Bringing trust to the Internet of Things

- Establishes a root of trust for device authentication and data protection
- Provides validation of authenticity and integrity of device firmware updates
- Protects data from chip to cloud with certified encryption and key management
- Utilizes HSMs for protection of sensitive PKI private keys
- Interoperates with multiple partner applications
- Backed by professional services from the nCipher Professional Services

nCipher HSMs enable the root of trust in the manufacture and operation of IoT devices

The ability to distribute connected devices across a geographically-dispersed network provides organizations valuable functionality and opportunities for additional revenue. However, the "Internet-of-Things" (IoT) also presents considerable security risks and challenges for organizations. Specifically:

- Attackers impersonating a trusted device could conduct man-in-the-middle or other attacks
- Attacks on unsecured devices could expose protected content or enable access to other connected systems
- Without a root of trust, communications could be compromised, delivered incompletely, or lost
- The privacy and integrity of data stored on, and transmitted with, unsecured devices cannot be guaranteed

According to the 2018 Ponemon PKI Trends Study, 42% of IoT devices will use digital certificates for identification and authentication in the next two years. With billions of devices being deployed, demand for public key infrastructures (PKIs) to issue digital certificates is rapidly increasing. Once devices are deployed, operators must also ensure that code updates sent to devices are authorized and authentic, as software that has been altered or corrupted can expose the entire organization once it executes.

Protecting IoT data collected from dispersed endpoints presents a myriad of challenges, but one thing is certain: if you can't trust the data, there's no point in collecting, analyzing and making business decisions based on it. nCipher's solutions for IoT focus on the fundamentals of both device security and data protection to provide a root of trust for the entire ecosystems.

IoT
INTERNET
OF
THINGS
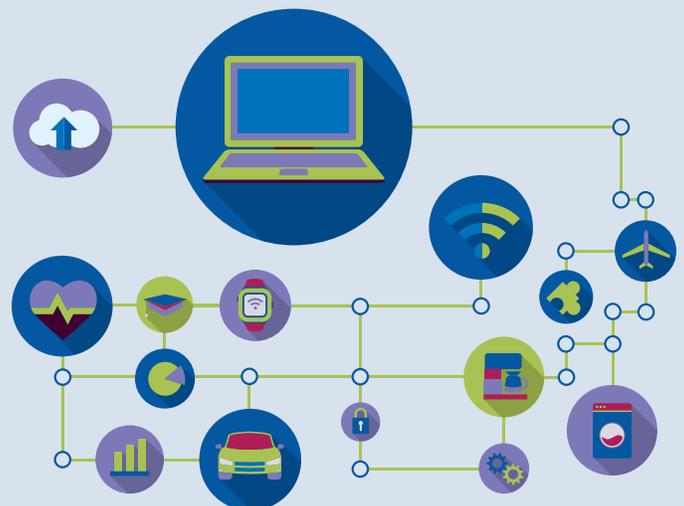
nCipher HSMs enable the root of trust in the manufacture and operation of IoT devices

To securely participate in the IoT, each connected device needs a unique identification – even before it has an IP address. This digital credential establishes the root of trust for the device's entire lifecycle, from initial design to deployment to retirement.

nCipher's nShield hardware security modules (HSMs), combined with supporting security applications from nCipher Technology partners, enable manufacturers to provide each device a unique ID using the strongest cryptographic processing, key protection, and key management available. A digital certificate is injected into each device to enable:

- Authentication of each device introduced to the organization's architecture
- Verification of the integrity of the operating system and applications on the device
- Secure communications between devices, gateway, and cloud
- Authorized software and firmware updates, based on approved code

All nShield HSMs feature our market-leading Security World key management architecture—proven technology that protects application keys within the safe confines of the HSM, yet allows them to be managed in a straightforward and convenient manner.

PKI SUPPORT

The IoT requires a secure and scalable solution for managing and protecting digital certificates. Based on the knowledge gained during dozens of PKI deployments, we have the expertise to help you build a PKI that meets your needs, regardless of scale or complexity. By securing the process of issuing certificates and proactively managing signing keys, you prevent their loss or theft, thereby creating a high-assurance foundation for digital security. Whether you work with one of our industry-leading PKI partners or tap into our Professional Services for support, nCipher HSMs provide an independently certified, tamper-resistant devices to secure some of your most sensitive keys and business processes in the organization—a widely recognized PKI best practice.

FAST, EFFICIENT CRYPTOGRAPHY

nCipher nShield supports all major cryptographic algorithms and offers the world's fastest support for elliptic curve cryptography (ECC). Given the limited processing power available with many small connected devices, ECC provides a strong and efficient alternative to traditional algorithms. Custom algorithms are also supported, executing them within the protected environment of the HSM using nCipher's unique CodeSafe capability.

SECURING OFFSHORE PRODUCTION

When outsourcing production, either in part or completely, organizations need assurance that manufacturing is completed according to project specifications. A combination of nCipher HSMs and credentialing software allows manufacturers to control the number of units produced as well as what code is built into each, even in a geographically-dispersed supply chain. This prevents unauthorized production runs and the introduction of unapproved code.

CODE SIGNING

The nCipher code signing solution helps software producers of all types implement highly secure and efficient code signing processes that protect their organizations from risks associated with software tampering. Combining tamper-resistant nShield HSMs with services from nCipher's Professional Services, the nCipher code signing solution is backed by our extensive expertise in code signing best practices and standards of due care. Our proven HSMs provide tamper-resistant, certified protection for private code signing keys and a secure platform to perform critical digital signature processes.

DEVICE-LEVEL SECURITY AND DATA PROTECTION

The combination of device-level protection delivered by nCipher nShield HSMs provide high assurance security to enterprise and cloud-based deployments where IoT data is stored, aggregated and analyzed.

Contact your account representative today or visit www.ncipher.com to learn how we can help you deliver trust to your IoT implementations.

> " nCipher's proven track record of delivering best-in-class cryptographic hardware security and key management will benefit our developers and the larger ecosystem by enabling a new generation of IoT products and applications to enter the market with enhanced privacy and security features critical for the broad array of products and services."
> – Curtis Sasaki, VP Ecosystems, Samsung Electronics

ascertia · CERBERUS Security Laboratories · CSS Certified Security Solutions, Inc. · *cybertronixx*

DEVICE AUTHORITY IoT Security Simplified · Entrust Datacard Trusted Identities | Secure Transactions · exceet SECURE SOLUTIONS · HID

IDENTOS · Microsoft · neXus · PrimeKey

redhat · SAFELAYER · TRUSTONIC