Microsoft AD CS

Integration and Functionality Overview

Enterprise Certificate Management Backed by Industry-Leading HSMs

A Customizable, Hardware-Secured Solution

Microsoft Active Directory Certificate Services (AD CS), through a server that acts as a certificate authority (CA), manages certificates distributed to users, devices, and other endpoint clients as part of a Public Key Infrastructure (PKI). When the private keys used for signing these endpoint clients are stored in software, an elevated risk of compromise is introduced. By using Futurex's FIPS 140-2 Level 3 validated hardware security modules to store these private keys and perform signing operations, security can be significantly enhanced while also expediting the process of onboarding new clients.

With a certificate authority created by Microsoft AD CS, third-party identities can be verified upon receipt of a digitally signed message. Since the CA continues to manage every aspect of the certificate lifecycle, including issuance and revocation, using a compliant hardware security module is essential to establishing a secure, trusted environment.

Security with Convenience

Microsoft AD CS is strengthened by integrating with a Futurex HSM, such as the Excrypt Series. These devices operate at industry-leading throughput rates and are compliant with the most rigorous security requirements, including FIPS 140-2 Level 3 validated physical security.

Incorporating hardware-backed security to an existing infrastructure is easy, requiring minimal resource and time commitments. The integration is accomplished using Microsoft CNG and requires no additional development, and separate root private keys can be logically segregated to fulfill information security best practices.

Core Features At-A-Glance

- Full Encryption Key Lifecycle Management
- Turnkey Deployment and Seamless Enhancement
- Virtually Limitless Scalability of Signing Operations
- Enterprise-Grade Security for Private Keys

Cloud-Based Scalability and Functionality

- The VirtuCrypt Hardened Enterprise Security Cloud offers scalability and disaster recovery, proof of concept testing, or hosting of an entire cryptographic infrastructure

Xceptional Support

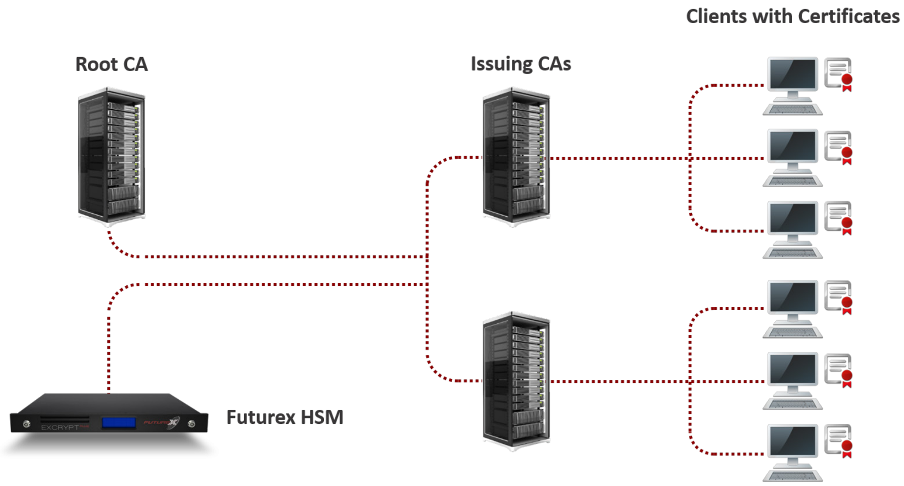
- 24x7x365 support available from industry-certified Solutions Architects
- 100% project success rate for custom initiatives

Product Overview: Vectera Series

PKI Solution Hierarchy

The diagram to the right represents a two-tier hierarchy as a proposed PKI solution. The CAs depicted here are supported by Microsoft Active Directory Certificate Services and the hardware security module is a network-attached Futurex device.

This example of a possible solution provides opportunities for different security levels and geographic locations due to the dispersed nature of the CAs.



Supported Key Types and Protocols

- 3DES
- AES (128-256)
- DSA (512-4096)
- HMAC (MD5, SHA-1, SHA 256-512)
- ECC (NIST recommended and user defined)
- RSA (512-8192)
- SHA-1
- SHA-2 (256-512)

Excrypt Manager GUI

- Full graphical user interface (GUI) makes configuration simple and easy
- No command line interface required for installation and initial setup
- Scalable architecture, with the ability to increase processing throughput rates without removing the unit from a production environment

Reporting and Audit Logging

- Automatically transmit data logs to a remote server for internal and external audits
- Digitally sign log files, ensuring that data integrity is maintained and that logs cannot be altered
- Remotely access internal logs via the Futurex HSM's web-based management interface

FUTUREX.COM

ENGINEERING CAMPUS / 864 OLD BOERNE ROAD, BULVERDE, TEXAS 78163 USA
TF/ (800) 251-5112 P/ +1 (830) 980-9782 INFO@FUTUREX.COM

Product Specifications

Industry Compliance Standards

- Compliant with FIPS 140-2 Level 3
- ANSI/ISO
- PCI HSM

Futurex HSM - Front View

Futurex HSM - Back View

Limitless Expansion

Increase your infrastructure's throughput capacity at any time.

Cryptographic Interfaces

- Excrypt API
- PKCS #11
- JCA/JCE
- MS CAPI/CNG

Web Browser Based Administration Tool

- Upgrade firmware
- Update network settings
- Execute secure application code
- Alter host software application parameters
- Adjust syslog levels
- Alter TLS settings

Integrate The Excrypt Touch

Combine Futurex HSMs and the Excrypt Touch for remote access and centralized management of keys.

General-Purpose and Financial Processing

Futurex HSMs offer both general purpose and financial processing cryptographic functionalities, allowing organizations to conduct both types of tasks within a single Secure Cryptographic Device. This ability provides unparalleled versatility and applicability.