THALES

www.thales-esecurity.com

BUILDING TRUST FOR PUBLIC KEY INFRASTRUCTURE (PKI)

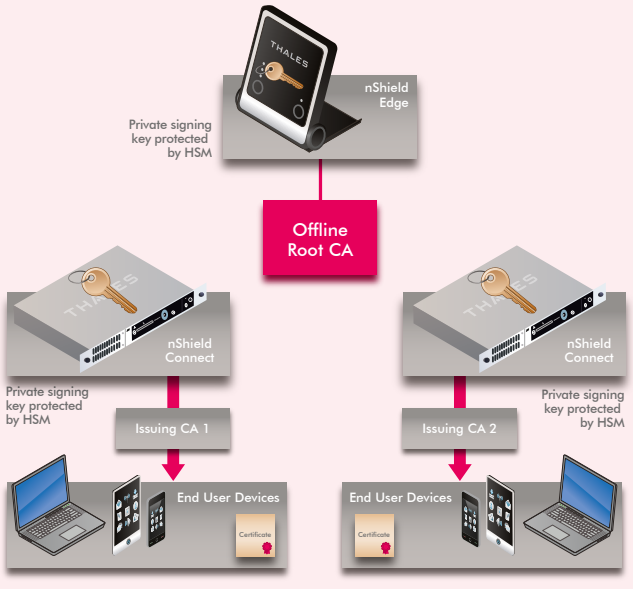
Solution Benefits

- Strengthens Microsoft identity and access solutions
- Extends the security of Windows Server
- Protects transactions and PKI-enabled business applications
- Delivers robust FIPS 140-2 Level 3 validated key protection
- Facilitates compliance with data security regulations

Microsoft

Thales e-Security

Enhanced Security: Thales High Assurance for Microsoft Active Directory Certificate Services



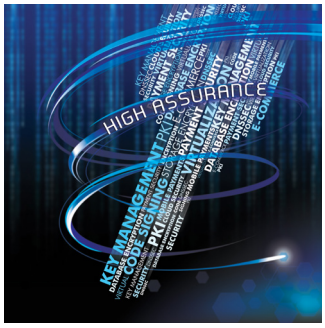
Thales nShield HSMs secure the issuance and validation of identities within Microsoft Active Directory Certificate Services, and establish a root of trust for the entire system.

The Problem: Dependency on an organizational public key infrastructure (PKI) by an increasing number of business applications

As data breaches become increasingly sophisticated, organizations have turned to their public key infrastructures (PKIs) to protect and control access to critical applications and sensitive data. Within a PKI, one or more certificate authorities (CAs) issue electronic credentials to validate online identities and to enforce access controls. Analyzing such aspects as the number of digital certificates being used, the importance and value of the applications they support, and whether these applications are subject to higher levels of scrutiny due to government or industry regulatory compliance are critical factors to ensure that the PKI can meet growing demands.

The Challenge: Building trust for identity and access controls

Protecting the integrity and security of the CA that underpins a system is of critical importance not just for the trust of the PKI, but also for the information it protects. As PKIs increasingly support changing user access topologies including mobile and bring your own device (BYOD) schemes, organizations need to ensure that the private cryptographic keys are protected and managed in a trusted manner.



ENHANCED SECURITY: THALES HIGH ASSURANCE FOR MICROSOFT ACTIVE DIRECTORY CERTIFICATE SERVICES

The Solution: Microsoft and Thales together deliver robust protection of digital identities

Microsoft Active Directory Certificate Services (AD CS) issues, manages and validates the digital identities used to bind persons, devices or services to their corresponding private keys. The validity of each issued certificate depends upon the protection of the CA key issuing the identities. When the issuance process is executed on a server using a key stored locally in a file, that key can be vulnerable to duplication, modification, and substitution. Today, most Windows CAs are used to issue certificates for use within an organization. Internally, certificates are typically used to perform wired and wireless authentication, secure socket layer/transport layer security (SSL/TLS) connections, and virtual private network (VPN) authentication. As expanding applications need the services of a PKI, the demands on the CAs and the need for enhanced security need to be considered.

Thales hardware security modules (HSMs) increase the assurance level of the PKI by protecting the private root and signing CA keys. Thales nShield HSMs safeguard the issuance, management, and validation processes – enabling organizations to strengthen the identity and access solution. Thales nShield HSMs easily integrate with Microsoft AD CS using the Microsoft standard cryptographic application programing interfaces (CAPI) and CAPI next generation (CNG) interfaces. When Thales nShield HSMs are used, all certificate issuance and validation processing occurs within the protected confines of the HSM module. Private root and signing keys are never accessible or in a readable format outside the HSM. Even during backup, archiving, and recovery processes, a Thales nShield HSM ensures that private keys are not susceptible to manipulation and compromise.

Why use Thales HSMs with Microsoft AD CS

Breach identification, recovery, and contingency planning are important steps that can be taken to strengthen the security of a PKI. A hardened, high assurance PKI provides an environment that protects security-critical keys from theft and misuse. Binding certificate issuance to identity checks and approvals using a Thales nShield HSM and controlling the issuance of certificates, have been important lessons learned from CA security compromises.

Certified to stringent security standards including FIPS 140-2 Level 3, Thales nShield HSMs:

- Store keys for signing and issuing digital certificates in 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

Thales

Thales nShield HSMs have supported AD CS since its Windows Server 2003 release. Simplifying the management of credentials across multiple applications and PKIs, they can operate in virtualized environments including Hyper-V. Thales 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: embedded PCI Express HSM for Windows Server
- nShield Connect: a high performance, network-attached HSM

Microsoft

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

- Manage identities across organizations
- Distribute certificates for authentication
- Control user access rights to data resources

For more detailed technical specifications, please visit **www.thales-esecurity.com** or **www.microsoft.com**

Follow us on:

Americas – Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Sunlight Tower, Unit 4101, 248 Queen's Road East, Wanchai, Hong Kong. • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com