THALES

www.thales-esecurity.com

Thales e-Security

Upgrading and Improving the Trust of Microsoft Windows Certificate Authorities

Author:
Mark B. Cooper

White Paper

June 2014

Contents

Foreword

Almost all of the Windows Server 2003 support will end on July 14th, 2015.
This is the perfect time to move on to the latest and greatest operating system for your organization's Public Key Infrastructure (PKI) needs. Microsoft Active Directory Certificate Services (AD CS) 2012 R2 is leaps and bounds richer than Windows 2003 Certificate Services. We have added several new services such as Online Responder (OCSP), we have added capabilities to enroll from non-domain joined PCs and have several other enhancements such as default encryption enforcement on requests, support for stronger algorithms, suite-B, and better entropy etc.…

It's also perfect timing to get your Certificate Authority (CA) keys protected with a Hardware Security Module (HSM). AD CS provides great features and enhancements for your PKI environment, but having your valuable CA keys stored in software does not guarantee their security. HSMs are a great way to provide this assurance. To get maximum benefit, a PKI should be designed and deployed with an HSM to provide the best level of assurance in the CA keys. Existing PKIs can also improve their security by integrating HSMs and creating new CA keys that are protected by the HSM. Also, you should ensure the physical security of HSMs. It's important to ensure the devices are secured to manage physical and logical access to the HSM.

Take the time to research, design and plan for your new PKI environment.
This paper is a helpful resource and there is lot of help on Microsoft TechNet.

Rashmi Jha
Certificate Services Program Manager, Microsoft

Introduction

This paper examines the history of Microsoft Windows 2003 Server, the cryptographic landscape when it was introduced and improvements made since then. The paper will also explore the process of improving certificate authority (CA) security and protection by using Thales nShield hardware security modules (HSMs) and migrating to Microsoft Windows Server 2012 R2. This paper also contains security recommendations and guidelines for new and existing PKIs that do not need to be migrated as well. For more information about those scenarios, turn to the Hardware Security Module section to start.

Enterprises around the world use PKI to protect information critical to their business. PKIs can be used to provide strong authentication of users and computers in the organization such as wireless authentication (EAP-TLS) and smart card authentication to protect critical business assets.

A properly designed, deployed and maintained PKI help a business provide basic security controls such as confidentiality and integrity to their computer systems. A poorly managed PKI however, can introduce far more risks and attack surfaces in an organization than it solves. As PKI systems often act as a central resource that can allow a high level of access to an IT infrastructure, they are a logical target for any persistent and determined attackers. A compromised PKI can enable intruders to authenticate as any user in the organization, create unauthorized signatures, open encrypted secure socket layer (SSL) or transport layer security (TLS) traffic to snooping and allow access to corporate networks over virtual private networks (VPN) and wireless networks. All of these attacks are extremely difficult to identify and remediate after a compromise. This makes it all that much more critical to design and secure a PKI properly.

The announcement from Microsoft that all support for the Windows Server 2003 product family will end on July 14, 2015 should be considered a potential for security threats. After support has ended, these older operating systems will be a prime target for attackers because they know that any new attack vectors will not be mitigated by a Microsoft patch. Compound this security threat with marginal, aging cryptographic standards used in older CAs, and you find that enterprise PKIs around the world are facing a huge threat.

The cryptographic landscape is entering a period with a great many changes. In the last several years we have seen the deprecated use of hashing algorithms such as MD1, MD5 and SHA1 that were industry mainstays for decades. Cryptographic key sizes of 512 and 1024 which were once the most commonly issued key-size around the world are now considered unsafe and generally unavailable in the commercial market place. Set all these changes against the backdrop of organizations still running their CAs on Windows Server 2003, and the threat profile grows considerably. The risk of running an enterprise on out dated and unsupported software is too great a risk to ignore.

Overview of Active Directory Certificate Services (AD CS)

The most common implementation of a PKI for organizations is Microsoft's Windows Server operating system. While the name has changed over the years, Microsoft currently refers to their product offering as AD CS and has been available since Windows NT 4.0 as part of an Option Pack. Windows Server based CAs became popular with the release of Windows Server 2003. As a result, a great number of CAs were installed and set up to provide basic certificate needs to an organization.

AD CS provides services for creating and managing public key certificates used in software and network infrastructure security systems. Organizations use certificates to enhance security by binding the identity of a person, device, or service to a corresponding private key. However, in order to realize the enhanced security made possible by certificates, organizations need a cost effective, efficient, secure way to manage the distribution and use of certificates.

AD CS provides a number of PKI services for an enterprise. The most common service employed is the CA. A server configured as a CA provides the management features needed to regulate certificate issuance, distribution, and use. A CA:

- **Configures the format and content of certificates and issues certificates to users, computers, and services**
- **Establishes and verifies the identities of certificate holders**
- **Sets policies that control how certificates are to be used**
- **Revokes certificates if they should no longer be considered valid and publishes certificate revocation lists (CRLs) to be used by certificate verifiers**
- **Logs all request, issuance, renewal, and revocation transactions**

Today, most Windows CAs are used to issue certificates for use within an organization – they are rarely used for public facing websites. Internally, certificates are used to establish wired and wireless authentication, SSL (HTTPS) connections, and VPN authentication. Certificates are also used to enable Windows encrypted file systems, secure email (S/MIME), code signing, and user authentication (typically using smart cards). However, as use cases for digital certificates expand to include secure manufacturing, bring your own device (BYOD) and the internet of things (IoT), etc…, so will the demands on the CAs and the need for securely designed PKIs.

Windows Server 2003

Windows Server 2003 and its subsequent update (Windows Server 2003 R2) built upon the Windows Server model introduced with Windows Server 2000. It was the beginning of the era of Microsoft Trustworthy Computing initiative and as a result, the release focused on "attack surfaces" and "security postures" in the Windows Server product line.

This release proved to be a popular choice for many corporations and the adoption and deployment of CAs on the operating system grew considerably over the years. The ease of installation, management and integration with Active Directory made Certificate Services a compelling choice that was hard to ignore. In addition, Microsoft free licensing model made an attractive solution all that much easier to select.

Microsoft has subsequently released five newer operating systems with improved security postures and new features including many enhancements to AD CS. But many organizations still haven't migrated off of the Windows Server 2003 product family. This decision to delay upgrading is often driven by budget concerns, availability of product experts or the lack of a compelling business reasons to take action.

History of Windows CAs

Since Windows 2003 was such a ubiquitous platform in organizations, a large percentage of PKIs were either upgraded or deployed based on this operating system. The cryptographic options provided by Certificate Services addressed nearly all the needs of an organization at the time. These included RSA keys ranging from 512-4096 and hash algorithms such as MD-1, MD-5 and SHA-1.

The ease of installation, integration with the operating system and user interface presented almost no barrier to standing up a Windows CA. As a result, a large number of CAs were installed without consideration to long term cryptographic needs. Very few PKIs are designed and deployed with foresight of security concerns 10-15 years after implementation. These CAs that were designed to improve the security of a network are now themselves becoming a security threat. They now suffer from an aging set of cryptographic algorithms, limited certificate enrollment mechanisms and a soon to be unsupported operating system.

Subsequent Enhancements

Building on the success of Windows Server 2003, Microsoft released a number of updates to the Server product line with Windows Server 2008, Server 2008 R2, Server 2012 and the current iteration of Windows Server 2012 R2. Along with improvements in speed, functionality and security, a number of enhancements were made to Certificate Services which evolved into AD CS in the Server 2012 product line.

Windows Server 2008 introduced an entirely new cryptographic engine called Crypto Next Generation (CNG). CNG not only changed the structure and expandability of the cryptographic engine, but it included a new generation of key providers such as elliptical curves and SHA-2 based hashes. It also included many new features that expanded the reach of the PKI within an enterprise and made it easier to enroll and manage device certificates across networks and firewalls.

To comply with Common Criteria (CC) requirements, long-lived keys must be isolated so that they are never present in the application process. CNG provides Key Isolation and is enabled by default in Windows Server 2008 and newer. Key Isolation ensures that only trusted kernel level processes can load and access key material. These processes then present a handle to applications that can then request cryptographic actions using the keys represented by the handle. While the keys are isolated, they are still subject to exploits targeting memory and disk systems. Key Isolation was not available prior to Windows Server 2008.

Another value proposition of CNG is cryptographic agility, sometimes called cryptographic agnosticism. Converting implementation of protocols like SSL or TLS, CMS (S/MIME), IPsec, Kerberos, and so on, to CNG, however, was required to make this ability valuable. At the CNG level, it was necessary to provide substitution and discoverability for all the algorithm types (symmetric, asymmetric, hash functions), random number generation, and other utility functions. The protocol-level changes are more significant because in many cases the protocol APIs needed to add algorithm selection and other flexibility options that did not previously exist.

Features in CNG, include:

- **A new crypto configuration system, supporting better cryptographic agility**
- **Finer-grained abstraction for key storage (and separation of storage from algorithm operations)**
- **Process isolation for operations with long-term keys**
- **Replaceable random number generators**
- **Thread-safety throughout the stack**
- **Kernel-mode cryptographic API**

End of Life - Support

To better define its support responsibility and provide customers with predictable timelines, Microsoft created the support lifecycle policy. This policy dictates how long a product will be supported by Microsoft including updating features and patching security issues. Additionally, the policy offers large organizations the ability to purchase extended support which provides the same level of support for several additional years.

The Windows product family is driven by defined lifetimes based on future Service Pack releases as well as newer operating systems. In the case of Windows Server 2003, Mainstream Support, which provided support for any customer, ended in 2010. Thousands of large corporation opted to continue to use the operating system and contracted with Microsoft for Extended Support, and that support ends July 14, 2015.

The Impact

Undoubtedly, the temptation to continue to use Windows Server 2003 outside of support will interest some organizations. This is a risky strategy. In the last ten years Microsoft's operating system design, security posture and mitigation tactics have changed a great deal.

Moving forward, Microsoft has been very clear that there will be no additional support for a product past the Extended Support phase. That includes security hotfixes or patches to combat new threats.

Microsoft has a focused patch process that can leave older operating systems vulnerable. When an issue has been discovered, the process to identify and remedy the issue also determines which operating systems are affected. This process doesn't generally include out of support products and as a result they can remain susceptible to known attacks. This makes Windows Server 2003 a prime target for attackers.

Combine a fragile, unpatched, unmaintained operating system with key enterprise services such as Certificate Services – it's a recipe for disaster. Since CAs provide centralized administration, issuance and management of identities in an organization, their presence on an operating system like this presents an enormous security threat to an organization if they are compromised.

Windows Server 2012 R2

There are four editions of Windows Server 2012 R2: Foundation, Essentials, Standard and Datacenter. As with Windows Server 2012, the Datacenter and Standard editions are feature identical, varying only based on licensing (particularly licensing of virtual instances). The Essentials edition has the same features as the Datacenter and Standard products, with some restrictions.

From a security point of view, Windows Server 2012 R2 has added a number of new and improved security features aimed at enhancing the protection of the operating system and services. These new features compliment a CA by protecting the underlying operating system components and providing a safer platform to run a PKI. These new features include UEFI Secure Boot, Network protected BitLocker volumes, DNSSEC for name resolution integrity, Kerberos authentication armoring (RFC 6113) and Active Directory claims.

AD CS was enhanced in 13 different areas with new or improved security features including PowerShell and Server Core support, AD DS Site Awareness, Certificate Lifecycle Notifications, and Certificate Template improvements.

Key AD CS Improvements

From a licensing standpoint, the unification of features across the Server editions has greatly lowered the cost to deploy a Windows CA. Prior to Windows Server 2008 R2, organizations typically needed one or more Enterprise editions of Windows Server to provide Active Directory integration and auto-enrollment capabilities to automatically enroll certificates for computers and users in the enterprise. The Enterprise edition cost was significantly more than the Standard edition. With 2012 R2, it no longer matters which edition of the operating system you choose to deploy – though most organizations will choose to use Standard edition as it meets all the needs of AD CS.

The key Windows Server 2012 R2 AD CS improvements build on many of the new features introduced in Server 2008 R2. These include:

- **CNG Suite B Support**
- **Diversified Client Enrollment Services**
- **Encrypted Certificate Enrollment**
- **Trusted Platform Module Enrollment**

CNG Suite B Support

First implemented with Windows Server 2008, Windows CNG includes support for the Suite B algorithms. In February of 2005, the U.S. National Institute of Standards and Technology (NIST) announced a coordinated set of encryption, asymmetric secret agreement (also known as key exchange), digital signature and hash functions for future use called Suite B.

Suite B cryptography recommends use of elliptic curve cryptography (ECC) in many existing protocols such as the internet key exchange (IKE, mainly used in IPsec), TLS, and S/MIME. CNG includes support for Suite B that extends to all required algorithms: AES (all key sizes), the SHA-2 family (SHA-256, SHA-384 and SHA-512) of hashing algorithms, elliptic curve Diffie-Hellman (ECDH), and elliptic curve DSA (ECDSA) over the NIST-standard prime curves P-256, P-384, and P-521.

Additionally, the ECC algorithms offer an exponential increase in the security and efficiency of key materials. These algorithms are not only significantly stronger and harder to compromise, but their shorter key sizes offer increase performance and throughput in any key related operations.

Suite B provides the ability for businesses to greatly improve the cryptographic standards in use for their PKI. These advanced algorithms dramatically increase the security and protection of the information and authentication processes in the organization. The SHA-2 hashes replace the older MD1, MD5 and SHA-1 options that have been shown to be weak and should no longer be used. These hashes are no longer considered commercially acceptable and are no longer available through mainstream commercial certificate providers.

Diversified Client Enrollment Services

Certificate Enrollment Web Services is a feature that was added in Windows 7 and Windows Server 2008 R2. This feature allows online certificate requests to come from untrusted Active Directory Domain Services (ADDS) domains or even from computers that are not joined to a domain.

The ability to centrally manage the certificate enrollment and renewal process for an enterprise is an important benefit of using AD CS. With key-based renewal, administrators can now manage certificate enrollment for computers regardless of their location or network access. Whether it's a server in a DMZ or a user computer in a remote location connected to the internet, certificate management is as easy as computers on the corporate network.

Encrypted Certificate Enrollment

This new security feature ensures that certificate enrollment requests generated by client computers are protected as they are transmitted to a CA. Without this feature, it is possible for a certificate request to be manipulated by a man-in-the-middle attack and enable an attacker to compromise the certificate that is issued by the CA.

When a certificate request is received by a CA, encryption for the request is enforced by the CA via the RPC_C_AUTHN_LEVEL_PKT, as described in MSDN article Authentication-Level Constants (http://msdn.microsoft.com/library/aa373553.aspx). On Windows Server 2008 R2 and earlier versions, this setting is not enabled by default on the CA. On a Windows Server 2012 or Windows Server 2012 R2 CA, this enhanced security setting is enabled by default.

Trusted Platform Module Enrollment

AD CS in Windows Server 2012 R2 allows for a certificate to be configured so that it will be renewed with the same key. This allows the assurance level of the original key to be maintained throughout its lifecycle and applied to a succession of certificates. Windows Server 2012 R2 supports generating Trusted Platform Module (TPM)-protected key pairs on end-user devices such as laptops by using TPM-based key storage providers (KSPs). The benefit of using TPM-based KSP is true non-exportability of keys protected by the anti-tampering mechanism of TPMs. Administrators can configure certificate templates so that Windows 8.1 and Windows Server 2012 R2 give higher priority to TPM-based KSPs for generating keys. Also, using renewal with the same key, administrators can remain assured that the key still remains protected by the TPM after renewal.

An important consideration when implementing TPM-based keys for end-users is the integrity of the CAs in the PKI. Even though the user's private keys are stored in a TPM on the end-user device, if the CA's signing keys are not properly protected, the value of TPM storage is greatly diminished. Using the default software storage for CA signing keys, the end-users would have a higher level of protection than the CA. To properly secure these keys, and preserve the integrity afforded by TPMs, an HSM should be implemented to protect the entire PKI chain. A compromise of the CA's signing keys affects the entire chain of CAs and end-users below it. Whereas, a compromise of an end-user certificate is limited in scope to that specific user.

Hardware Security Modules

The most vulnerable part of a PKI is the CA's own cryptographic keys. The CA signing keys are used to sign every certificate and revocation list used in the PKI and are considered the anchor in trusting the CA. Access to these keys would allow an entity to impersonate the CA and issue certificates that will be fully trusted in the environment. This makes the CA keys an extremely attractive target for attackers, a risk needs to be mitigated in order to protect the trust and integrity of the PKI.

By default, Microsoft Windows uses the Data Protection API (DPAPI) to secure CA signing keys. DPAPI is a password-based data protection service and is designed to use the logon password of the calling security context, such as a user or service account. The drawback is that all protection provided by DPAPI rests on the strength of the password.

Yet DPAPI presents a number of scenarios where the CA signing keys can be compromised. Since DPAPI protection is dependent on account passwords, anyone with access to log onto the CA can potentially compromise the keys. These scenarios include:

1) Loading of keys used by the CA into server's memory from disk storage – This means that the CA signing keys can be present on hard disks even after they have been removed from a server. Since the operating system manages the access to the keys and their storage, it is nearly impossible to completely control access to the keys.
2) Authorized administrators, users, and others with legitimate access to the CA – While they are operationally allowed today, they could be a threat to the organization in the future after changing roles or leaving the organization.
3) Windows system state backups which contain the DPAPI protected storage folders – With one of these backups, an attacker could replicate a CA and create certificates that are trusted in the organization.
4) Virtual servers running AD CS present an easy target – Since the operating system and its protected keys are already in a single file, it presents a simple target for an attacker to copy the virtual hard disk (VHD) and recreate the CA.

Soft versus Hard Keys

Because of the critical nature of CA signing keys, the storage, security and management of these keys needs to be well defined. Microsoft Windows default CAPI Cryptographic Service Providers (CSP) and KSP store CA signing keys in an encrypted state on the system partition. This type of key storage is considered a "soft key" since the control and storage of the key is governed strictly by software.

When accessed, these keys are unencrypted and presented to the calling application – such as AD CS. In Windows 2008 and newer, CAPI and CNG use a Key Isolation service which provides handles to the keys requested, but applications do not have direct control over the keys. Even with Key Isolation, soft keys can be a potential threat to the integrity of the CA keys. Since the key material must be loaded in memory to be accessed, it can be exposed through memory dumps and kernel attacks.

Hard keys on the other hand use HSMs to store and manage key access. These devices use a CSP or KSP that interfaces with the Windows CAPI and CNG interface and alter the creation, signing and storage of keys. The resulting keys are then only accessible within the hardware device itself. When an application, such as AD CS, requires a key, the HSM retrieves and loads the key in its protected firmware and provides a handle back to the application. At no time is the key material loaded or present in the operating system. If the memory was dumped or the operating system compromised, there would be no sensitive key material present. This drastically increases the protection of the private keys – an important consideration for CAs that are responsible for information integrity and confidentiality.

Thales nShield HSMs are used to protect and manage cryptographic keys – fundamentally keeping keys away from the operating system and locked inside an isolated security device. HSMs are traditionally used in a PKI to provide secure creation, storage and management of CA keys. They also provide functionality that organizations can use to enforce operational and logical security of the CA. HSMs support strong authentication for systems administrators and enable dual controls to be enforced where no single person or 'super-user' can act alone on the system to conduct a malicious attack. Finally, as a side benefit, HSMs provide cryptographic acceleration which is particularly important where large volumes of certificates are issued, as well as when extra-long or computationally difficult keys are employed.

In Perspective – The Heartbleed Vulnerability

The Heartbleed vulnerability of the OpenSSL service illustrates the risk of soft keys. While this bug was found only in specific versions of OpenSSL, the same potential threat exists with any operating system.

Any software protected private key should be considered a weakness and subject to potential exploitation.

Mitigating Risks with a Thales nShield HSM

HSM devices offer greater control over the access to key materials through the use of user card sets. Keys can be created with the HSM so that specific passphrases or cards must be presented to access the keys. This can be a manual process where users identify themselves for each key access request (low volume and high security scenarios) or automatically presented to trusted applications (online and high volume scenarios).

For optimal results, an HSM should be part of an initial PKI design plan to ensure the CA keys are completely protected. However, even if an HSM was not initially used, it can be implemented at any time. This includes during a migration of AD CS from older operating systems to Windows 2012 R2, in fact, a migration exercise is a perfect time to re-evaluate security policies and assess the value of deploying HSMs.

Through the proper planning, migration and security control, many of the HSM improvements can be implemented in existing PKIs. Alternatively you may decide to implement a new PKI as part of your migration strategy that will leverage HSMs for all of the new CAs.

Gartner Research on Hardware Security Modules

In a July 2012, Gartner Research released a report titled "Decision Point for Public-Key Infrastructure". The report states: "Key management and storage for the CA itself should be implemented using an HSM capable of protecting against logical and physical attacks on the key store. Such devices should be appropriately accredited to standards such as FIPS 140-2 or other national equivalent."

Migrating to Server 2012 R2

The process to migrate to Server 2012 R2 is not to be taken without proper research, preparation and planning. Fortunately there are defined steps and options for just about any migration scenario, including the addition of a Thales nShield HSM during a migration. While the specific step-by-step procedures for the migration are beyond the scope of this white paper, there are a number of important topics and considerations in planning the migration. The considerations to review for the migration include the existing PKI integrity, cryptographic suitability for future certificate needs, and the security of the CA signing keys.

It is also important to note that Microsoft provides an upgrade path direct to Windows Server 2012 R2 from any older operating system. That means you do not need to upgrade to intermediate versions of Windows to perform the upgrade. However, there is a restriction in performing in-place upgrades of an existing operating system. Beginning with Windows Server 2008 R2, the server operating system became available only as a 64-bit operating system. If you have a 32-bit version of an older operating system you will not be able to do an in-place upgrade. You will either need to migrate the CA to another server or you will need to back-up the CA and perform a full installation of Windows Server 2012 R2.

Considerations

Prior to migrating AD CS to Windows Server 2012 R2, there are a number of areas that need to be carefully considered. These will form the backbone for the migration plan and will greatly affect the integrity of the PKI. The planning and execution of the migration needs to ensure the integrity and security of the CA is not diminished as a result of improper handling or missing security practices. In addition, there may be some cases where the existing PKI lacks sufficient integrity and trust that a migration of the existing infrastructure is pointless. In this scenario, the design and deployment of a new PKI may be a better option for the organization.

If the existing PKI has been well maintained and is considered secure, then it is a candidate for migration. This decision should be based on the health and operation of the CA, integrity of keys, cryptographic key strength, physical and logical security controls and architectural suitability for certificate needs. If any of these areas are found to be lacking, the migration planning should focus on the design and deployment of a new PKI instead. Existing certificates can then be renewed with the new PKI to allow the old architecture to be safely retired and removed from operation.

Integrity of Existing PKI

The integrity of your existing PKI must be carefully examined to ensure it is operationally healthy and secure. If the PKI is meeting or exceeding the requirements of your organization, then it is a good candidate for upgrading to Windows Server 2012 R2. However, if the integrity of the PKI is in doubt, you should plan on deploying a new PKI and then transition away from the older PKI.

When reviewing the integrity of the PKI you should consider the current health of the operating system, success versus failure of certificate issuance, CRL and Authority Information Access (AIA) availability, architectural design and its suitability for your certificate issuance needs, documentation, physical and logical security controls as well as hierarchical design to ensure CAs are properly managed and maintained.

Cryptographic Algorithms

While there are many new cryptographic options available in Windows Server 2012 R2, a careful analysis is required. Implementing the newest algorithms can prove to be difficult in many organizations due to application and operating system compatibility. In general, if client operating systems are Windows 7 or newer, they will have full support for any of the new SHA-2 hashes and ECC based encryption keys.

Since the older PKI most likely has legacy CA cryptographic keys in use, the migration to Windows Server 2012 R2 can be crafted to improve the cryptographic value of these keys. There is no mechanism available to switch from legacy RSA keys to Suite B ECCDSA keys. If there is a desire to implement and use these new encryption types then you will need to design and deploy a new PKI. Existing certificate holders can be re-enrolled from the new PKI.

Windows Server 2012 R2 does however support changing the hash algorithm used to sign certificates. You can implement the change to SHA-2 based signatures at any time after upgrading the CA. Existing certificate holders will not be affected unless you choose to renew their certificates.

CA Key Protection

The protection of the CA keys is paramount to the integrity and trust of the CA. If your PKI was deployed with an HSM, the migration to Windows Server 2012 R2 can continue to leverage that protection. If however, your PKI has been relying on software protection, then it's time to mitigate those risks and implement an HSM.
A Thales nShield HSM can be introduced into your PKI in one of two ways depending on the level of trust you want in your organization.

If the existing PKI trust and integrity meet your needs and you wish to integrate an HSM, this can be accomplished during the migration. After the installation of the CA onto the new operation system, the CA keys can either be imported into the HSM directly or the CA can create a new key that is protected by the HSM. This option affords some key protection, but lacks full integrity of the keys since the CAs have a history of keys that existed outside of an HSM.

The other migration option is to design and deploy a new PKI that integrates a Thales nShield HSM from the start. This new PKI will be used to replace the older infrastructure and can be configured to be significantly more secure, robust and able to maintain a higher level of integrity. The CA keys will be generated and always exist in the HSM and thus protected to a higher level than a migrated PKI.

Existing certificates can be re-issued by the new PKI and the old PKI decommissioned after all clients have been migrated.

Migration Overview

The migration to Windows Server 2012 R2 has a number of considerations and variables depending on your unique needs. However, there are several high-level steps in a typical migration. This section shows a typical migration where the existing PKI is maintained and is upgraded to Windows Server 2012 R2. In addition, a Thales nShield HSM is introduced to protect the CA keys moving forward and ensure the CA maintains an adequate level of integrity for its cryptographic keys.

Step 1: Build New CA Server
This step can be performed at any time prior to the actual migration date as it has no impact on the existing PKI. The operating system is installed, patched and readied for AD CS. In addition, the HSM is installed and its CSP is installed and configured to support AD CS.

Step 2: Back up CA Configuration Data
The CA has a number of elements that need to be backed up and migrated to the new installation, these include registry keys, CA database and the CA keys. Prior to the start of the backup, the CA should have its templates removed to prevent any further enrollments after the backup is completed. The backup is then transported to the new CA and readied for installation.

Step 3: CA Installation on New Computer
The installation of AD CS is started and the existing CA key from the backup is used. After the installation is completed, the CA database is restored. The registry keys are then examined for key configuration settings and applicable ones are manually added to the registry on the new computer.

Step 4: Improve CA Key Protection
The CA is then configured to create a new key-pair using the CSP provided with the HSM. This will ensure that the keys used by the CA going forward are properly protected in the secure key management architecture of the HSM.

Step 5: Verify Operations
After the migration is completed, you should verify the PKI is working properly. This includes availability of CRL and AIA, enrollment and renewal operations and manual enrollment with tools such as Microsoft Management Console (MMC) and the Web Enrollment pages.

Step 6: Decommission Old CA
Once the new CA is found to be working properly, the old CA can be decommissioned and removed from the network.

Summary

As illustrated in this paper, the integrity and security of CAs is of critical importance not just to the trust of the PKI, but also the information in the organization it protects. Relying on outdated security technology and unsupported operating systems exposes an organization to compromise and data theft. As Microsoft retires older operating systems, these systems will become bigger targets for attackers and result in an increasing number of compromises. Coupled with outdated cryptographic solutions, organizations need to be active in moving away from these older services.

There have been many changes to the PKI landscape over the last 10 years since Windows Server 2003 was released. The Microsoft Windows Server 2012 R2 improved security features, AD CS enhancements and improvements to the AD CS cryptographic engine provide a better platform for today's trust and authentication system. Services for managing certificate enrollment over a diverse client base and managing clients disconnected from a corporate network are compelling features for many organizations.

Perhaps one of the biggest benefits of migrating to Windows Server 2012 R2 is the ability to leverage the enhanced cryptographic algorithms to increase the complexity of CA signing keys. Coupled with the integration of a Thales nShield HSM, the integrity and trust of AD CS is exponentially increased. These two components will help organizations protect their valuable information and secure authentication systems for many years to come.

As demonstrated by the recent OpenSSL Heartbleed vulnerability, the protection and management of key material is of paramount importance to information security. While Windows provides a base level of software protection for CA signing keys against basic threats, it has no ability to offer positive control over access and management of these keys. Using a Thales nShield HSM allows organizations to define, execute and manage complete control over the use of their CA signing keys.

All of these factors illustrate now is the time to assess your organization's security threats and data protection needs. It should include a thorough review of your PKI, including the protection of and cryptographic usefulness of CA signing keys, and the underlying operating system. Taken together, these risks will become the basis for a migration and upgrade plan. Waiting any longer will expose organizations to greater risks and larger financial liabilities than addressing the issue proactively.

THALES

About the Author

Mark B. Cooper, President and Founder of PKI Solutions Inc., is a former Microsoft Senior Engineer and subject matter expert for Microsoft Active Directory Certificate Services (AD CS). Known as "The PKI Guy" at Microsoft for 10 years, he traveled around the world supporting PKI environments for Microsoft's largest customers. He focused on supporting security solutions for Fortune 500 companies and acted as their trusted advisor in all things related to PKI. He has worked with customers in the financial, manufacturing, technology, transportation, and energy sectors as well as many levels of state and federal governments. Upon leaving Microsoft, Mark founded PKI Solutions Inc. and now focuses on providing PKI consulting services to select companies.

About Thales e-Security

Thales e-Security is a leading global provider of data encryption and cyber security solutions to the financial services, high technology manufacturing, government and technology sectors. With a 40-year track record of protecting corporate and government information, Thales solutions are used by four of the five largest energy and aerospace companies, 22 NATO countries, and they secure more than 80 percent of worldwide payment transactions. Thales e-Security has offices in Australia, France, Hong Kong, Norway, United Kingdom and United States.
For more information, visit www.thales-esecurity.com

Follow us on:

Americas – Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Unit 4101, 41/F, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com