliver secure and trusted solution for IoT in healthcare

THE SOLUTION: DEVICE AND DATA TRUST FOR IOT IN HEALTHCARE

Device Authority's KeyScaler platform integrated with the nCipher 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 NCIPHER 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. nCipher nShield is available in several form-factors: as an appliance, PCIe, USB, and and as a service.

DEVICE AUTHORITY

Device Authority is the leading provider of Identity and Access Management (IAM) for the Internet of Things (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

NCIPHER - AN ENTRUST DATACARD COMPANY

nCipher Security, a leader in the general purpose HSM market, empowers world-leading organizations by delivering trust, integrity and control to their business critical information and applications. Our cryptographic solutions secure emerging technologies - cloud, IoT, blockchain, digital payments - and help meet new compliance mandates, using the same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensuring the integrity of your data and putting you in complete control - today, tomorrow, at all times. The addition of nCipher to the Entrust Datacard family further extends its ability to provide customers with solutions that meet their demand for high assurance, as well as addressing the increased demand for data security stemming from regulations such as the EU General Data Protection Regulation (GDPR) and the electronic identification, authentication and trust services (eIDAS) regulation.

LEARN MORE

To find out more how nCipher Security can deliver trust, integrity and control to your business critical information and applications, visit www.ncipher.com

To find out how Device Authority can help you secure your IoT deployments visit www.deviceauthority.com