SOLUTION BRIEF

SafeNet Luna Hardware Security Solutions for Microsoft Certificate Services
High-assurance PKI root key protection for Microsoft AD CS

The Microsoft Active Directory Certificate Services (MS AD CS) on Windows provides customizable services for creating and managing public key certificates for software security systems employing robust public key infrastructure (PKI). AD CS is a server configured as a certification authority (CA) providing the management features needed to regulate certificate distribution and use.

The heart of trust in a PKI is the CA, and fundamental to this trust is the security of the CA’s root cryptographic signing key which is used to sign the public keys of certificate holders and more importantly its own public key. The compromise of a CA’s root key by malicious intent, inadvertent errors, or system failures can be of catastrophic proportions. Hence, this root-signing key must be diligently protected by using the highest security standards available such as a Hardware Security Module (HSM).

SafeNet Luna HSMs - Integral PKI security
Gemalto’s SafeNet Luna HSMs complement and enhance MS AD CS. Since the function of an HSM is to issue, validate, and store keys and certificates in a protected environment, HSMs make PKIs more secure. The combination of SafeNet Luna HSMs with MS Certificate Services helps meet the best practice security requirements set forth by legal and regulatory compliance bodies. Windows PKI security solutions include smartcard login, secure email, Active Directory access control, and file encryption. The highly secure operational key management provided by SafeNet Luna HSMs includes:

> Hardware-based cryptographic operations, such as random number generation, key generation, digital signatures and encryption
> Centralized key protection, management, and key backup/recovery
> Multi-layered authentication (MofN access) when performing security administration and operational key management
> Load balancing and fail over of operations in hardware modules through the use of multiple HSMs linked together
> FIPS 140-2 and Common Criteria EAL 4+ [AVA_VAN.5] validated cryptographic modules

Benefits
Increased Security:
> High-assurance, hardware cryptographic key protection
> Full key management functionality – keys are never exposed outside of the HSM
> FIPS 140-2 and Common Criteria validated
> Application independent authentication and policy management
> Tamper-resistant physical hardening

Ease of Installation and Management
> Support for CryptoAPI (CAPI) and CNG

Increased Application Performance
> 10,000 RSA 2048 bit and 22,000 ECA signings per second
> Includes native ECC support
> Supports MS Windows Server clustering capability
Ease of Integration

Successful testing by Microsoft reveals Gemalto’s plug-and-play compatibility with MS Certificate Services for Windows Integrated with Windows 2008R2, Windows 2012R2, Windows 2016. Adding hardware-secured key management and digital signing for MS PKI certificate issuance is simple, fast and cost effective. The MS Cryptographic API (CryptoAPI) enables application developers to add cryptography and certificate management functionality to their Windows applications. All cryptographic operations in software are performed by independent modules known as a cryptographic service provider (CSP).

The Windows Server PKI uses the CSP and CNG [cryptographic next gen provider] interface to allow the connection of third party HSMs into MS Certificate Services. Thus MS Certificate Services is enhanced with Gemalto’s security, speed, flexibility, and scalability with no impact on the application.

The SafeNet Luna Network and SafeNet Luna PCIe HSMs offer users of MS Certificate Services two flexible encryption options for their deployment scenarios:

- SafeNet Luna Network HSM is a network-attached HSM that connects to the server through TCP/IP. It can be leveraged by many servers, offering the ability to securely partition and share the HSM resource, and is a cost-effective way of extending the application.

- The SafeNet Luna PCIe HSM is a PCIe-card form factor HSM that connects to the server in the PCI bus and provides seamless deployment to a wide range of security applications. Its full cryptographic application program interface support makes integration quick and easy.

The ease of integration is complemented by the SafeNet Integration Guide Luna Network and Microsoft Active Directory Certificate Services. To access the guide visit https://safenet.gemalto.com/partners/microsoft/.

About SafeNet Luna Network HSM

SafeNet Luna Network HSM is a flexible, high-assurance and high-performance network-attached HSM providing up to 22,000 ECC and 10,000 RSA signings per second and hardware protected key management where security, strong administrative controls and performance are a top priority.

- Keys always remain in high-assurance, tamper-evident hardware
- Logical partitioning of up to 100 individual user object spaces (partitions) each providing their own unique access control and policy settings
- Meet compliance and audit needs with a FIPS 140-2 Level 2, Level 3, and Common Criteria EAL 4+ [AVA_VAN.5] validated cryptographic modules

Together we can help

To learn more about how the combination of SafeNet Luna HSMs with MS Certificate Services can help you secure your PKI and exceed best practice security requirements, visit the Gemalto website or contact us at info@gemalto.com.