securosys

Primus HSM – The Hardware Security Module

Securing Microsoft PKI Deployment based on Microsoft Active Directory Certificate Services (AD CS)

Introduction

Microsoft Active Directory Certificate Services (AD CS) provide customizable services for creating and managing public key infrastructure (PKI) certificates, used in software security systems. Applications supported by AD CS include secure e-mail (S/MIME), secure wireless networks, VPN connections (IPsec), Encrypting File System (EFS), smart card logon, Secure Socket Layer/Transport Layer Security (SSL/TLS), and digital signatures.

AD CS is a certificate authority (CA) that issues, manages, and validates the digital identities used to verify an individual or a system. The trust of the entire system and validity of each issued certificate depends upon the protection of the CA key issuing the identities. In case the issuance process is using private keys stored in a local file, these keys are vulnerable to duplication and modification. Therefore, Microsoft best practices recommend storing private keys on a HSM.

The MS Cryptography Next Generation (CNG) API supports Cryptographic Algorithm Providers and Key Storage Providers (KSP) in software and hardware. This allows anybody to create and handle private keys and related cryptographic functions on Hardware Security Modules, thereby fulfilling new compliance requirements (e.g. GDPR).

Primus HSM – Boosting Microsoft PKI Security

The Primus Hardware Security Modules (HSMs) from Securosys improve drastically the security of Microsoft Active Directory services, and all applications based on Microsoft CNG API. The Primus HSMs are built to securely generate and store true random cryptographic keys, providing a central, certified secure storage. They also control and regulate access to the keys and the related cryptographic functionality. The Primus HSM combined with AD CS meets or exceeds the best practice security requirements and is one step ahead of fulfilling your compliance demands by providing:

- Hardware-based secure generation of true random cryptographic keys
- Central and highly secure storage of cryptographic keys
- Load balancing and fail-over by clustering the HSMs
- Controlled and regulated access to the keys
- Hardware acceleration of cryptographic operations such as encryption, authentication, and digital signatures, relieving the host server of processor intensive computations
- Scalable performance at manageable cost

All certificate issuance and validation processes occur within the protected confines of the HSM. Private keys are never accessible outside the HSM.

Microsoft Partner

Benefits

Increased Security

- Keys are never exposed outside of the HSM
- Tamper protection during transport, storage and operation
- Two high entropy hardware true random number generators
- Highest availability
- Designed, developed and manufactured in Switzerland

Simple Integration

- Via CNG Provider
- Simple setup, configuration and maintenance
- Windows Server 2016, 2012, 2008R2, Client 10, 7
- Scalable and flexible partitionable

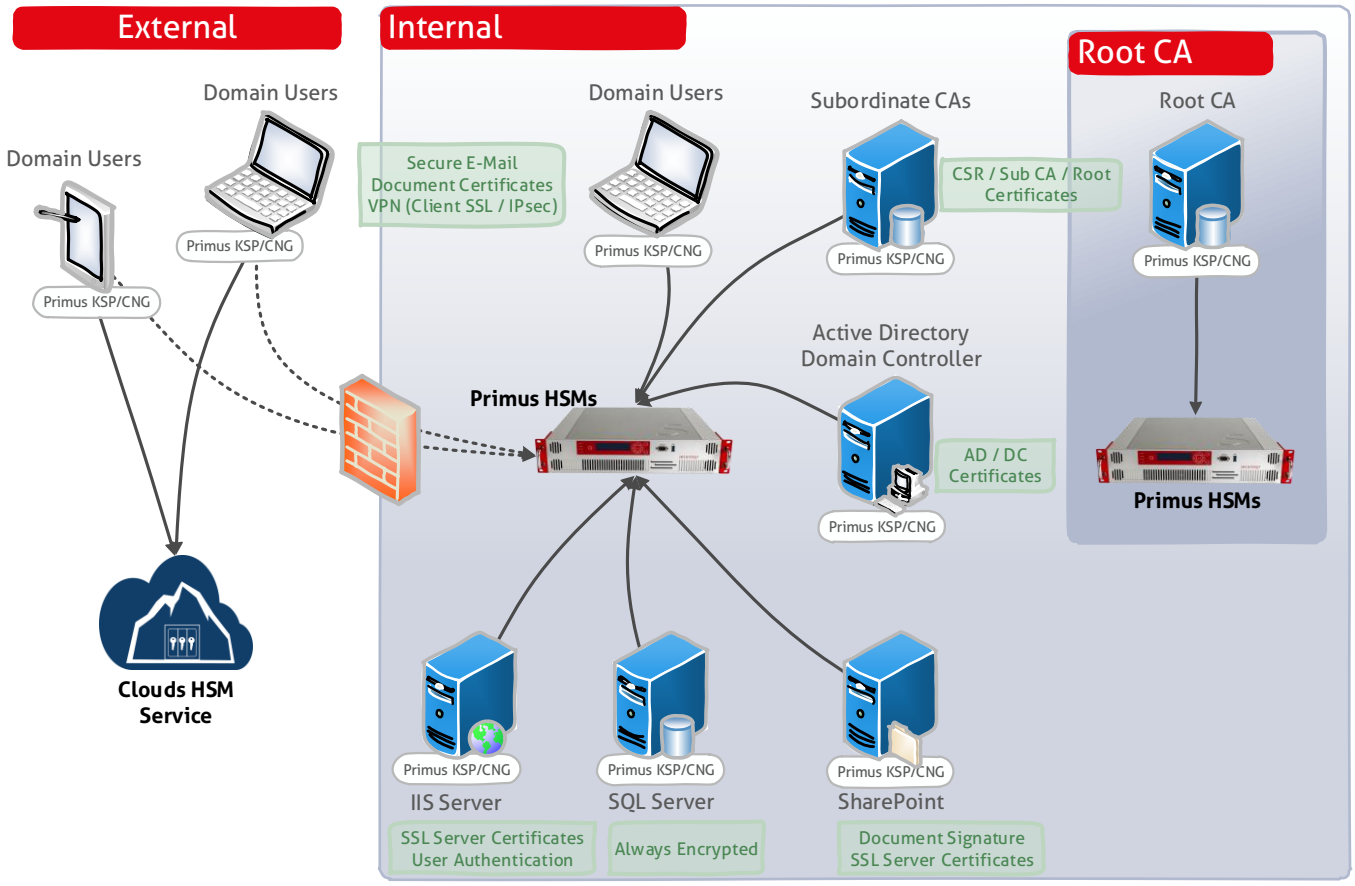
Application Performance

- Hardware accelerated digital signing, up to 4000 RSA 2048-bit signings/s per HSM
- Handling of larger key sizes or numbers without severe performance penalty

securosys

Simple Integration of Primus HSM

The Primus HSM can easily be integrated in a MS system by installing the Primus CNG Provider.
This enables all Windows servers and clients to generate and store their private keys and certificates securely in the HSMs, and perform all related cryptographic functionality, like signing or certificate validation, hardware accelerated on the Primus HSM.



The Root CA generates and stores the root private/public key securely on the Primus HSM and issues the certificates for the Subordinate CAs.

Subordinate CAs initially generate and store their private/public keys securely on the Primus HSMs and generate a Certificate Signing Request (CSR) to be signed by the Root CA. The Sub-CAs provide CSR templates for different purposes via the Active Directory and handle all CSRs to issue the necessary certificates for different applications:

- Approve and authorize applications with Code Signing (e.g. MS SignTool)
- Network access control with 802.1x authentication
- Protect user data with Encrypting Files System (EFS)
- Protect LDAP-based directory queries (Secure LDAP)
- Implement Secure E-Mail (S/MIME, signed/encrypted)
- Secure network traffic (IPsec)
- Protect traffic to internal web-sites with SSL/TLS
- MS SQL Server 2016 Always Encrypted, column encryption, protecting application data-at-rest and in-motion
- Handling of digitally signed documents

We recommend to setup the Primus HSMs redundant (local/geo redundant).

The Securosys "Clouds HSM" service (HSM as a Service) facilitates a fast and smooth implementation, supports external domain users and backup scenarios.

About Securosys Primus HSM Series

- Scalable and flexible solution
  - X-Series (enterprise grade)
  - E-Series (SMB solution)
  - Clouds HSM (as a service)
- Secure Remote Control with Decanus
- Multi-tenancy, up to 120 partitions, each 240MB
- Strict authentication, 4 eyes principle, 2 factor authentication
- Clustering, secure real-time synchronization across data centers without external control
- Constant tamper protection
- Designed, developed, and manufactured in Switzerland