This is a joint nCipher and IdentIT authored whitepaper

Microsoft Windows Server 2008 PKI and Deploying the nCipher Hardware Security Module

Abstract

This paper discusses the benefits that are unique to deploying the integrated solution of the Windows Server 2008 PKI and the nCipher nShield and netHSM hardware security modules (HSM). This includes the essential concepts and technologies used to deploy a PKI and the best practice security and life cycle key management features provided by nCipher HSMs..

Introduction

The modern corporation is using web based infrastructures in many ways to conduct business across the enterprise and around the globe. Whether it is with customers, partners or employees, the Internet provides instant access and global reach at a fraction of the cost of traditional channels. However, doing business via the Internet presents unique security challenges such as ensuring privacy, confirming identity, managing authorization and legitimizing business transactions. To address these issues, governments have enacted far-reaching privacy legislation and industries are mandating a growing list of new security requirements (GLBA, Sarbanes-Oxley, HIPAA, FDA 21 CFR Part 11, EU Data Privacy, EU Electronic Signature, etc.). Increasingly, there is a need for web based solutions that provide instant global access, yet also provide security and privacy in a cost effective manner.

PKI – A Crucial Component to Securing e-commerce

A Public Key Infrastructure (PKI) is an integral component of most web based business environments. A PKI provides the foundation for authenticating users by issuing each user with a unique credential – a digital certificate. This is used to identify a user on applications such as emails, web servers, single sign-on applications and databases. However, while PKI is recognized for its security features, it has traditionally been seen as complicated and expensive to deploy. Often organizations were reluctant to deploy a PKI due to concerns about cost and management. Both Windows Server 2008 PKI and its predecessor Windows Server 2003 PKI have addressed these concerns, allowing organizations to deploy cost effective PKI solutions that are easily managed using Microsoft® tools.

Microsoft Windows Server 2008

Windows Server 2008 PKI solution combines easy to install security functionality with a reduced total cost of ownership (TCO). As with the Microsoft Windows Server 2000 and Microsoft Windows Server 2003, the Microsoft Windows Server 2008 PKI is included with the operating system (OS) at no additional charge. It includes all the PKI components, such as a Certificate Authority (CA), Active Directory (AD) and Cryptographic Service Providers (CSP), to enable the deployment of enterprise wide PKI solutions.

Windows Server 2008 changes the installation and configuration of Active Directory Certificate Services by introducing management roles. The Windows Server 2008 AD CS role includes Certification Authority, Certification Authority Web Enrollment, Online Certificate Status Protocol, and Network Device Enrollment Service.

nCipher Hardware Security Modules

Using nCipher Hardware Security Modules (HSMs) to secure the private keys of the Microsoft Windows Server 2008 CA adds many benefits to a Windows Server 2008 PKI installation including: secure key generation, hardware key protection, key life cycle management, support for Cryptography Next Generation (CNG) algorithms, the ability to map user key security policy to the HSM, and improved performance for high volume CAs. The combination of nCipher HSMs with Microsoft Windows Server 2008 PKI meets or exceeds the best practice security requirements set forth by numerous legal and regulatory requirements.

This white paper provides a unique overview of the Windows Server 2008 PKI and the nCipher nShield or netHSM HSM integrated solution, and is complemented by two recommended papers: (1) the Microsoft white paper, Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure; (2) the nCipher Integration Guide (how to install an nCipher module), Microsoft Certificate Services and nCipher Modules.

Details of deployment planning for Windows Server 2008 PKI is available in Brian Komar's Windows Server® 2008 PKI and Certificate Security book by Microsoft Press.

Best Practice Security – nCipher HSMs with Windows Server 2008 PKI

Overview

Best practice security in an e-business environment is a combination of hardware, software policies, practices and procedures. Each is a building block to a secure web based environment. As highlighted in this white paper, cryptography and the secure administration and distribution of the cryptographic keys is a critical component of "best practice" security – so important, that laws and industry standards have been created specifically to address the need to secure cryptographic keys. This section identifies the best practice standards, laws and specific industry requirements.

Hardware vs. Software

It is well understood that with software-based cryptography, all the cryptographic components on the host are vulnerable to attack, where they are susceptible to duplication, modification or substitution. Hardware based cryptography protects the private keys by only ever exposing them as plain text within the secure confines of a tamper-resistant HSM. By using a FIPS 140-2 Level 3 validated module, users can be assured cryptographic keys are protected from misuse. The nCipher nShield and netHSM HSMs take this security concept further:

- Security and Flexibility: nCipher HSMs combine FIPS 140-2 Level 3 validated key management hardware and software to manage the cryptographic keys. The solution allows an organization to take advantage of best practice security and scalability within a unified system.
- Split key management responsibility: nCipher's Security World allows for physically splitting key management responsibilities. Split responsibility is a widely accepted control within most security policies. Through its multi-party "k-of-n" control functionality, important key functions, procedures or operations can mandate that more than one person is required to perform these tasks. Instead, a quorum of key holders (the "k" in the "k-of-n") must authorize the actions of the console operator.
- Remote key management: nCipher's Remote Operator feature provides users with the ability to present their operator credentials to a single nCipher nShield and authorize key usage at any number of remote or unattended modules. This allows users to manage their modules in remote locations without delegating authority that could result in a compromise of the overall solution.

Statutory and Regulatory Requirements

Lost, stolen or compromised data can have a significant impact on an organization which stands to lose customers, revenue and brand equity. But the need to protect sensitive data has also become a business issue because laws and industry regulations are providing substantial penalties associated with compromised user information. Failing to keep sensitive information secure can lead to expensive

lawsuits, and perhaps more importantly, it can place companies in violation of high-profile legislation. Governments around the world now require organizations to establish strong policies, adopt best practices and take legal responsibility for keeping personal data safe or face potentially hefty fines. The following laws have been enacted which require private information to be secured:

- COPPA – U.S. Children Online Privacy Protection Act
- E-SIGN – U.S. Electronic Signatures in Global and National Commerce
- GISRA – U.S. Government Information Security Reform Act
- GLBA – U.S. Gramm-Leach-Bliley Act
- HIPAA – U.S. Health Insurance Portability and Accountability Act
- California State Bill SB 1386
- Sarbanes-Oxley
- EU Data Privacy
- EU Electronic Signature

While legislation has forced companies to be proactive about security and privacy, industry standards have been providing vital best practice benchmarks for years.

Many of these standards have expanded beyond their original sector-focused origins to become de facto standards for industry as a whole, or as the foundation for standards in other countries. Some standards are providing vital guidelines in areas where none previously existed. Many others are currently in development by organizations such as the Center for Internet Security and the National Institute of Standards and Technology. In every case, leveraging these highly specific standards can help companies in their mission to comply with legislation that lacks implementation specifications. At the same time, adopting industry standards is essential to establishing prudent best practices and in turn, protecting against lawsuits. The following industry standards require private information to be secured:

- Payment Card Industry – Data Security Standard (PCI-DSS)
- Verified by Visa
- Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)
- ISO 17799, Code of practice for information security management
- U.S. FDA 21 CFR Part 11, Electronic Records; Electronic Signatures
- ISO 11568, Banking – Key Management (Retail)
- ISO 15782, Banking – Certificate Management
- AICPA.CICA, Web Trust Program for Certificate Authorities
- American National Standards Institute X9.57, Public Key Cryptography for the Financial Services Industry: Certificate Management
- American National Standards Institute X9.79, Public Key Infrastructure (PKI) Practices and Policy Framework

Windows Server 2008 PKI

Overview

Windows Server 2008 provides the complete infrastructure for an enterprise wanting to deploy a PKI. The Microsoft PKI is scalable and customizable, readily able to support both the smallest and the largest of PKI deployments. It is easy to install and administer, and the infrastructure is provided as part of the operating system. Unlike other competing PKI products, and regardless of the PKI deployment size, there is no charge per certificate.

The Windows Server 2008 PKI provides the strong authentication component of Microsoft's Identity and Access solutions. Many Microsoft and PKI-aware applications can leverage the Microsoft PKI to provide:

- **Digital signing**. The .NET security framework permits organizations to extend the use of their PKI through digital signing of the application code to ensure application integrity. Signing certificates can also be used to sign Microsoft Office documents, Adobe PDF files, or S/MIME E-mail messages.
- **Authentication certificates**. The Certificate Enrollment wizard permits acquisition of either software-based or two-factor device-based certificates for authentication purposes. The certificates may be used to authenticate to virtual private networks (VPNs), Web portals, or to Active Directory Domain Services (AD DS).
- **Encryption certificates**. Encrypting File System (EFS) and S/MIME E-mail encryption prevent inspection of data by unauthorized users.
- **Two factor authentication**. The Windows Server 2008 CA in conjunction with the Windows Vista Certificate Enrollment Wizard can issue smart card certificates for two factor authentication solutions.

Windows Server 2008 Active Directory Certificate Services Role Services

The Windows Server 2008 Active Directory Certificate Services (AD CS) is comprised of four core role services. In previous versions of the Windows PKI, only the certification authority and the Web enrollment pages were included in the base operating system. Other components were available through add-ons or included in the Windows Server Resource Kits.

The core role services of AD CS are:

- **Certification Authority**. The certification authority (CA) issues and manages certificates in a Windows Server 2008 PKI.
- **Certification Authority Web Enrollment**. The Web enrollment pages provide a simple Web interface to allow users to request and renew certificate, download certificate revocation lists (CRLs), and to download CA certificates.
- **Online Responder**. The Online Responder provides the ability to deploy Online Certificate Status Protocol (OCSP) for revocation checking in a Windows Server 2008 PKI.

- **Network Device Enrollment Services (NDES)**. The NDES role service allows you to issue and manage certificates for routers and network devices that support Cisco's Simple Certificate Enrollment Protocol (SCEP).

Active Directory Domain Services

Active Directory Domain Services (AD DS) is the (LDAP based) directory service for the Windows Server family of operating systems. AD DS stores information about objects on the network, and makes this information simple for administrators, users and services to find and use. Active Directory uses a structured data store as the basis for a logical, hierarchical organization of directory information. It is a core component in any Certificate Services CA deployment, providing an X.509 certificate store and authentication/identity related information for users and services, including certificate templates.

The following components in Active Directory facilitate management of the Windows Server 2008 PKI:

- **CRL fault tolerance**. The Active Directory forest provides for the distribution of CRLs and delta CRLs to all domain controllers, allowing distributed access to revocation information.
- **CA certificate storage**. The CA certificates in the certificate chain are stored in Active Directory to allow all forest-joined computers to trust and utilize certificates issued by the CA hierarchy.
- **Enhanced client cross-certification**. This feature is enhanced by enabling the capability for department-level and global-level cross certifications. More information is available in the Microsoft paper "Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003".
- **Credential Roaming Services**. User software certificates can "roam" between client computers, reducing the issuance of duplicate certificates to users that work at more than one computer.
- **Encryption certificate storage**. Active Directory acts as a publication point for encryption certificates to allow sending of S/MIME encrypted email and sharing EFS encrypted files.

What's New in Certificate Services for Windows Server 2008

The Active Directory Certificate Services in Windows Server 2008 includes all of the new features included in Windows Server 2003 Certificate Services. In addition, the following new features have been added:

- **Cryptography Next Generation (CNG)**. Cryptography Next Generation is a replacement cryptography API for the original Windows CryptoAPI. The new APIs will allow the use of newer, stronger encryption and signing algorithms when implementing cryptography. The most recognized feature of CNG will be the implementation of National Security Agency Suite B algorithms, providing enhanced standards for symmetric encryption, key exchange, digital signatures and hash algorithms.

- **Online Certificate Status Protocol (OCSP)**. Online Certificate Status Protocol allows clients to receive immediate revocation status for a specific certificate by sending a revocation status request to a designated OCSP responder. The OCSP responder responds with the status of the requested certificate by inspecting the latest base CRL or delta CRL published by the associated CA. OCSP provides more up-to-date revocation information than the standard practice of certificate revocation lists (CRLs). The Windows Server 2008 OCSP responder works with both Windows CAs and non-Windows CAs. Windows Vista and Windows Server 2008 include a built-in OCSP client.
- **Network Device Enrollment Services (NDES)**. Windows Server 2008 implements Cisco System's Simple Certificate Enrollment Protocol (SCEP) as a standard component of the operating system. NDES allows network devices that support SCEP to request certificates automatically from a Windows Server 2008 CA without having a computer account in Active Directory.
- **Version 3 Certificate Templates**. Windows Server 2008 provides further customization options for certificate templates in the new version 3 certificate templates. Version 3 certificate templates allow you to implement CNG algorithms within certificates based on the version 3 certificate template.
- **Detailed Enrollment Agent delegation**. The Windows Server 2008 CA allows you to limit designated enrollment agents to only issuing smart cards based on specific certificate templates. In addition, you can limit which users and groups can receive smart cards based on the designated certificate templates.
- **Detailed Certificate Manager restrictions**. The Windows Server 2008 CA allows you to better restrict certificate managers. Where previously you could only limit certificate managers to managing certificates to specific groups, Windows Server 2008 allows you to define the combination of groups and certificate templates. For example, consider the configuration for certificate manager restrictions shown in Figure 1.

In this example, the EFS Managers group can only manage certificates that are based on the Archive EFS certificate

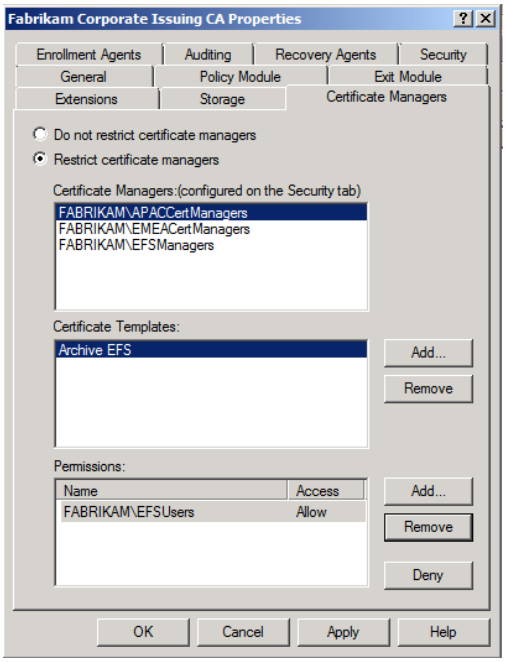

FIGURE 1

Implementing certificate manager restrictions in Windows 2008

template. In addition, the certificates can only be managed if they are issued to members of the EFS Users group.

Hardware Security Modules

An HSM is a hardware encryption device that is physically or logically connected to a server via a PCI or PCI-X interface or over a network connection. The function of an HSM is to provide highly secure operational key management, this includes:

- Hardware based cryptographic operations, such as random number generation, key generation, digital signatures and encryption.
- Hardware key protection and management, with centralized key backup/recovery.
- Multi-layered authentication capabilities (e.g., "k-of-n" access) when performing security administration and operational key management.
- Acceleration of cryptographic operations, relieving the host server of highly processor intensive cryptographic calculations used in Secure Sockets Layer (SSL) and other protocols.
- Load balancing and fail-over of operations in hardware modules through the use of multiple HSM modules linked together.
- FIPS 140-2 Level 3 certification.

From an application standpoint, the interface to the HSM can be through the Microsoft CryptoAPI interface or the new Microsoft CNG interface.

HSM Form Factors

nCipher HSMs are available in two form factors: dedicated and network attached.

- The dedicated nCipher HSM (the nShield) is attached to the CA computer through the PCI, PCI-E, or PCI-X bus of the computer. All communications are directly through the hardware bus and the private key material never leaves the protective space of the HSM un-encrypted.
- The network-attached nCipher HSM (the netHSM) is connected to the CA through either a private or corporate network. The client securely connects to the netHSM by using the inter-module path protocol. This protocol ensures that all data transmitted between the client and the netHSM is protected.

Both form factors of the nCipher HSMs are FIPS 140-2 level 3 rated and can be used together in the same nCipher Security World key management framework.

How Hardware Security Modules Integrate with Microsoft Windows Server 2008

nCipher HSMs can integrate with two of the Active Directory Certificate Services Role Services: the Certification Authority and the Online Responder. The following sections illustrate common models for integrating nCipher HSMs with each of the role services. When the HSMs are integrated with Active Directory Certificate Services, the two principle interfaces used for communication between the nCipher HSM and Microsoft PKI are the CryptoAPI or CNG.

Integration with Active Directory Certificate Services Role Services

nCipher HSMs can be used to protect private key material for:

- Certification Authorities
- Online Responders

Integration with the Certification Authorities

There are three typical integration scenarios for integrating nCipher HSMs with Windows Server 2008 Certification Authorities:

- Deploying nCipher nShield HSMs at each CA in the CA hierarchy.
- Connecting all CAs in the CA hierarchy to an nCipher netHSM.
- Deploying nCipher nShield HSMs for offline CAs and sharing a netHSM between online CAs.

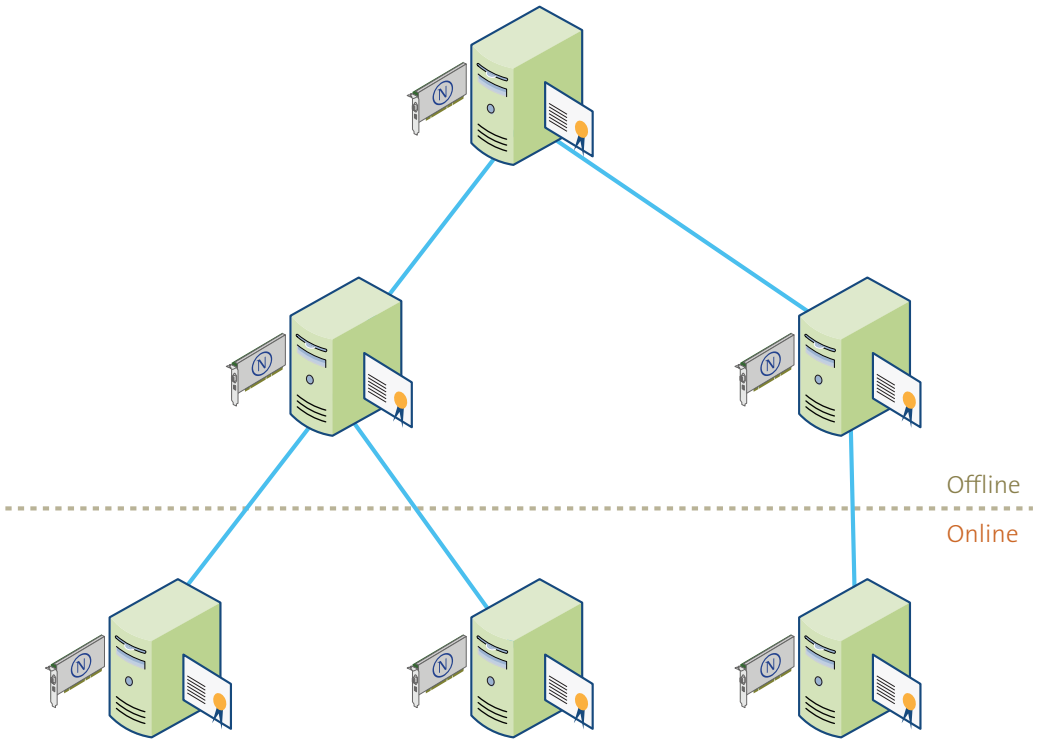

FIGURE 2

Implementing nShield HSMs at each CA in the CA hierarchy

Deploying nCipher nShield HSMs for each CA in the CA Hierarchy

In this model, as shown in Figure 2, each CA is deployed with an nShield HSM. Each nShield HSM is dedicated to protecting the private key material of the local CA.

This model ensures that:

- Each CA has its own dedicated HSM.
- Network connectivity is not required for the offline CAs.

Deploying an nCipher netHSM for all CAs in the CA Hierarchy

In this model (shown in Figure 3), all CAs connect to a netHSM. To prevent the offline CAs from being exposed to the corporate network, the offline CAs are connected to the secondary network port on the netHSM through a private network. Note that a netHSM can support virtualized CA deployments.

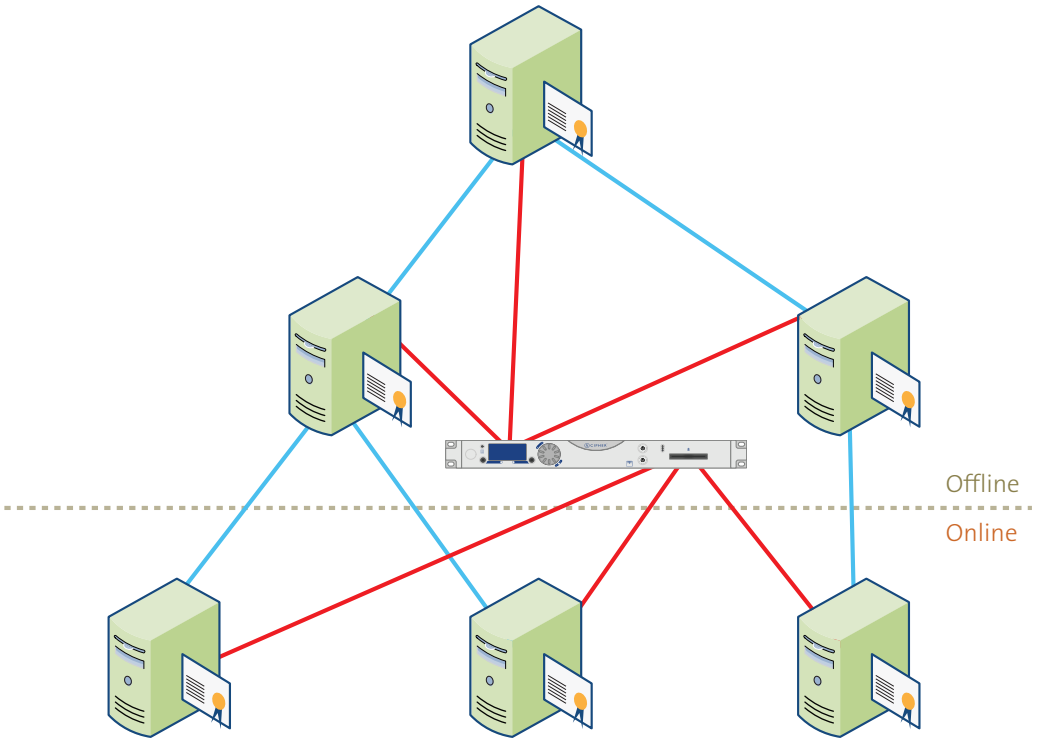

FIGURE 3

Implementing nShield HSMs at all CA in the CA hierarchy

This model:

- Reduces HSM deployment costs.
- Provides support for up to a maximum of 20 clients.
- Can have increased client security by implementing nCipher nToken cards at each client; the nToken cards provide strong cryptographic identification of a client endpoint.
- Supports virtualized CAs (without the benefits of an nToken card).

Deploying a mix of nShields and netHSMs

This model (shown in Figure 4), combines the best protection for each type of CA. Offline CAs are protected by dedicated nShield HSMs. The online issuing CAs share a common netHSM for key protection.

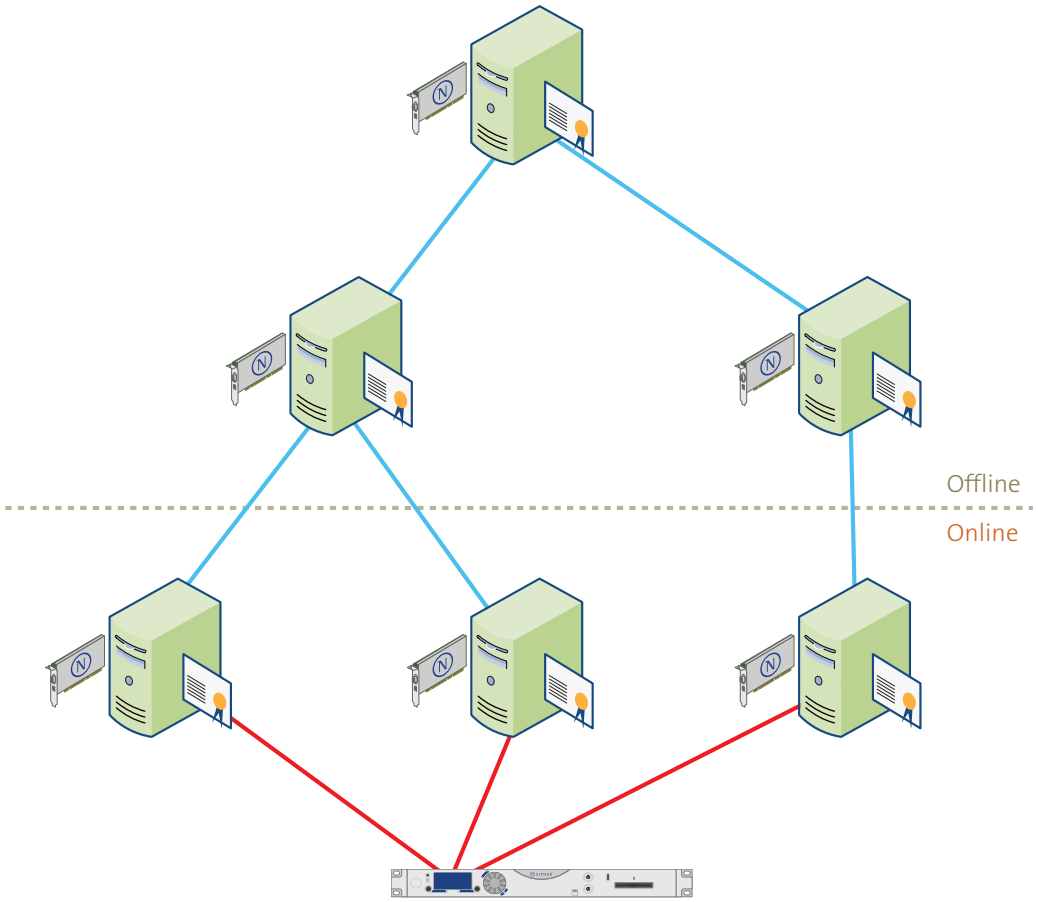

FIGURE 4

Implementing nShield HSMs and netHSMs at each CA in the CA hierarchy

Integration with Online Responders

The Online Responder uses an OCSP Signing certificate. The private key associated with the signing certificate is used to sign the OCSP responses that are returned to OCSP clients. Typically, if there is an existing netHSM in the environment, the OCSP responder is added as an additional client to the netHSM. A netHSM can provide cryptographic security to any device that needs protection of their private key material.

When deployed, the Online Responder would be simply an additional client for the netHSM shown in Figure 4.

CryptoAPI

The Microsoft Cryptographic API (CryptoAPI) provides services that enable application developers to add cryptography and certificate management functionality to their Win32® applications. Applications can use the functions in CryptoAPI without knowing anything about the underlying implementation,

in much the same way that an application can use a graphics library without knowing anything about the particular graphics hardware configuration.

The Microsoft CryptoAPI provides a set of functions that allow applications to encrypt or digitally sign data in a flexible manner. All cryptographic operations are performed by independent modules known as a cryptographic service provider (CSP). A number of software CSPs, including the Microsoft RSA providers and DSA/DH providers, are bundled with the operating system.

CryptoAPI supports many different types of CSP. Some provide different cryptographic algorithm suites while others contain hardware interface components such as smart cards and hardware security modules. Figure 5 illustrates the CryptoAPI support for CSPs.

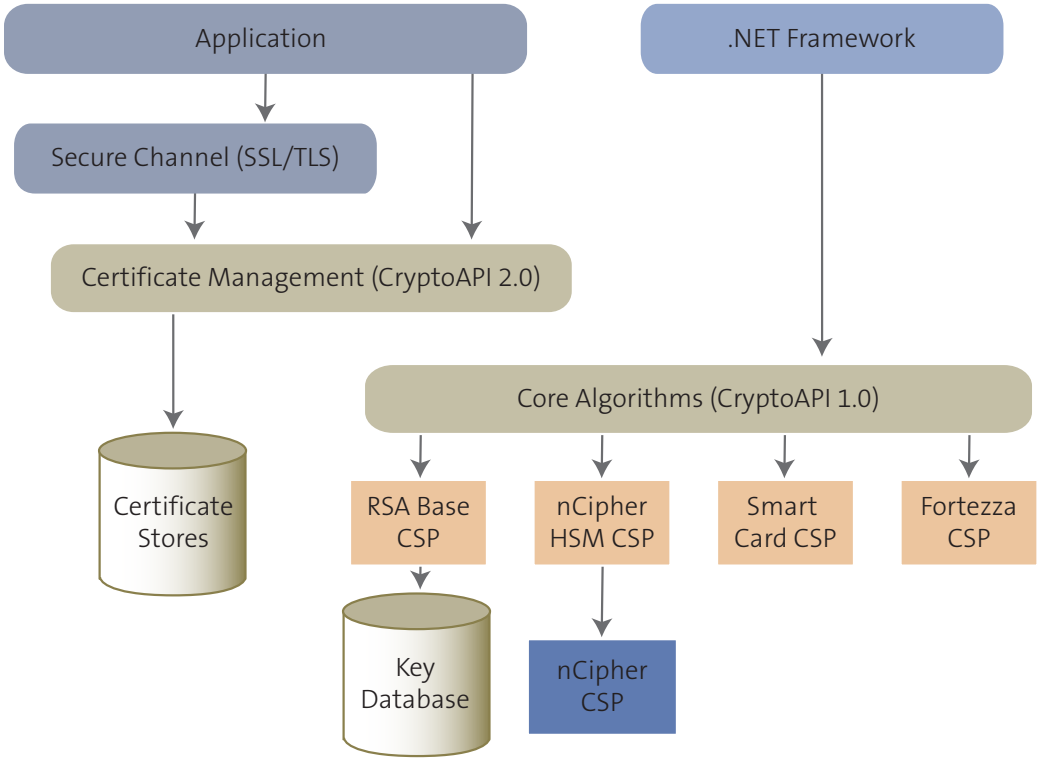

FIGURE 5

An Overview of the Cryptographic Service Provider (CSP) framework using CryptoAPI with nCipher HSMs

CAPICOM

The CryptoAPI interface can also be accessed through a method called CAPICOM which is built on CryptoAPI. CAPICOM is a COM client wrapper. CAPICOM can be used in applications created in many programming languages including Microsoft Visual Basic, C# and C++ to perform fundamental cryptographic tasks. A Visual Basic application for example can use CAPICOM objects to digitally sign data, verify digital data signatures, and encrypt and decrypt arbitrary data.

For additional information regarding the CryptoAPI programming model or CAPICOM, refer to the Microsoft Developer Network (MSDN) at (http://msdn.microsoft.com).

.NET Framework Cryptography

The .NET Framework cryptography model provides a cryptographic model that supports many standard algorithms in the .NET managed code. This model relies on the CryptoAPI 1.0 to implement the various algorithms. Figure 5 illustrates the .NET Framework relationship with respect to the CryptoAPI. Additional information about the .NET Framework cryptography model can be found at the Microsoft Developer Network (MSDN) at http://msdn.microsoft.com.

Cryptography Next Generation (CNG)

Cryptography Next Generation (CNG) implements a new cryptography infrastructure to replace the existing CAPI 1.0 APIs. CNG allows customers to plug new cryptography algorithms into Windows or to replace an implementation of an existing algorithm (for example, implementing a national version of an encryption algorithm due to local law requirements).

CNG currently coexists with CryptoAPI on Windows Vista and Windows Server 2008.

CNG has the following features that differentiate it from the legacy CryptoAPI:

- **Auditing**. CNG increases auditing abilities to include capturing events during testing of keys, cryptographic operations, reading and writing persistent keys to and from the operating system, and management of key pairs. To automatically generate KSP audit logs you must use auditpol.exe to enable collection of all KSP auditing by running auditpol / set /subcategory:"other system events" /success:enable/failure:enable.
- **Certification and Compliance**. CNG is targeting Federal Information Processing Standards (FIPS) 140-2 level two validation together with Common Criteria evaluation on selected platforms.
- **Cryptographic Agility**. CNG will support cryptographic agility, or the ability to deploy new cryptographic algorithms for an existing protocol such as SSL/TLS or to disable algorithms if a vulnerability is found with the specific algorithm. To a large degree, cryptographic agility was obtained by separating key storage from the actual key operations.
- **Kernel Mode Support**. CNG supports cryptography in kernel mode. Kernel mode provides better performance for common cryptographic features such as SSL/TLS and IPSec. That being said, not all CNG functions can be called from kernel mode. You can determine whether a function can be called from kernel mode by reviewing the reference topic for the specific function. If the function does support kernel mode, the caller must be running at PASSIVE_LEVEL IRQL. Note that supported cryptographic algorithms available in kernel mode are those implementations provided by Microsoft through the kernel mode CNG APIs.

- **Key Storage**. CNG provides a model for key storage that supports both legacy CryptoAPI and CNG-capable applications. The Key storage router, shown in Figure 6, conceals details for key access from both the application and the storage provider used.

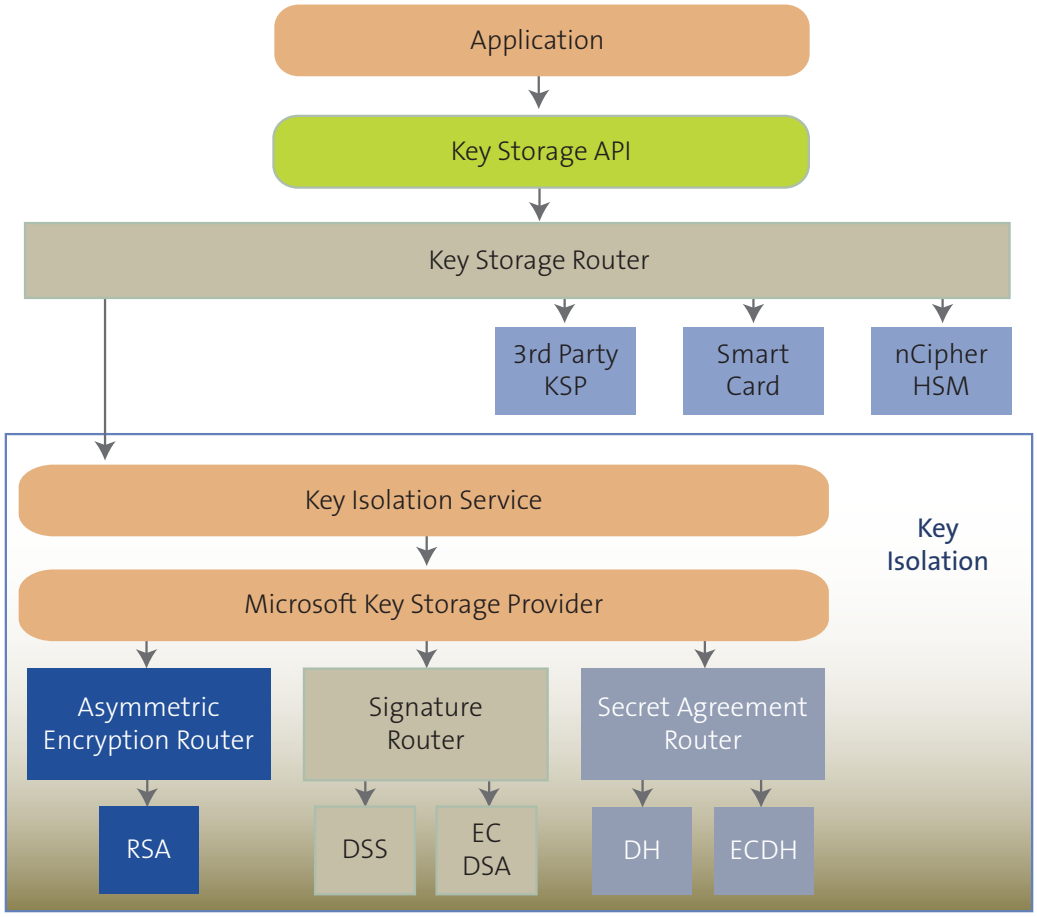

FIGURE 6

Key Storage Provider Model

- **Key Isolation**. CNG isolates long-lived keys so that they are never present in the application process. For example, CNG allows any computer with an HSM to provide key isolation and key storage in the HSM. The Local Security Authority (LSA) process is used as the key isolation process to maximize performance. The key isolation feature is not available on platforms prior to Windows Vista and Windows Server 2008. Also, only the Microsoft KSP is loaded in the key isolation service. Third party key storage providers (KSP) are blocked from being loaded in the LSA process.
- **Legacy Support**. CNG provides support for the current set of algorithms in CryptoAPI 1.0 for legacy applications.
- **Replaceable Random Number Generators**. Developers can replace the default random number generator for all cryptographic service providers

when using CNG. Previously, it was not possible to redirect Microsoft Base CSPs to another random number generator.

- **Thread Safety**. All functions within CNG are designed to support multithreaded/concurrent execution. This was not the case with the previous CryptoAPI functions.
- **Suite B Support**. This is probably the most recognized feature of CNG. In 2005, the United States National Security Agency (NSA) announced Suite B, a coordinated set of symmetric encryption, key exchange, digital signature, and hash algorithms for US government use. Suite B algorithms must be used for the protection of information designated as Top Secret, Secret, and private information.

The nCipher CNG providers include support for the Suite B and legacy algorithms out of the box; reference Table 1 in Appendix:

Hardware Cryptographic Service Provider (CSP)

Hardware based CSPs are used to provide enhanced performance by offloading cryptographic operations from host processors to specialized hardware. For the Microsoft Certificate Services, a hardware-based CSP also provides a higher level of assurance for the storage of private keys. Protecting private keys in specialized tamper-resistant hardware greatly increases their security as well as the overall security of the CA and the certificates it signs. It is a best practice to protect CA key material using hardware CSPs like the nCipher nShield or nCipher netHSM.

nCipher HSMs provide both FIPS 140-2 level 2 and level 3 validated solutions. For additional information on FIPS 140-2, please visit the National Institute of Standards and Technology web site, http://csrc.nist.gov/cryptval/140-2.htm. This includes the nCipher NIST approved evaluations.

nCipher Hardware Security Modules

Overview

The nCipher HSM provides hardware key storage, transactional acceleration, tamper-resistant physical hardening and full key-management functionality. This makes the nCipher family of HSMs ideally suited for use with certificate authorities and other PKI applications that use the Microsoft CryptoAPI.

nCipher nShield and nCipher netHSM HSMs are validated to Level 3 of U.S. Federal Information Processing Standards (FIPS), FIPS 140-2. This widely recognized security validation is an important factor in establishing the overall system security of a customer's PKI deployment. FIPS 140-2 validation is especially relevant in federal government and financial markets, where security policies frequently mandate FIPS validated products.

In addition, the nCipher HSMs provide cryptographic acceleration by offloading the RSA signature operations from the host CPU to the nCipher HSM. Thus, the CPU resources of the host server become available to perform other application processing. The nCipher HSM is capable of sustaining over 400 1024-bit RSA key signings per second (depending on model).

A unique feature of the nCipher HSM model is that the HSM securely stores keys on the server hard disk. Other solutions that store keys exclusively within the physical confines of the HSM, limit the number of keys that can be used by the HSM and complicate both back-up and disaster recovery activities, and the sharing of these keys with other HSMs. nCipher addresses these issues by storing 3DES or AES encrypted private keys (key blobs) on the host server to deliver best practice security and key management flexibility. This key management functionality is part of the nCipher Security World – nCipher's key management framework.

For more information about the nCipher HSMs and the nCipher Security World, refer to the nCipher Web site at: www.ncipher.com

nCipher Security World – A Key Management Framework

The nCipher Security World is a framework which maps security policies onto a flexible hardware-based security infrastructure. With nCipher's Security World, organizations can separate administrative and operational roles. It permits application keys that are securely stored as key blobs on the host to be easily shared between modules, backed up and recovered, and ensures that they can only be used within the confines of the tamper-resistant HSM. This security architecture easily scales to accommodate a growing PKI infrastructure; at any time additional modules can be added to an existing nCipher Security World.

The nCipher Security World framework consists of the following components:

- One or more nCipher HSMs (nShield, netHSM, or a combination of both)
- Smart cards for the administrative and operational roles
- Management software to install and manage the HSM(s) and cryptographic keys

- Host server that stores nCipher-specific management information

All the nCipher software components to support the Security World framework are shipped as standard with the nCipher HSMs. The software components work with both the dedicated nShield and the network-attached netHSM products.

Security World Key Management Concepts

The nCipher Security World differentiates between functions carried out for administrative purposes (e.g. adding a new hardware module, disaster recovery or backup and restoration) and functions for operational usage (e.g. key generation, key loading, etc). The role separation is enforced by the use of different sets of smart cards; an Administrator Card Set (ACS) for administrative functions and multiple Operator Card Sets (OCS) for operational functions.

The nCipher Security World model combines role separation with flexible access control management for individual roles. This paradigm fits nicely with the extensive role separation capabilities implemented in Windows Server 2008 PKI, where it is possible to enforce that each CA function is managed by a different user according to their organizational duties, e.g. different users can be specified for archival, recovery, backup and other processes. For more information on the CA separation of roles, refer to the Microsoft white paper, "Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure."

The major functionality of the ACS is:

- Restore a Security World
- Recover keys (if key recovery was enabled)
- Replace the existing ACS
- Delegate FIPS 140-2 level 3 authorization activities
- Passphrase recovery
- Manage key counting

The major functionality of the OCS is:

- Authorize use of application key(s)
- Authorize FIPS 140-2 level 3 management related activities

Note that each card set (ACS and OCS) in the nCipher Security World operates its own "k-of-n" threshold based secret share scheme. For example, an OCS may have been created with an "n" of 5 cards and a "k" of 3, which would require 3 out of the 5 card shares to be presented to the HSM to perform operational duties. Thus, if the quorum is set correctly no single person can have total control of a card set. Each card set may be created to optionally include passphrase authentication for each card in a set.

Typically, for conducting administrative tasks, the ACS will be managed by a team headed by the security officer. Whereas the OCS would be controlled by a team of operational staff members responsible for managing applications that require cryptographic actions such as signing and key generation. Each card from a card set would be managed by a unique individual, and

any administrative or operational functions can only be executed after the respective quorum of individuals correctly present their smart cards.

Key Access and Storage

An application "key blob" consists of the key material, the key's Access Control List (ACL), and a cryptographically strong checksum, all encrypted with a 3DES or AES key. In the case of a card set-protected application key, the 3DES or AES wrapper key used is stored via secret-sharing across the Operator Card set and is known as a Logical Token. In the case of a module-protected application key, the 3DES or AES key used is the Security World Module Key, stored in the HSM's nonvolatile memory.

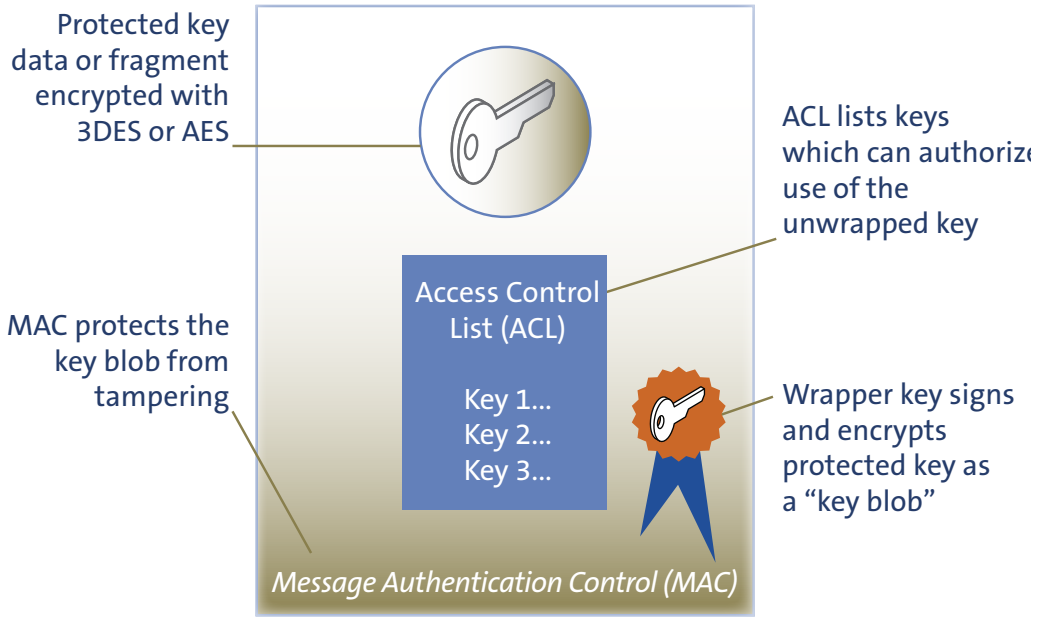

FIGURE 7

Components of a Key Blob

The Security World Module Key is itself stored in a blob on the host filesystem; the key data, ACL and checksum are encrypted with a 3DES or AES Logical Token stored on the ACS. This allows the Administrator Card Holders to load the Security World Module Key into additional HSMs. The security world module key can be loaded on both dedicated nCipher nShield HSMs and on nCipher netHSMs.

A Logical Token remains in the HSM and on the smartcards and is never passed to the host even in encrypted form. Additional encryption of the Shares of a Logical Token ensures that the passphrases (if set) are required to assemble the Shares into the original 3DES or AES key, and in the case of Operator Cards, to ensure that the card set is used only in HSMs possessing the Security World Module Key.

OCS-protected application keys with Recovery enabled are also stored in a Recovery Blob alongside the main working blob. The Recovery Blob is encrypted using an RSA key pair known as the Recovery Encryption Key. The private half of the Recovery Encryption Key is again stored as a blob protected by a Logical Token stored on the ACS. This allows the Administrator Card Holders to perform the recovery from lost or unusable Operator Cardsets as shown in Figure 8.

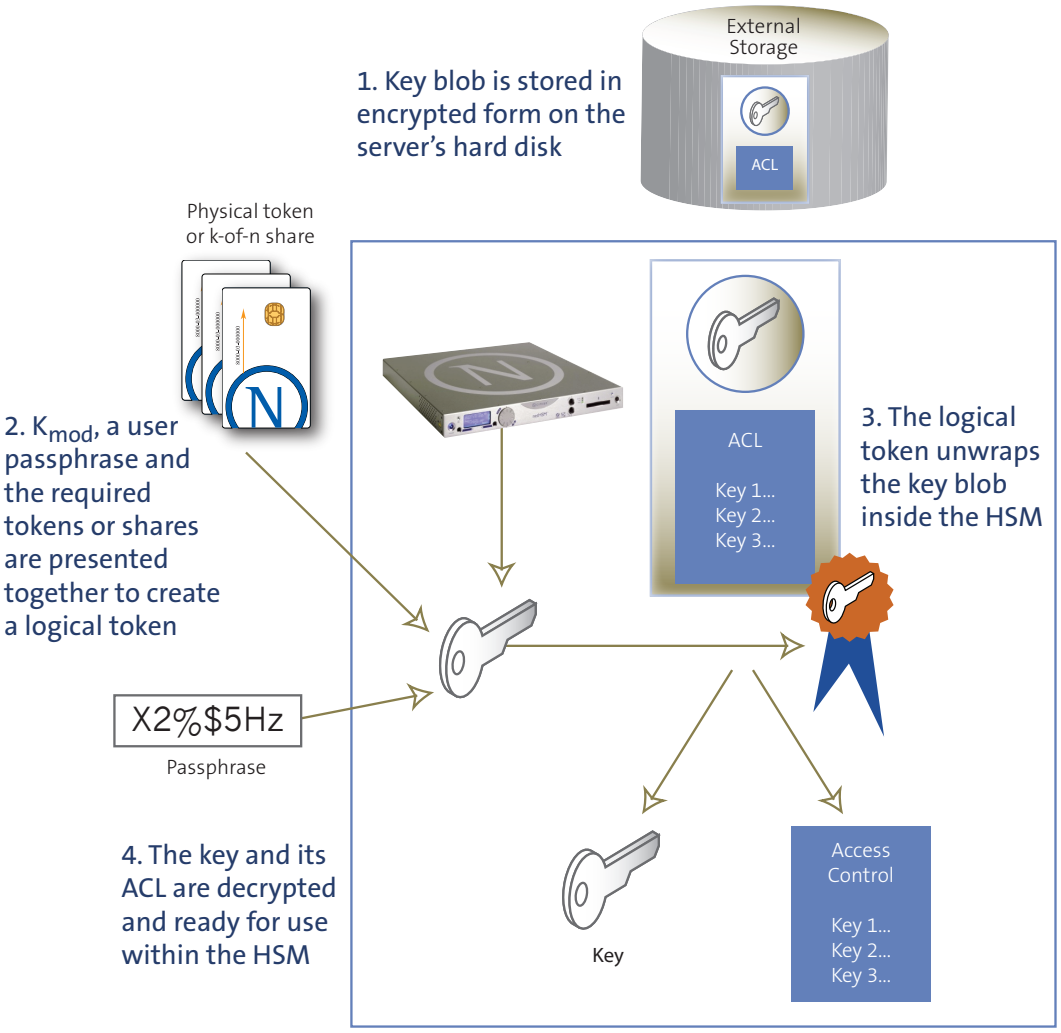

FIGURE 8

The process of fetching a key blob from the key store

Key Life Cycle Management Features

The nCipher Security World allows the key security policy to be mapped to the HSM, thereby providing for full life-cycle management:

Key Security

The private key is always generated inside the HSM, and never leaves the HSM security boundary as plaintext. The Security World securely stores each key as a blob on the host. This permits secure easy backup and recovery of important key data.

Key Generation

When generating a key pair, it is necessary to use a random number generator (RNG). A good RNG is crucial to creating keys that are not easily cracked. The RNG should be hardware based and located inside the HSM. An application that uses a software RNG produces only pseudo-random numbers and is therefore inferior to a hardware RNG. The true RNG used for creating a key pair inside the nCipher module is based on hardware. The number is derived from the thermal noise of a diode to ensure true randomness, preventing the random number sequence from being predicted. The RNG conforms to the tests specified in FIPS 140-2.

Shared Management and Role Separation

The ACS and OCS have clearly defined roles that apply to the specific Security World they were created with. At card creation, each card set is specified with its own "k-of-n" quorum. This means a minimum number of "k" cards must be presented before any action can be taken with the module. In addition to card possession, the nCipher Security World permits mandating that each card holder also authenticate themselves with a pass phrase. It is recommended that "k" is always less than "n" in order to ensure that a card loss or failure does not prevent a quorum being maintained.

The Ability to Support Key Policy

The Security World is very flexible, allowing it to be mapped to a variety of key policies. For example a policy might require: (1) that an application key may persist and continue to be used in the HSM after removing the OCS; (2) that key use should be limited to a specific amount of time; (3) that the key backup and recovery process should conform to existing IT policies for backup.

Secure and Simple Backup of Private Keys

The nCipher Security World stores the key blobs outside of the HSM in a secure manner on the host server. This makes the backup of the keys very simple. For example, a security policy may state that the key store should be backed up during the regular backup of the system by the server administrators, which can be accomplished without ever exposing any secrets because the keys are 3DES or AES encrypted. The backed up private keys cannot be used without access to the Security World in which they were created. The number of keys that can be stored on the host is limited only by the available disk space of the host server.

Secure and Simple Disaster Recovery

Recovering from a failed server or failed HSM is straightforward and secure, and can be easily documented in a security procedure. If both server and HSM failed, the server administrator copies the key store from the backup media to the new server. Once the key store has been recovered, the HSM administrators must introduce a new module and reload the old Security World using their existing ACS, and the Operators must present their OCS before key usage can finally occur. Thus, no one individual can subvert the process. Further, if the Security World contains more than one module on a network, the backup can be copied across the network to all the HSMs; this permits architectural flexibility whilst preserving security and scalability.

Load Balancing

The nCipher Security World permits the modules to share the cryptographic load, i.e. load balance. As the system load increases, it is easy to add another module to accommodate the extra load. For example, adding a new PCI HSM is straightforward using a PCI bus. Likewise, a client can connect to two or more netHSMs to achieve load balancing.

Failover

By adding more than one module to the system, failover is provided. This means that if one of the modules should fail during operation, the other module(s) will continue operating – a critical feature in a 24x7 enterprise.

Standards Compliance

The nCipher nShield and nCipher netHSM HSMs are validated to FIPS 140-2 level 3, the Federal Information Processing Standard 140-2 - Security Requirements for Cryptographic Modules. Many users require this high level of standards assurance, providing an independent third party security validation of the HSM. nCipher has also submitted its nShield for Common Criteria certification.

Scalability

The nCipher Security World allows keys to be safely shared across a series of HSMs. Hence, a large scale PKI installation, that may be geographically dispersed, can be assembled and consistently managed without any compromise in the security. Also, the nCipher Security World can be enlarged at any time to accommodate system growth – it is a simple task to add another module to a server.

The Synergy: Windows Server 2008 PKI and nCipher HSMs

A PKI solution requires strong synergy between the PKI application and a hardware security module. A critical part of this synergy is the ability to cater to both the security requirements and the business requirements – this means an infrastructure that has the flexibility and security policies to support the total key life cycle.

Key life cycle management relates to the secure administration of cryptographic keys throughout their entire life cycle. This includes key generation, key distribution, installation, backup, archival, usage and termination of use. As proposed by the KPMG best practices white paper, Figure 9 demonstrates the major stages in the life cycle of a key. Full life cycle management is achieved by integrating the properties of the Windows Server 2008 PKI and the nCipher Security World using the nShield or netHSM.

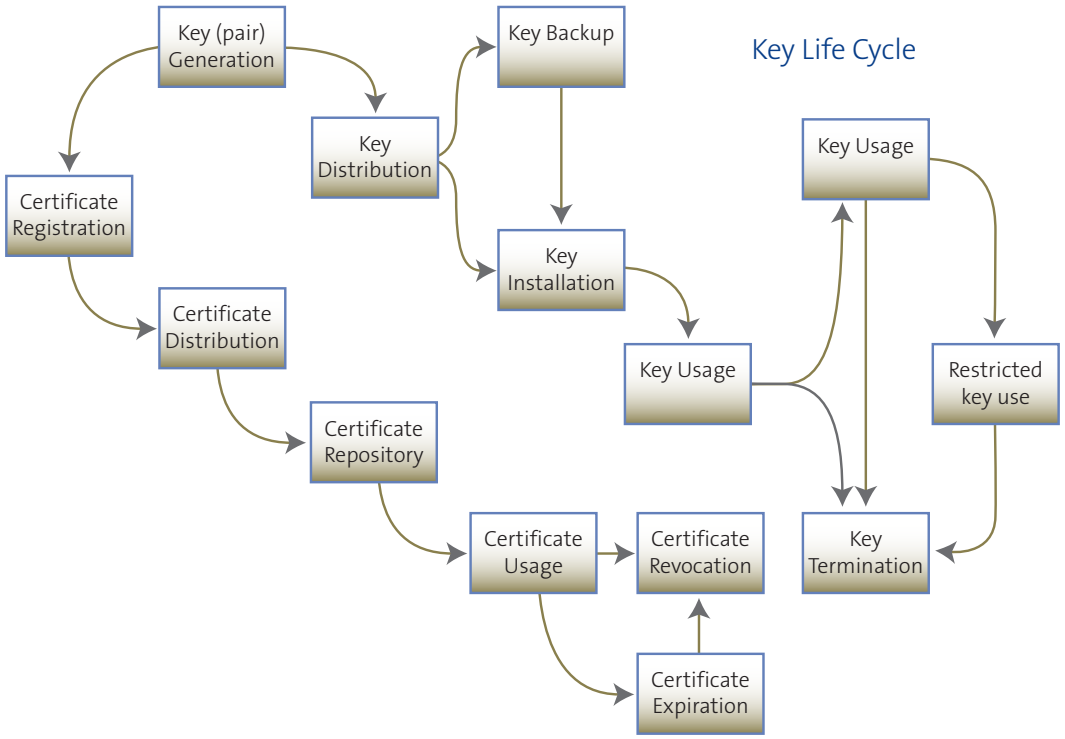

FIGURE 9

The complete life cycle of a key

Referring to Figure 9 and Table 6.0, each part of the key life cycle is analyzed with respect to the integrated solution, and illustrates how the nCipher and Microsoft components provide full key life cycle management. Table 6.0 clearly demonstrates the synergy between the Microsoft Windows Server 2008 PKI and the nCipher nShield or netHSM, and how together, the integrated solution meets all key management requirements of the modern enterprise.

It can be seen that for each step in the life cycle, the key is managed either by the Windows Server 2008 PKI or the nCipher nShield or netHSM module, or both. This is a clear demonstration of the solution synergy.

APPENDIX

Table 1.0 Supported Asymmetric Encryption Algorithms

ALGORITHM	TYPE	DESCRIPTION	STANDARD(S)
RSA	Legacy	The Rivest Shamir Adleman public key algorithm.	PKCS#1 v1.5 and v2.0

Table 2.0 Supported Symmetric Encryption Algorithms

ALGORITHM	TYPE	DESCRIPTION	STANDARD(S)
3DES	Legacy	The triple data encryption standard symmetric encryption algorithm.	FIPS 46-3, FIPS 81, SP800-38A
3DES_112	Suite B	The 112-bit triple data encryption standard symmetric encryption algorithm.	FIPS 46-3, FIPS 81, SP800-38A
AES	Suite B	The advanced encryption standard symmetric encryption algorithm.	Standard: FIPS 197

Table 3.0 Supported Hash Function Algorithms

ALGORITHM	TYPE	DESCRIPTION	STANDARD(S)
SHA1	Legacy	The 160-bit secure hash algorithm.	FIPS 180-2, FIPS 198
SHA256	Suite B	The 256-bit secure hash algorithm.	FIPS 180-2, FIPS 198
SHA384	Suite B	The 384-bit secure hash algorithm.	FIPS 180-2, FIPS 198
SHA512	Suite B	The 512-bit secure hash algorithm.	FIPS 180-2, FIPS 198
SHA224	Suite B	The 224-bit secure hash algorithm	RFC 3874

Table 4.0 Supported Digital Signature Algorithms

ALGORITHM	TYPE	DESCRIPTION	STANDARD(S)
DSA	Legacy	The digital signature algorithm.	FIPS 186-2
ECDSA_P256	Suite B	The 256-bit prime elliptic curve digital signature algorithm	FIPS 186-2, X9.62
ECDSA_P384	Suite B	The 384-bit prime elliptic curve digital signature algorithm	FIPS 186-2, X9.62
ECDSA_P521	Suite B	The 521-bit prime elliptic curve digital signature algorithm	FIPS 186-2, X9.62
ECDSA_P224	Suite B	The 224-bit prime elliptic curve digital signature algorithm	FIPS 186-2, X9.62

Table 5.0 Supported Key Agreement Algorithms

ALGORITHM	TYPE	DESCRIPTION	STANDARD(S)
DH	Legacy	The Diffie-Hellman key exchange algorithm.	PKCS #3
ECDH_P256	Suite B	The 256-bit prime elliptic curve Diffie-Hellman key exchange algorithm.	SP800-56A
ECDH_P384	Suite B	The 384-bit prime elliptic curve Diffie-Hellman key exchange algorithm.	SP800-56A
ECDH_P521	Suite B	The 521-bit prime elliptic curve Diffie-Hellman key exchange algorithm.	SP800-56A
ECDH_P224	Suite B	The 224-bit prime elliptic curve Diffie-Hellman key exchange algorithm.	SP800-56A

Table 6.0 Key Life Cycle and Application Coverage

STAGE IN LIFE CYCLE	RESPONSIBLE COMPONENT IN THE INTEGRATED SOLUTION	COMMENTS
Key Generation	nCipher	At the request of the application (the CA), the nCipher HSM generates a key pair with the appropriate properties for the application (e.g. key size, OCS protected, passphrase, persistent etc.).
Key Distribution	Windows Server 2008 PKI nCipher	Here the private key is securely sent to the appropriate assigned application and any backup devices. For a CA key, this could mean cloning the CA so that a duplicate backup system is available in the event of failure in the first system. This would require exporting the CA certificate and key blob to the backup system.
Key Backup	Windows Server 2008 PKI nCipher	The private key is backed up to prevent loss from an unexpected event such as a disk crash. The nCipher Security World stores all keys it generates as key blobs on the host disk. The key blobs can then be backed up using the standard backup policies and roles available with the Windows Server 2008 OS. Thus, the CA root key blob can be securely and easily backed up applying the standard OS backup procedures to the nCipher key store on the host. Key backup may occur in parallel to key distribution in some applications. If a key is recovered from the backup store, then it can be reinstalled at the key installation stage.
Key Installation	Windows Server 2008 PKI nCipher	The key is installed in the designated application/device for use. In the case of the CA, the key will be generated by the nCipher CSP and secured within the CSP. For a duplicate backup CA system, the key will need to be safely exported and installed on the second system. A non-CA example would be a web farm running Microsoft IIS 7. The certificate and key may need to be installed across a number of servers. In some application scenarios, key installation may occur in parallel with key distribution.

STAGE IN LIFE CYCLE	RESPONSIBLE COMPONENT IN THE INTEGRATED SOLUTION	COMMENTS
Key Usage	Windows Server 2008 PKI nCipher	The private key is used for its intended purpose. This requires both the nCipher HSM and Certificate Services functionality to accomplish the signing. The CA will receive and validate a certificate signature request (CSR) and the nCipher HSM will provide the cryptographic processing.
Key Archival	Windows Server 2008 PKI nCipher	Keys may need to be archived and therefore be available for some future use. For example, an employee leaves the company and their documents must be verified or decrypted with their key. The CA has the ability to encrypt and archive user and machine keys in it own database, and recover them using a key recovery agent certificate. Independently, the nCipher HSM automatically maintains a secure store of all key blobs it creates.
Key Termination	Windows Server 2008 PKI	In practice each key will have a finite life time. In a PKI installation the Certificate Services CA administrators will determine the life span of a certificate, and thereby the useful life span of the respective key. The CA can revoke a certificate before the termination date and then distribute the information using a base or delta CRL. (The nCipher HSM does not delete keys in its key store.)
Restricted Key Usage	Windows Server 2008 PKI	Sometimes it is necessary to authorize access to a user's archived key (e.g. to allow access to the encrypted files of a former employee and verify their authenticity – see key archival). The CA can be set up as a key recovery agent to retrieve and use the key for the immediate.
Certificate Registration	Windows Server 2008 PKI nCipher	The CA will receive a CSR and sign a valid request, using the nCipher HSM to perform the signing operation.
Certificate Distribution	Windows Server 2008 PKI	This is the process of transferring the signed certificate to the correct service or device.

STAGE IN LIFE CYCLE	RESPONSIBLE COMPONENT IN THE INTEGRATED SOLUTION	COMMENTS
Certificate Repository	Windows Server 2008 PKI	This stage denotes that the certificate is publicly available. The CA maintains a database of the certificates it has issued and their status.
Certificate Usage	Windows Server 2008 PKI	This step in the life cycle runs concurrently with the key usage step. The certificate and respective key is available for its intended purpose.
Certificate Expiration	Windows Server 2008 PKI	The CA creates certificates valid for a specific time. When the certificate expires both the certificate and the associated private key are no longer available for active use. Note that an encryption certificate can still be used to decrypt previous data, but can no longer be used to encrypt new data.
Certificate Revocation	Windows Server 2008 PKI nCipher	For any number of reasons, a certificate may be revoked before its normal expiration time. The CA will issue a base CRL or delta CRL with the latest revocations which prevents any future trust in the certificate. Windows Server 2008 can also utilize OCSP to provide revocation information to clients. The HSM protects the private key of the OCSP signing certificates used to sign the OCSP responses.

Glossary

ACL	Access Control List
ACS	Administrator Card Set
CA	Certificate Authority
CAPICOM	Certificate API COM
CNG	Cryptography Next Generation
COM	Component Object Model
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
IETF	Internet Engineering Task force
ISO	International Organization for Standardization
NDES	Network Device Enrollment Service
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OCS	Operator Card Set
OCSP	Online Certificate Status Protocol
PCI	Peripheral Component Interconnect
PCI-E	Peripheral Component Interconnect Express
PCI-X	Peripheral Component Interconnect- eXtension
PKI	Public Key Infrastructure
RFC	Request for Comment
RNG	Random Number Generator
TCO	Total Cost of Ownership

Further Reading and Related Links

For more information on Windows 2003 PKI Best Practices, see the Microsoft white paper, Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure, at
http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx

Information on nCipher's nShield
http://www.ncipher.com/products/hardware_security_modules/8/nshield/

Information on nCipher's netHSM
http://www.ncipher.com/products/hardware_security_modules/10/nethsm/

Further information on installing the nCipher nShield in a Microsoft PKI environment can be found in the nCipher Application Guide, Microsoft Certificate Services and nCipher Modules
http://active.ncipher.com/integrationguides/Microsoft/

nCipher Security World
http://active.ncipher.com/whitepapers/nCipher_security_world_wp.pdf

A white paper discussing key management policy and framework, refer to the KPMG document Key Management Policy and Practice Framework
http://www.ncipher.com/resources/white_papers/

Further technical information about the Windows Server 2003 Certificate Services can found at
http://msdn.microsoft.com

Further information on Windows Server 2003 autoenrollment can be found at
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/autoenro.mspx

For information on installing, configuring, and Troubleshooting OCSP in Windows Server 2008, see
http://go.microsoft.com/fwlink/?LinkId=101269

For information on Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003, see
http://technet.microsoft.com/en-us/library/cc787237.aspx

A white paper, Planning and Implementing Certificate Templates in Windows Server 2008, can be found at
http://go.microsoft.com/fwlink/?LinkID=92522

For more a white paper on Key Archival and Management in Windows Server 2008, see
http://go.microsoft.com/fwlink/?LinkID=92523

A Windows Server 2003 PKI Operations Guide can be found at
http://www.microsoft.com/downloads/details.aspx?familyid=8e25369f-bc5a-4083-a42d-436bdb363e7e&displaylang=en

An overview of Microsoft's Active Directory technology in Windows server 2003 can be found at
http://www.microsoft.com/windowsserver2003/technologies/activedirectory/default.mspx

Active Directory Certificate Server Enhancements in Windows Server Code Name "Longhorn"
http://www.microsoft.com/downloads/details.aspx?FamilyID=9bf17231-d832-4ff9-8fb8-0539ba21ab95&displaylang=en

Information on PKI Enhancements in Windows XP Professional and Windows Server 2003 can be found at
http://technet.microsoft.com/en-us/library/bb457097.aspx

...continued from prevous page

For additional information regarding the CryptoAPI programming model or CAPICOM, refer to the Microsoft Developer Network
http://msdn.microsoft.com/

For the latest information about Microsoft's .NET framework see
http://www.microsoft.com/net/

Information on FIPS 140-2 can be found at the NIST site
http://www.csrc.nist.gov/cryptval/

Information on IETF RFC 5280 and other IETF PKI standards can be found at
http://www.ietf.org

About IdentIT

Based in Canada, IdentIT Inc. was formed in 2003 by Paul Adare and Brian Komar, two acknowledged leaders in the fields of network security, identity and access management with nearly 40 years of combined experience working with the various product groups at Microsoft.

www.indentid.ca | +1 (416) 848-7331 | info@identit.ca

About nCipher

nCipher is the premier encryption and key management products and services provider to the world's most security conscious organizations. For 12 years nCipher has focused exclusively on delivering the world's most advanced yet practical encryption and key management solutions critical to protecting sensitive information. nCipher provides confidence to 800 customers worldwide by delivering solutions that strongly contribute to data protection and integrate with systems that rapidly retrieve critical information when needed.

THE KEY TO ENCRYPTION IS HOW YOU MANAGE IT™

North America
nCipher, Inc.
1655 McCarthy Blvd
Milpitas, CA 95035 USA
92 Montvale Avenue #4500
Stoneham, MA 02180 USA
Tel: +1 800 nCIPHER

EMEA
nCipher Corporation
Jupiter House
Station Road
Cambridge CB1 2JD
UK
Tel: +44 (0) 1223-723600

Asia/Pacific
nCipher K.K.
15th Floor, Cerulean Tower
26-1 Sakuragaoka-cho
Shibuya-ku, Tokyo
Japan 150-8512
Tel: +81-3-5456-5486

www.ncipher.com
info@ncipher.com