Trusted Cyber Technologies

THALES
Building a future we can all trust

Thales TCT Luna Hardware Security Solutionsfor 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.

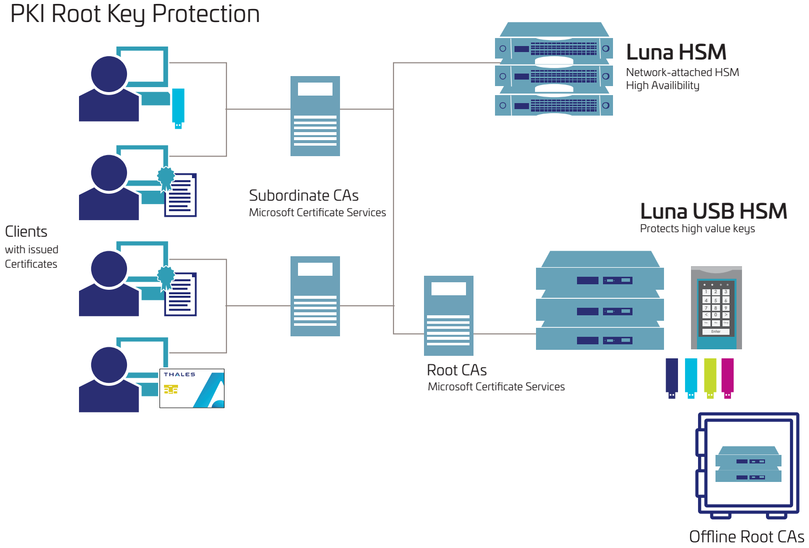
The heart of trust in a PKI is the CA, and fundamental to this trust is the security of the CA's root cryptographic signing key which is used to sign the public keys of certificate holders and more importantly its own public key. The compromise of a CA's root key by malicious intent, inadvertent errors, 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 Trusted Cyber Technologies (TCT) Luna T-Series 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
- 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 Level 3 validated cryptographic modules

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 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
- 10,000 RSA 2048 bit and 20,000 ECA signings per second
- 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 T-Series Network and Luna T-Series PCIe HSMs offer users of MS Certificate Services two flexible encryption options for their deployment scenarios:

- 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 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.

About Luna T-Series HSMs

Luna T-Series HSMs are the choice for government agencies when storing, protecting and managing cryptographic keys used to secure sensitive data and critical applications. Meeting government mandates for U.S. Supply Chain, the high-assurance, tamper-resistant Luna T-Series HSMs are designed, developed, manufactured, sold, and supported in the United States.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

For more information, visit www.thalestct.com