www.ncipher.com

Device enrollment services and hardware security modules enable secured registration of IoT devices

- Increase integrity of network device certificates
- Enable use of existing PKI to support device registration
- Offer secure storage and management of keys
- Provide FIPS 140-2 level 3 validated key protection
- Facilitate compliance with data security regulations

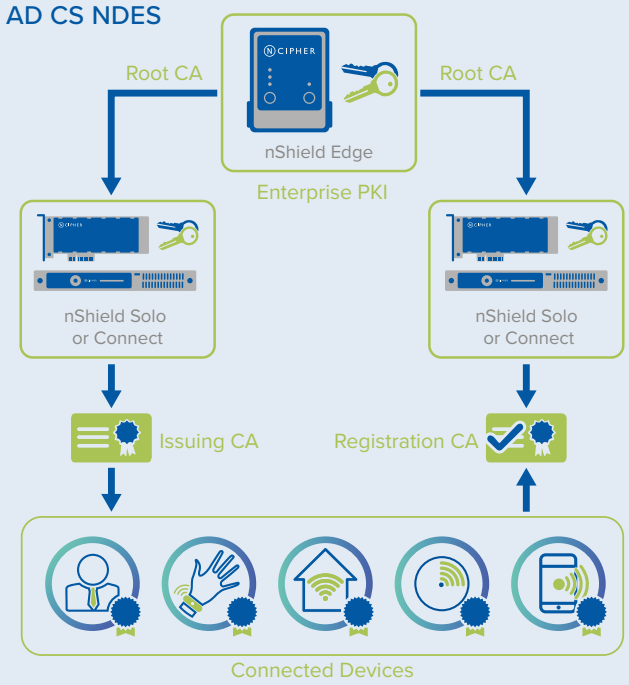
Microsoft and nCipher deliver enhanced security and trust for the Internet of Things

THE PROBLEM: GROWING NUMBER OF INTERNET-CONNECTED NETWORK DEVICES USING DIGITAL CERTIFICATES FOR IDENTIFICATION AND AUTHENTICATION ALSO NEED TO SUPPORT CERTIFICATE ENROLLMENT.

As more devices are connected to the Internet and enterprise networks, their identification and authentication are critically important. Unauthorized devices can create vectors for the introduction of malware into closed domains, posing significant risks. While public key infrastructures (PKIs) are used to issue and manage device credentials for identification and authentication, a trusted registration process must also be in place.

THE CHALLENGE: ENABLING GROWING NUMBER OF CONNECTED DEVICES TO SECURELY ENROLL CERTIFICATES USING TRUSTED DOMAIN-BASED CREDENTIALS.

Issuing device certificates is only the first step in establishing a secure network environment where increasing numbers of authorized devices connect to restricted domains. Enrolling these certificates from a certificate authority (CA) is necessary to validate and control device connections. Safeguarding and managing the cryptographic keys that underpin the registration process is vital for providing a foundation of trust for the entire system.



nCipher nShield HSMs not only protect the enterprise PKI Root and Issuing CA keys but also the private keys used to bind device certificates to the CA root of trust for certificate integrity and validation.

Microsoft and nCipher deliver enhanced security and trust for the Internet of Things

THE SOLUTION: USING MICROSOFT AND NCIPHER TOGETHER CAN ENABLE SECURE ENROLLMENT OF CONNECTED DEVICE CERTIFICATES.

As one of the facilities of Microsoft Active Directory Certificate Services (AD CS), Network Device Enrollment Service (NDES) implements the Simple Certificate Enrollment Protocol (SCEP) to define communication between connected devices and a Registration Authority (RA) for certificate enrollment. Cloud-based and on-premises solutions such as Microsoft Intune and System Configuration Manager, use NDES to provision and enroll devices. NDES enables the enrollment and validation of digital identities of devices connected to Windows Servers by binding them to a corresponding private key. Using a CA as the root of trust, the service enables the enrollment of certificates and the validation of their authenticity and integrity.

When the issuance process is executed on a server using a key stored locally in a file, the key can be subject to attacks that make it vulnerable to duplication, modification, and substitution. nCipher nShield hardware security modules (HSMs) increase the assurance level of the certificate enrollment process by protecting the private NDES key. nCipher nShield HSMs integrate with Microsoft NDES using the Microsoft standard cryptographic application programing interfaces (CAPI).

WHY USE NCIPHER HSMS WITH MICROSOFT NDES?

As more connected devices are deployed to support the growing Internet of Things (IoT), PKIs are expected to not only protect the Root CA private key that underpins the security of certificates issued across the domain, but also the registration of these increasing numbers of certificates. Organizational PKIs not using HSMs to protect their private keys and not employing mechanisms to enroll and validate certificates leave themselves vulnerable to disruption with potential severe consequences. HSMs provide a hardened environment that protects security-critical keys from theft and misuse, and enables their full life cycle management, with failover support where multiple HSMs are used for high availability. Binding certificate issuance to identity checks and approvals using a nCipher nShield HSM, and controlling the enrollment and validation of certificates, have been important lessons learned from CA security compromises.

CERTIFIED TO STRINGENT SECURITY STANDARDS INCLUDING FIPS 140-2 LEVEL 3, NCIPHER NSHIELD HSMS:

- Store the Root CA and the 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

nCipher nShield HSMs have supported AD CS since its Windows Server 2003 release and have been deployed across a wide global customer base. Support of NDES is an extension of this service. Simplifying the management of credentials across multiple applications and PKIs, they can operate in virtualized environments including Hyper-V. nCipher nShield HSMs help organizations meet audit and compliance requirements such as the Payment Card Industry Data Security Standard (PCI DSS) and are available in the following variants:

- nShield Edge: portable USB-attached HSM for offline root CAs
- 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

MICROSOFT

Microsoft has transformed the way business resources are shared and how identities and access controls are managed. Systems based on Microsoft AD CS and NDES provide customized services for creating and managing public key certificates to establish trustworthy business environments between people and devices. Microsoft NDES:

- Provisions and registers device certificates with RA
- Secures enrollment using domain-based credentials
- Enables certificate validation and revocation service

Contact your account representative today or visit www.ncipher.com or www.microsoft.com

Search: nCipherSecurity

www.ncipher.com