nCipher
AN ENTRUST DATACARD COMPANY

www.ncipher.com

Deploy and maintain secured identity management solutions with nCipher services and hardware security modules

- Protect identity of individuals and device
- Develop the right process and procedures
- Assess health of existing PKI deployments
- Migrate PKIs to meet expanding demands
- Facilitate security auditing and compliance

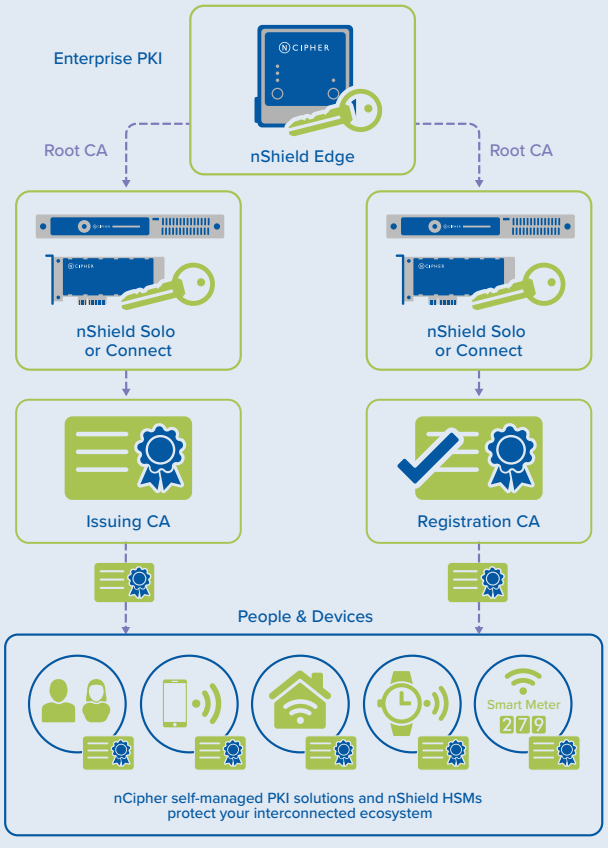
nCipher delivers self-managed PKI solutions to address enterprise-specific security needs

THE PROBLEM: GROWING ADOPTION OF INTERCONNECTED TECHNOLOGIES IS STRETCHING CAPABILITIES OF EXISTING PUBLIC KEY INFRASTRUCTURES (PKIs) AND DRIVING THE NEED TO STAND-UP NEW ONES.

Growing use of cryptographic-enabled applications and the impact of the Internet of Things (IoT) is creating unprecedented new demands on PKIs. Expanding credentialing requirements and the need to manage how devices and sensors securely connect to close network ecosystems is driving enterprises to reassess the health of their existing PKIs. Paired with changing security standards, enterprises are rethinking their PKI implementation strategies and in some cases redesigning and migrating to new, more robust deployments.

THE CHALLENGE: MAINTAINING A STRONG ROOT OF TRUST ACROSS THE ENTERPRISE PKI THAT FULFILLS THE OPERATIONAL DEMANDS OF MORE SECURITY-SENSITIVE APPLICATIONS.

With more security-sensitive applications using PKIs, the security of underpinning private keys is essential. According to the 2018 Ponemon Institute PKI Trends Study, the top five applications using digital certificates include SSL/TLS for public-facing websites, virtual private networks, public cloud-based applications, email, and device authentication. Digital certificates enable identification of applications and devices and authentication into trusted ecosystems. This requires the protection and management of increasing numbers of private keys in an automated and trusted manner.



nCipher deliver self-managed PKI solutions to address enterprise-specific security needs

THE SOLUTION: NCIPHER SELF-MANAGED PKI OFFERINGS COMBINE CONSULTANCY SERVICES WITH THE RIGHT SECURITY HARDWARE TO ASSIST CUSTOMER FROM REQUIREMENTS DEFINITION TO DEPLOYMENT AND TRAINING.

Enterprise PKI requirements are typically unique depending on their business, their clients, and the applications they support. nCipher self-managed PKI offerings combine technical expertise in the design and implementation of organizational PKIs, with the security hardware necessary to provide a robust root of trust for the system. Services include initial requirements assessment and development of processes and procedures, together with design and implementation of the infrastructure necessary to ensure customers can deploy PKIs that meet current and future requirements. Consultancy can support operational settings needing high availability and redundancy, or laboratory environments to assist customers in developing their own PKI skill sets. For customers deploying PKIs for the first time, offerings include documentation and deployment services combined with supporting security hardware. For customers with existing and growing PKI deployments, offerings include health checks, and migration services, including SHA migration service together with security hardware.

nCipher nShield hardware security modules (HSMs) increase the assurance level of PKI deployments. Designed to protect and manage underpinning private key in a certified isolated environment, nCipher nShield HSMs support PKIs from Microsoft, Red Hat, Entrust, RSA, Safelayer, and Insta using standard cryptographic application programing interfaces (CAPIs).

WHY USE NCIPHER HSMs WITH SELF-MANAGED PKIs

The deployment of more security-critical applications and connected devices is placing increased demand on PKIs, expecting them to not only protect the root certificate authority (CA) private keys of individual and device certificates issued across domains, but also their registration. Organizational PKIs not using HSMs to protect their private keys leave themselves vulnerable to disruption with potential severe consequences. HSMs provide a hardened environment that protects security-critical keys from theft and misuse, and enable their full life cycle management with failover support. Binding certificate issuance to identity checks and approvals using an HSM has been an important lesson learned from CA security compromises. Certified to stringent security standards including FIPS 140-2 Level 3 and Common Criteria EAL 4+, nCipher nShield HSMs:

- Store root CA and enrollment keys in a secure and tamper resistant environment
- Manage administrator access with smart card-based policy and two-factor authentication
- Comply with regulatory requirements for public sector, financial services, and enterprises

NCIPHER — AN ENTRUST DATACARD COMPANY

Simplifying the management of identity credentials across the enterprise, including virtualized environments, nCipher nShield HSMs help organizations meet audit and compliance requirements suchas the Payment Card Industry Data Security Standard (PCI DSS). nCipher HSMs are available in the following models to meet specific customer needs:

- nShield Edge: portable USB-attached HSM for offline root CAs and for developer applications
- nShield Solo / Solo+ / Solo XC: embedded PCI Express high performance HSM for servers
- nShield Connect` / Connect+ / Connect XC: network-attached high performance HSM for data centers

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

Search: nCipherSecurity

nCIPHER
AN ENTRUST DATACARD COMPANY