z/OS 3.1 IBM Education Assistant

Solution Name: Remove private key of expired certificate, Disable Directory Name format in CRL Distribution Point extension

Solution Element(s): PKI Services

July 2023

Agenda

- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

Objectives

- Provide continuous certificate enhancements to fulfil customer requirements
- At the end of this presentation, you would understand the support from:
  - PKI Services Remove private key of expired certificate
  - PKI Services Disable Directory Name format in CRL Distribution Points extension

PKI Services Remove private key of expired certificate

Overview

- PKI Services supports two ways of requesting certificates using the key through the supplied Certificate Signed Request (CSR) or letting PKI Services generate the keypair from the ICSF's PKCS#11 token support and store the key related objects in the Key Token dataset (TKDS)
- Currently PKI Services provides options to remove certificates/keys after a specified period after expiration
  - expired certificates (keypair was generated by the requestor)
  - expired certificates and keys (keypair was generated by PKI)
- Some customers would like to keep the expired certificates but have the keys removed from the TKDS

Overview (cont'd)

- Who (Audience)
  - z/OS customers who request certificates with keys generated by PKI Services and store in the TKDS
- What (Solution)
  - In this release, PKI Services will provide a new option for expired certificates with PKI generated keys
    - just remove the certificate related objects (which include the private key) in the TKDS token without removing the certificate in the PKI backend store, Issued Certificate List (ICL)
- Wow (Benefit / Value, Need Addressed)
  - This new option allows greater flexibility to certificate and key management so that customer can utilize the TKDS storage according to his/her need.
  - This satisfies requirement RFE 97489

Usage & Invocation

- To enable this option, specify the new keyword **RemoveExpiredKeysOnly** in the PKI Services configuration file, pkiserv.conf.
- For example, if you want to remove the keys of those certificates 4 weeks after the expiration date, specify:
  - RemoveExpiredKeysOnly = 4w

Interactions & Dependencies

- Software Dependencies
  - No
- Hardware Dependencies
  - No
- Exploiters
  - Customers who want PKI Services to generate the keypair for the certificate

Upgrade & Coexistence Considerations

- While there are no new migration and coexistence issues introduced by this initiative, in a sysplex environment:
  - the new option RemoveExpiredKeysOnly should not be enabled until all members are brought up to the same level

Installation & Configuration

- Update the pkiserv.conf file with RemoveExpiredKeysOnly specification (refer to slide 8)

PKI Services Disable Directory Name format in CRL Distribution Points extension

Overview

- When PKI Services creates a certificate, it includes the Certificate Revocation List Distribution Points extension (CRLDP) on it, if this extension is required according to the configuration in pkiserv.conf
- There are two different formats in CRLDP when this extension is created:
  1. Directory Name format: prepending the CRL name to the CA's Subject Distinguished Name, for example
     - if the CA's subject name is OU=My internal CA, O=My Company, C=US, the CRLDP extension on the certificate would be CN=<CRL name>, OU=My internal CA, O=My Company, C=US
  2. URI format in the form of http:// or ldap://, for example
     - URL=http://mycompany.com/PKIServ/crls/CRL1.crl
     - URL=ldap://mycompany.com/cn=CA,dc=example,dc=com?certificateRevocationList;binary
- Currently PKI Services **always** creates the Directory Name format when the URI format is created
- There is no way to exclude the Directory Name format

Overview (cont'd)

- Who (Audience)
  - z/OS customers who request certificates from PKI Services to include the CRLDistributionPoints extension
- What (Solution)
  - In this release, we will provide an option to disable the creation of the Directory Name format when the CRLDistributionPoints extension is created
- Wow (Benefit / Value, Need Addressed)
  - Some certificate validation program can't handle the Directory Name format in the certificate's CRLDP extension. This new option allows the exclusion of this format so that PKI Services issued certificates can be utilized by different applications accordingly
  - This satisfies requirement RFE 233479

Usage & Invocation

- To enable this option, specify the new keyword **CRLDistDirectoryName** with value **F** in the PKI Services configuration file, pkiserv.conf.
- For example, if you want to exclude the Directory Name format in the CRLDistributpoints extension, specify:
  - CRLDistDirectoryName = F
- If this keyword is not specified or specified with value T, the Directory Name format will be included as before
- When this option takes effect, all the new certificates will be created without this format in the CRLDP extension.
  - Note this new option won’t affect the previous issued certificates

Interactions & Dependencies

- Software Dependencies
  - No
- Hardware Dependencies
  - No
- Exploiters
  - PKI Services customers who wants to exclude the Directory Name format in the CRLDP extension in the certificate

Upgrade & Coexistence Considerations

- While there are no new migration and coexistence issues introduced by this initiative, in a sysplex environment:
  - the new option CRLDistDirectoryName = F should not be specified until all systems are brought up to the same level

Installation & Configuration

- Update the pkiserv.conf file with CRLDistDirectoryName = F specification (refer to slide 14)

Summary

- Now you would understand the support from:
  - PKI Services Remove private key of expired certificate
  - PKI Services Disable Directory Name format in CRL Distribution Point extension
  - Both the supports require an update on the pkiserv.conf file. If no updates are made, the existing behavior continues

Appendix

- Publication references
  - Cryptographic Services PKI Services Guide and Reference