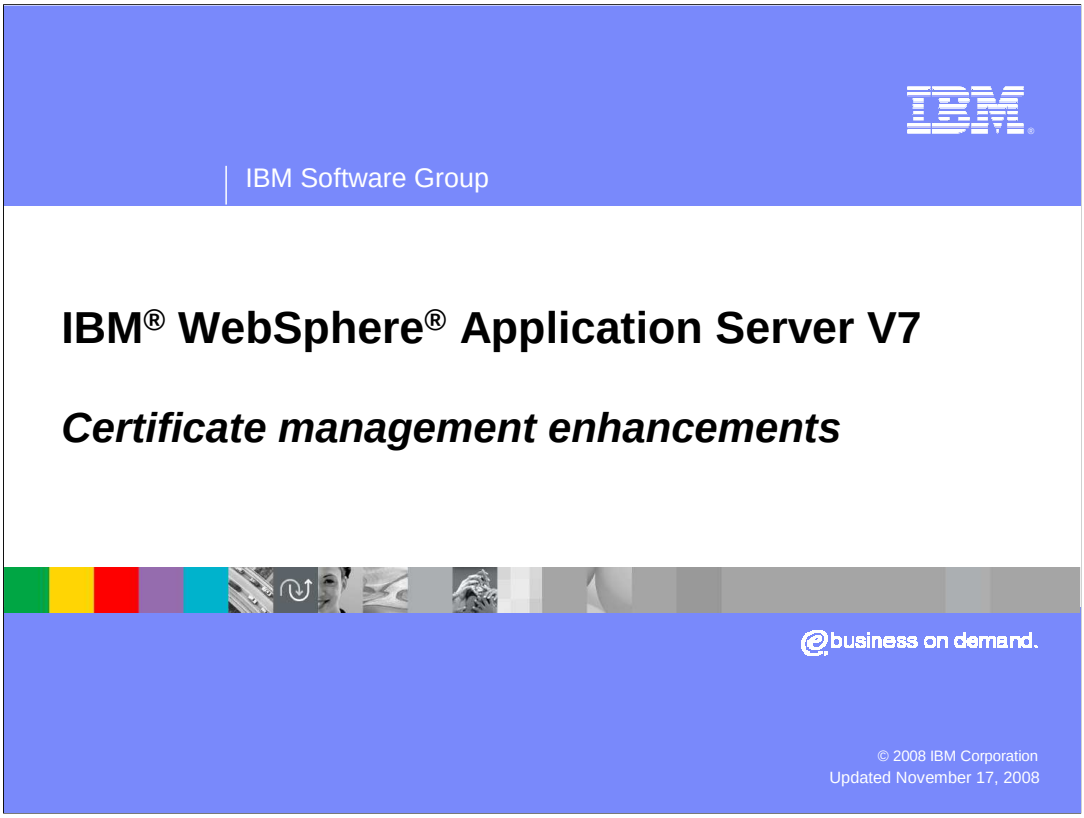

This presentation explains several enhancements to certificate management in WebSphere Application Server version 7.

For version 7, there are several enhancements to certificate management, including support for chained certificates and changes to profile creation that allow improved control over the certificates generated.

Section

Certificate management enhancements

This section explains the various enhancements to certificate management in WebSphere Application Server V7.

Certificate management enhancements

- Added ability to create chained personal certificates
  - Personal certificate signed by another personal certificate
  - More scalable solution for flexible management certificates
- Added ability to make certificate decisions at profile creation time (advanced path only)
- Added ability to generate personal certificates by connecting directly to internal Certificate Authority (CA) servers
  - More robust solution for customers who may have CA servers
- Writeable SAF Key rings

WebSphere Application Server version 7 has added the ability to create chained personal certificates, which are personal certificates that have been signed by another personal certificate. This is used to provide a scalable certificate solution for signing personal certificates in a flexible management environment. During the advanced path profile creation, you have more options to choose for certificate creation. Personal certificates can also now be created by directly connecting to an internal certificate authority. There are also writeable SAF key rings in version 7.

Chained personal certificates

- A chained certificate is a personal certificate signed with another certificate known as a root certificate
- The public key of the root certificate will be added to the common trust store (trust.p12 in the cell directory)
  - This should provide all the trust necessary for all servers to communicate with each other
  - These root certificates need a longer lifespan (~20 years by default) to avoid the need to replace signers in the trust stores
- The personal certificates signed by these root certificates have a shorter lifetime (one year) and unique private keys, thus the communications remain secure
  - Personal certificates signed by a root certificate can be replaced without any impact to communication if the client has the signer from the root certificate

A chained certificate is a personal certificate that has been signed with another certificate referred to as a root certificate. The root certificate can be used to assert trust when the personal certificate has expired. The root certificates will have a longer lifespan to avoid the need to replace the signers in trust stores, so they will typically have a lifespan of 20 years. The public key for the root certificate is added to the common trust store, this is used to provide trust between servers that communicate with each other. The personal certificates signed by the root certificates typically have a shorter lifespan and unique private keys, insuring that communications remain secure. As long as the client has the signer for the certificate, personal certificates signed by the root certificate can be replaced without impacting communications.

Default certificates

- The default personal certificate, the one used in the server key.p12 file, will be signed by another certificate, the root certificate
  - The default root certificate is a self-signed certificate that will have a default life span of 20 years
- The server's default personal certificate will have a life span of one year and will be signed by the default root certificate
  - The personal certificate can be replaced with the same root certificate without affecting any communications
  - The creation of the root certificate and a server's personal certificate will take place at profile creation time
- These certificates are meant for internal WebSphere Application Server communications
  - Not meant to act as a CA to distribute certificates to application clients

In WebSphere Application Server version 7 the default personal certificate is signed by the default root certificate. The default personal certificate is stored in the server's key.p12 file and will have a lifespan of one year. The root certificate will have a lifespan of 20 years. Both certificates are created at profile creation time and can be configured at that time by using the advanced profile creation path. Both of these certificates are meant to be used for internal WebSphere Application Server communications; they are not meant to act as a certificate authority and used to distribute certificates to application clients. That should still be done as it has been in the past.

Profile creation

- During 'Advanced Path' profile creation, users will be presented with the ability to make certificate decisions
  - Certificate DN Customization and life span
  - Import custom default and root certificates
  - Setting default password for key stores
- Allows for fully customizable certificate environments

The personal certificates can be configured during profile creation time, when using the advanced path profile creation option. Various options can be configured, including; certificate distinguished names and life spans, the ability to import custom default personal or root certificates, and setting the default key store passwords. The aim is to allow for full customized certificate environments at installation time.

Certificate deletions

- Personal certificates that are deleted are moved to a recovery key store
  - DmgrDefaultDeletedStore for a deployment manager
  - NodeDefaultDeletedStore for an application server
- Once in the recovery key store users will have the option to recover that certificate or to permanently delete the personal certificate
  - The certificate can be restored by using the importCertificate or exportCertificate tasks
- When a personal certificate is deleted from the recovery key store then it is permanently deleted
- The recovery key store will be emptied when the certificate expiration monitor is run

Another new change in WebSphere Application Server version 7 has to do with certificate deletions. Now personal certificates that are deleted are moved to a recovery key store. There is a different recovery key store for a deployment manager and an application server. Once certificates have been moved to the recovery key store they can either be recovered, or permanently deleted. When a certificate is deleted from the recovery key store it is permanently removed and cannot be recovered. In order to insure the recovery key store doesn't hold certificates forever it will be emptied when the certificate expiration monitor is run.

Additional enhancements

- WSPKIClient interface allows users to make certificate request to a certificate authority (CA)
  - More robust solution for customers who may have CA servers
- Writable SAF keyring support
  - Certificate write operations can be performed using the administrative console or scripting as with file based key stores
  - Configurable when running z/OS® Release 1.9 or at z/OS Release 1.8 with APAR OA22287 - resource access control facility (RACF®) (or the APAR for your equivalent security product) and APAR OA22295 – SAF
- Added a key store to hold default trusted certificates
  - New key stores are generated with all signer certificates present in the key store

A new interface has been introduced to allow users to make certificate requests directly to a certificate authority; this is a more flexible option for customers who have their own certificate authority servers. z/OS has introduced a writable SAF keyring, where write operations can be performed through the administrative console or using scripts. Also a key store has been added to hold default trust certificates.

Summary

- Improvements to certificate management
  - Chained certificates
  - Importing certificates during profile creation
  - Recover deleted certificates

In summary, WebSphere Application Server version 7 has introduced several enhancements to certificate management. This includes adding support for chained personal certificates, importing certificates during profile creations, and the ability to recover deleted certificates.

Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send e-mail feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_WASv7_CertificateManagementEnhancements.ppt

This module is also available in PDF format at:
../WASv7_CertificateManagementEnhancements.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.

Trademarks, copyrights, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM RACF WebSphere z/OS

A current list of other IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements or changes in the products or programs described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.