At a glance:
Server Consolidation
Improved Existing Scenarios
Software + Services
Strong Authentication

PKI Enhancements in Windows 7 and Windows Server 2008 R2

John Morello

This article is based on pre-release code. All information herein is subject to change.

It seems like just yesterday I was writing an article titled "PKI Enhancements in Windows." That article, which ran in the August 2007 issue of TechNet Magazine, focused on some of the innovations that shipped in Windows Vista and Windows Server 2008. These innovations included such things as enrollment UI improvements and OCSP (Online Certificate Status Protocol) capabilities. While those enhancements were valuable and well received by users, you could argue that the changes were really incremental changes from an IT professional's perspective. Windows 7, however, will deliver PKI enhancements that greatly improve the deployment and operational experience for users, enabling powerful new scenarios while decreasing operational costs.

The improvements in Windows 7 and Windows Server 2008 R2 are focused around four core areas (shown in **Figure 1**):

Server consolidation. This allows organisations to reduce the total number of certificate authorities (CAs) required to meet their business objectives.

Improved existing scenarios. This focus is on such elements as offering more complete SCEP (Simple Certificate Enrollment Protocol) support and including a Best Practices Analyser (BPA).

Software + Services. This is to enable autonomous enrollment of users and devices for certificates regardless of network boundaries and certificate providers.

Strong authentication. This area focuses on improvements to the smart card experience, the introduction of the Windows Biometric Framework, and so on.

In this article, I explore some of the major changes in these areas from the perspective of an IT professional.

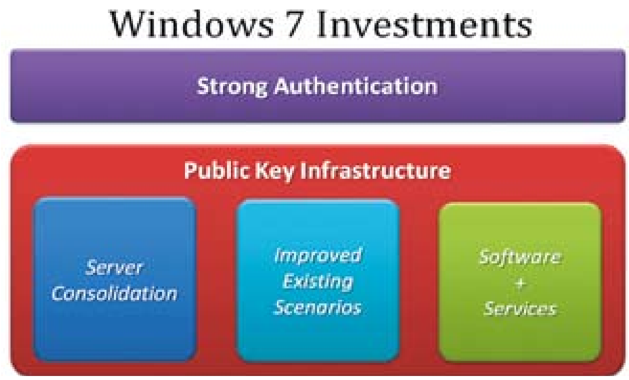


Figure 1 **The four core areas of PKI improvements**

Server consolidation

One of the predominant themes in IT over the past few years has been server consolidation. Simply put, this is about reducing the total footprint of your server computing environment while still meeting, or even expanding, your business objectives. The current global economy has made cost savings a top priority for many IT groups, and server consolidation can certainly be one component of that general strategy. While most organisations do not have large, absolute numbers of CAs, many do have more than they need solely based on certificate creation throughput. In other words, many organisations have CAs that are vastly under-utilised.

There are two primary reasons for this under-utilisation. First, some organisations may require separate CAs for regulatory or security policy reasons. For example, some customers have chosen to issue certificates to external parties from a completely separate CA than the ones that issue certificates to internal users and machines. In these cases, virtualising the CA on Hyper-V can eliminate the need for separate server hardware (though the CA itself must still be managed, even as a VM).

The second common reason is that autoenrollment has only been supported in intra-forest scenarios. Specifically, a CA has only been able to automatically enroll entities for certificates when those entities are part of the same forest that it is joined to. Even in cases where bi-directional forest level trusts exist, separate CAs have been required for each forest where autoenrollment is used.

One of the key new features in Windows Server 2008 R2 is the ability to perform autoenrollment across-forest trust relationships, creating the potential to drastically reduce the total number of CAs required in an enterprise. Consider a typical enterprise network that has already done some consolidation work and now has four forests: production, development, test, and edge. Prior to R2, if you wanted to provide autoenrollment on each forest, at least four issuing CAs were required, even though all the forests trusted each other. With R2, you can reduce the total number of CAs in this scenario down to one, having a single CA in one of the forests issue certificates to entities in all the other forests.

For environments with more complex multi-forest designs, the total reduction in CAs can be even more dramatic and provide an immediate return on investment for the upgrade to R2.

Cross-forest enrollment also makes it easier to extend a PKI during mergers and acquisitions, since certificates can start being provisioned to the newly acquired assets as soon as a forest trust is put into place. And since cross-forest enrollment is a purely server-side change, the enrollment can start without making any changes to the client machines and it works with older client operating systems, such as Windows XP.

So how does cross-forest enrollment work? To the end user, the experience is completely seamless. As with any other autoenrollment scenario, the user just gets the certificates with little or no interaction required on his part. End users will likely never know from what forest the CAs have come and they will not need to take any special actions to obtain the certificates.

For an IT professional, the basic building blocks are mostly the same as with traditional intra-forest autoenrollment. The key difference is that the CA is now able to process requests received from an external forest and retrieve metadata about the request from a trusted Active Directory.

This ability to receive and properly process a request from a trusted forest is the key new capability in R2 that enables this scenario to work. In addition to having an R2 CA and the bi-directional forest trust, certificate templates must be replicated between the forest holding the CA and all other forests that will enroll against it. Microsoft will provide a Windows PowerShell script to automate this replication, which should be done after every change to a template. In many cases, it will be a good idea to have this script run automatically as a scheduled task.

There are a few other smaller features that can help with server consolidation. One is that the CA now supports non-persistent requests – these are requests for certificates, typically short lived, that are not written into the CA's database. For example, consider Network Access Protection Health Registration Authorities. These systems may issue thousands of certificates each day that are only valid for a few hours. Maintaining all these requests in the CA database adds little value, but greatly increases the storage required. With R2, these requests can be configured to not be written to the database and this configuration can be made at either the CA or template level (see **Figure 2**).

Another feature designed to make server consolidation easier is support for Server Core. With R2, the CA role can be installed on Server Core, though no other AD CS (Active Directory Certificate Services) role service is available on Server Core. When installed on Server Core, the CA can be managed with either local command-line utilities, such as certutil, or by using the standard MMCs from a remote system. Note that if hardware security modules (HSMs) are used, you should ensure that the HSM vendor supports running their integration components on Server Core.

Improved existing scenarios

Windows 7 and R2 include a number of incremental improvements to existing features. First is a change to SKU differentiation for Certificate Templates. In prior releases of AD CS, advanced (version 2 and 3) Certificate Templates that enable the autoenrollment functionality required Enterprise edition CAs. In Windows Server 2008 R2, a Standard edition CA will support all template versions. R2 also introduces some improvements to the Simple Certificate Enrollment Protocol support. In R2, the SCEP component will support device renewal requests and password reuse.

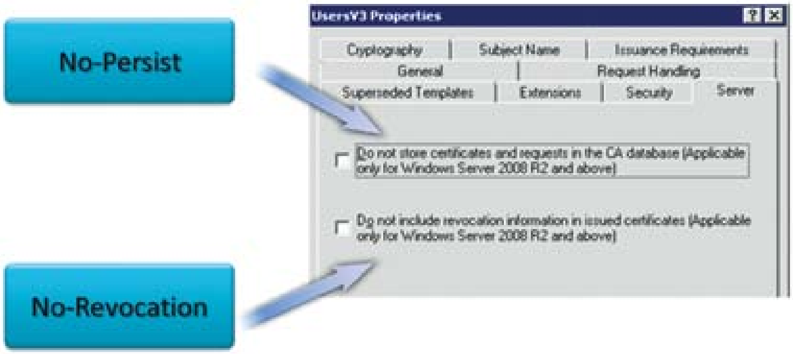
New to AD CS in R2 is a Best Practices Analyzer (see **Figure 3**). BPAs were created to provide an easy way for administrators to check their configurations against a database of best practices created and maintained by Microsoft feature teams. Data from customer support services indicate the majority of support calls on AD CS are caused by incorrect configurations, so the BPA should improve customer experiences by making it easier to verify that a CA is configured properly. The analyser will check for such issues as missing AIA (Authority Information Access) or OCSP pointers, certificates near expiration, and trust chaining problems.

In current releases of Windows, choosing a certificate for client authentication can be difficult for end users. When multiple certificates are valid for authentication, Windows doesn't make it easy for users to determine which one is the right one for a given usage. This leads to more help desk calls and increased customer support costs. In Windows 7, the certificate selection interface has been greatly enhanced to make it much easier to choose the right certificate for a given scenario. The list ordering has also been changed in order to assist in making smarter decisions by presenting the most likely certificate for a given scenario as the default choice. Finally, the selection UI now differentiates between certificates on smart cards and those stored on the file system and presents smart card certificates highest in the selection list, since they're more likely to be used. The differences are illustrated in the screenshots shown in **Figure 4**. Note that Internet Explorer 8 will make the improved filtering (but not UI changes) available on downlevel operating systems as well.

Software + services

During the Windows 7 design process, the team hosted a meeting with many of the top PKI users to brainstorm which areas should get attention in the new release. An overwhelming number of users indicated that it's too hard to manage certificates across organisational boundaries, such as between two separate companies that are business partners. Many also said that they see PKI as an ideal target for outsourcing, since it requires a specialised skill set to manage effectively. Windows 7 and Windows Server 2008 R2 will deliver a new technology that satisfies both these needs, making it easier to provision certificates across boundaries and opening new business models for hosted PKI solutions. This technology is HTTP enrollment.

HTTP enrollment is a replacement for the traditional RPC/DCOM-based protocol used for autoenrollment in previous releases (note that the RPC approach is still available in R2). However, HTTP enrollment is more than just an enrollment protocol – it's really a completely new approach to providing certificates to end entities, regardless of where they're located or whether they're a managed machine and with flexible authentication options. This new model eliminates many of the barriers found in traditional autoenrollment across organisational boundaries and provides a framework for third parties to easily provide



□ Do not store certificates and requests in the CA database (Applicable only for Windows Server 2008 R2 and above)

□ Do not include revocation information in issued certificates (Applicable only for Windows Server 2008 R2 and above)

Figure 2 **Choosing not to store certificates in the database**

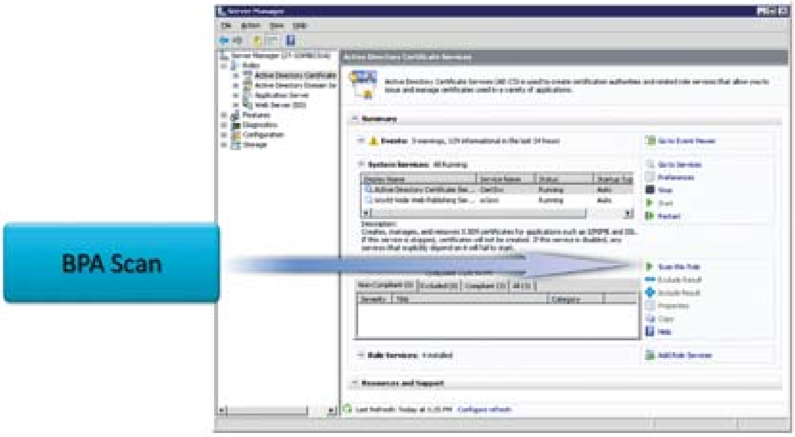


Figure 3 **Running the new Best Practices Analyzer**

autoenrollment services without requiring additional software on the clients.

HTTP enrollment implements two new HTTP-based protocols. The first protocol, known as Certificate Enrollment Policy Protocol, makes certificate templates available to users over HTTPS sessions. The end entities can come from machines in separate forests with no trust relationships and machines not even joined to a domain. Authentication uses Kerberos, user names/passwords, or certificates. The Enrollment Policy Protocol allows users to poll for templates and determine when to request certificates based on new or updated templates.

The Certificate Enrollment Service Protocol is an extension to WS-Trust. The protocol is used for obtaining certificates once the template information has been determined. It supports flexible authentication methods and uses HTTPS as its transport.

The example shown in **Figure 5** illustrates how this new enrollment model works.

- In Step 1, Certificate Templates are published from Active Directory to a server running the Certificate Enrollment Policy Web Service (a role service new to R2). The administrator publishing these templates is using the same MMCs and other tools with which they're already familiar.
- In Step 2, a client has polled the Web service via HTTPS to determine the list of templates available to enroll against. The client learns the URL for the Web service via Group Policy, script, or manual configuration. The client could be a domain-joined system, a system at a business partner, or a user's home system.
- In Step 3, the client has determined what templates he wants to enroll for and sends a request to the Certificate Enrollment Web Service to perform the actual enrollment.
- In Step 4, the server running the Enrollment Web Service sends the request to a CA for processing.
- In Step 5, the CA has looked up data about the requestor from Active Directory (such as his e-mail address or DNS name) that will be included in the issued certificate.
- In Step 6, the CA returns the completed certificate to the Enrollment Web Service.
- In Step 7, the Enrollment Web Service completes the transaction with the client via HTTPS and sends the signed certificate.

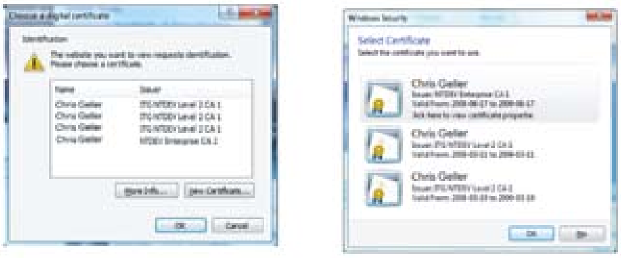
Flexibility was one of the key design principles in this new service and it's important to note how the design can be adapted to fit a diverse set of scenarios. Because the enrollment protocol is HTTPS, clients can easily enroll for certificates from anywhere, including behind corporate firewalls or from home ISP connections, without requiring a VPN. Because three different authentication methods are supported, clients can be joined to an organisation's internal domain, an untrusted domain of an external organisation, or no domain at all. Finally, because the server-side components are implemented as Web services, they can be installed separately from the CA and support segmented environments.

> End users will also benefit from Windows 7 PKI features that make it easier to use certificates in their daily work.

In addition to the classic scenario of enrolling end entities like users and desktops for certificates, HTTP enrollment also enables opportunities for provisioning certificates from trusted root CAs. Scenarios such as user S/MIME certificates, publicly facing Web servers, and other systems where implicit trust of certificates is important could all benefit from more autonomous enrollment. For example, many organisations with large numbers of Web servers maintain certificates manually, using lists of server names and expiration dates stored in Microsoft Office Excel workbooks. With HTTP enrollment, trusted root CAs can offer a service in which they provide certificates directly to these Web servers automatically, freeing the administrator from having to manually maintain the certificates on them. This combination of software and services allows organisations to choose the deployment models that fit their needs best, without having to design around network or organisational boundaries.

Strong authentication

Windows 7 includes the first in-box support for biometric devices with the Windows Biometric Framework (WBF). Initially focused on fingerprint-based authentication for consumer scenarios, WBF is designed to make biometrics an easier and more integrated experience for users. A unified driver model provides consistent user experiences across device types with support for Windows logon (both


Choose a digital certificate

Identification

The website you want to view requests identification. Please choose a certificate.

Name	Issuer
Chris Geller	ITG NTDEV Level 2 CA 1
Chris Geller	ITG NTDEV Level 2 CA 1
Chris Geller	ITG NTDEV Level 2 CA 1
Chris Geller	NTDEV Enterprise CA 2

Windows Security

Select Certificate

Select the certificate you want to use.

Chris Geller
Issuer: NTDEV Enterprise CA 1
Valid From: 2008-06-17 to 2009-06-17
Click here to view certificate properties

Chris Geller
Issuer: ITG NTDEV Level 2 CA 1
Valid From: 2008-03-11 to 2009-03-11

Chris Geller
Issuer: ITG NTDEV Level 2 CA 1
Valid From: 2008-03-18 to 2009-03-18

Figure 4 **A smarter way to present certificates**

local and domain), User Account Control (UAC), and autonomous device discovery. For enterprises, WBF provides a Group Policy–driven method to disable the framework for organisations that choose not to use biometrics. Enterprises can also choose to allow biometrics for applications, but not for domain logon. Finally, the enhanced device management can prevent device use in addition to simply preventing driver installation.

In addition to the biometrics improvements, Windows 7 also enhances user and administrator experiences for smart card scenarios. Smart cards are now treated as Plug and Play devices with Windows Update–based driver installation. The Plug and Play detection and installation process takes place before logon, meaning users who are required to log on with smart cards will be able to log on even in cases where the card has not been previously detected. Additionally, the installation does not require administrative privileges, making it suitable in least-privilege environments.

The smart card class mini-driver now includes NIST SP 800-73-1 support, so Federal agencies can use their PIV (Personal Identity Verification) cards without having to use additional middleware. The mini-driver also includes support for the emerging INCITS GICS (Butterfly) standard, providing a Plug and Play experience for those cards.

Windows 7 also introduces support for biometric-based smart card unlocking and includes new APIs to enable secure key injection. Finally, Windows 7 adds support for Elliptic Curve Cryptography (ECC) smart card certificates for both ECC certificate enrollment and for utilising those ECC certificates for logon.

Wrapping up

Windows 7 and Windows Server 2008 R2 contain some of the most important new PKI technology since Windows 2000 introduced automatic certificate requests. This new functionality makes PKIs easier and more efficient to manage, delivering a better experience for end users.

References

- **Introduction to the Windows Biometric Framework (WBF)**
  www.microsoft.com/uk/wbf
- **About Personal Identity Verification (PIV) of Federal Employees and Contractors**
  csrc.nist.gov/groups/SNS/piv/index.html
- **Windows Server PKI Home**
  microsoft.com/pki
- **Windows PKI Blog**
  blogs.technet.com/pki

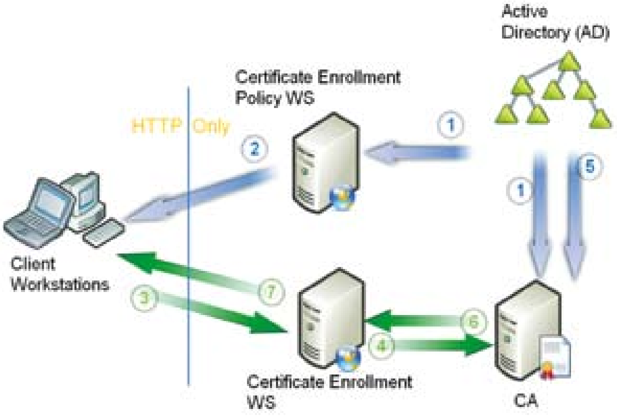


Figure 5 **The new enrollment model**

Windows 7 and Windows Server 2008 R2 include powerful new capabilities that make running a PKI more efficient while greatly enhancing the autoenrollment function. Cross-forest enrollment can dramatically reduce the total number of CAs required by an organisation and make it easier to manage PKI operations during mergers, acquisitions, and divestitures. The new Best Practices Analyser makes it easy for administrators to check for common configuration problems before outages occur. Capabilities such as support for Server Core and nonpersistent requests make it easier to tailor CA operations to specific organisational needs. And HTTP enrollment opens up new methods to automatically provision certificates across organisational and network boundaries.

End users will also benefit from Windows 7 PKI features that make it easier to use certificates in their daily work. The improved certificate selection interface makes it easier for users to choose the right certificate for a given purpose and successfully authenticate more quickly. Smart card improvements like Plug and Play–based driver installation and native support for card standards mean less time needs to be spent getting cards to work on user systems. Finally, the inclusion of native support for biometrics will provide a more consistent and seamless experience for both end users and administrators.

Check out the Beta if you haven't already and let us know what you think via the Feedback Tool or on our blog at: *blogs.technet.com/pki.*

JOHN MORELLO *has been with Microsoft since 2000. He spent five years in Microsoft Consulting Services where he designed security solutions for Fortune 500 corporations, governments, and militaries around the world. He's currently a Principal Lead Program Manager in the Windows Server Group. John has written numerous articles for* ***TechNet Magazine****, he has contributed to several Microsoft Press books, and he speaks regularly at conferences such as TechEd and IT Forum. You can read his team's blog at blogs.technet.com/WinCAT.*