cpl.thalesgroup.com

THALES
Building a future we can all trust

Thales Luna HSMs 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.

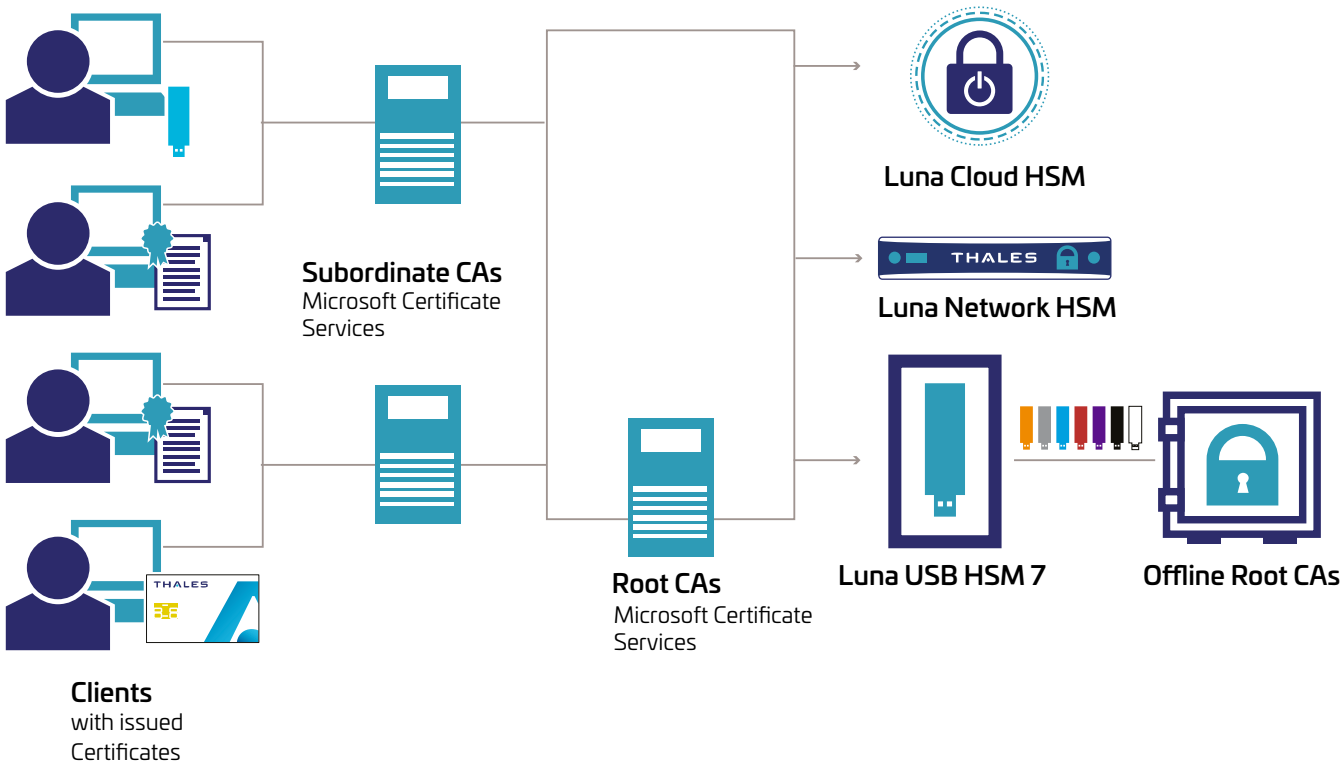
The heart of trust in a PKI is the CA, and fundamental to this trust is the security of the CA's root cryptographic signing key which is used to sign the public keys of certificate holders and more importantly its own public key. The compromise of a CA's root key by malicious intent, inadvertent errors, 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).

Luna HSMs - Integral PKI Security

Thales 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 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 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
- 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
- Flexible Deployment Options: Luna HSMs can be deployed either in the cloud, on-premises, hybrid or multi-cloud environments

PKI Root Key Protection



Benefits

Increased Security:

- High-assurance, hardware cryptographic key protection
- Full key management functionality – keys are never exposed outside of the HSM
- FIPS 140-2 Level 3 and Common Criteria validated
- Application independent authentication and policy management
- Tamper-resistant physical hardening

Ease of Installation and Management

- Integrated with Windows 2008R2, Windows 2012R2, Windows 2016
- Support for CryptoAPI (CAPI) and CNG

Increased Application Performance

- Includes native ECC support
- Supports MS Windows Server clustering capability

Ease of Integration

Successful testing by Microsoft reveals Thales'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 Thales's security, speed, flexibility, and scalability with no impact on the application.

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

- **Luna Network HSMs:** Secure sensitive data and critical applications by storing, protecting and managing cryptographic keys in Luna Network HSMs - high-assurance, tamper-resistant, FIPS 140-2 Level 3 certified network attached appliances offering market-leading performance.
- **Luna Cloud HSM:** Available from the Thales Data Protection on Demand (DPoD) Cloud HSM service, offers an as a service billing model without hardware to deploy and maintain.

About Luna HSM

Luna HSMs are a flexible, high-assurance and high-performance HSM 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 Luna HSMs with MS Certificate Services can help you secure your PKI and exceed best practice security requirements, visit the Thales website.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us