z/OS V2.5 IBM Education Assistant

Solution Name: RACF and PKI Fingerprint support, PKI Trust Policy plugin removal

Solution Element(s): RACF, PKI Services

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:
  - RACF Fingerprint support
  - PKI Services Fingerprint support
  - PKI Services Trust Policy plugin removal

RACF Fingerprint support

Overview

- To know the inventory of the certificates and know how they are being used are two of the many pain points from the customers
- Fingerprint is a HASH value over the entire certificate, it is a unique representation of a certificate
- We can make use of it to track the whole life cycle of the certificate in a z/OS system and see if the same certificate is being used on the other applications or platforms
- It involves all the major components that handle certificates. RACF is one of them.

Overview

- Who (Audience)
  - z/OS customers from various certificate enhancement requirements
- What (Solution)
  - RACF provides certificate fingerprint, a SHA256 HASH value, from:
    - RACDCERT command
    - SMF records for RACDCERT, R_datalib and initACEE functions
- Wow (Benefit / Value, Need Addressed)
  - The number of certificates used on z/OS is growing. The same certificate may exist across different applications or platforms. Administrator needs a way to identify them
  - Having a clear view on the certificate inventory and understanding what certificates are being used helps the better implementation on security policy based on certificates

Usage & Invocation

- RACDCERT LIST, LISTCHAIN and CHECKCERT will calculate and display the SHA256 fingerprint in colon separated printable hex format. For example,

```
Digital certificate information for user CHOI:
  Label: samplecert
  Certificate ID: 2QbmxsPI1smJl4OFmaPy
  Status: TRUST
  Start Date: 2019/08/02 00:00:00
  End Date:   2024/08/02 23:59:59
  Serial Number:
       >05<
  Issuer's Name:
     >CN=sampleCA.O=Test.SP=Poughkeepsie.C=US<
  Subject's Name:
    >CN=samplecert.O=Test.SP=Poughkeepsie.C=US<
  Subject's AltNames:
    IP: 127.0.0.5
    EMail: sample at us.ibm.com
    Domain: www.ibm.com
```

```
Signing Algorithm: sha2RSA
 Key Usage: HANDSHAKE
 Key Type: RSA
 Key Size: 2048
 Private Key: Yes
 PKDS Label: SAMPLECERT
 Certificate Fingerprint(SHA256):
    9C:3E:4A:FC:C4:91:DF:D3:32:F3:08:9B:85:42:E9:46:
    17:D8:93:D7:FE:94:4E:10:A7:93:7E:E2:9D:96:93:DE
 Ring Associations:
   Ring Owner: CHOI
   Ring:
    >testring<
```

Usage & Invocation

- Enable SMF recording to store the certificate fingerprint
  - For RACDCERT command (event code 66)
    - ADD, ALTER, BIND, CONNECT, DELETE, EXPORT, GENCERT, GENREQ, IMPORT, REKEY, REMOVE, ROLLOVER, UNBIND.
  - For R_Datalib callable service (event code 84)
    - DataPut, DataAlter, DataRemove
  - For initACEE callable service (event code 67)
    - register, deregister
- DBUnload will calculate the fingerprint value when it unloads a certificate
  - Fingerprint will be in the unload output even for previously existing certificates from earlier releases
- A sample $CERT01 in IRRICE is provided to display all the certificates in the RACF DB with the following information:
  - Owner
  - Label
  - SHA256 Certificate Fingerprint
  - Issuer Distinguished Name
  - Subject Distinguished Name
  - Signature Algorithm

Interactions & Dependencies

- Software Dependencies
  - No
- Hardware Dependencies
  - No
- Exploiters
  - Customers who use RACDCERT, R_datalib and initACEE.

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Sysplex must be at the new z/OS level:
  - No
- List any toleration/coexistence APARs/PTFs.
  - No
- List anything that doesn't work the same anymore.
  - No

Installation & Configuration

- N/A

PKI Services Fingerprint support

Overview

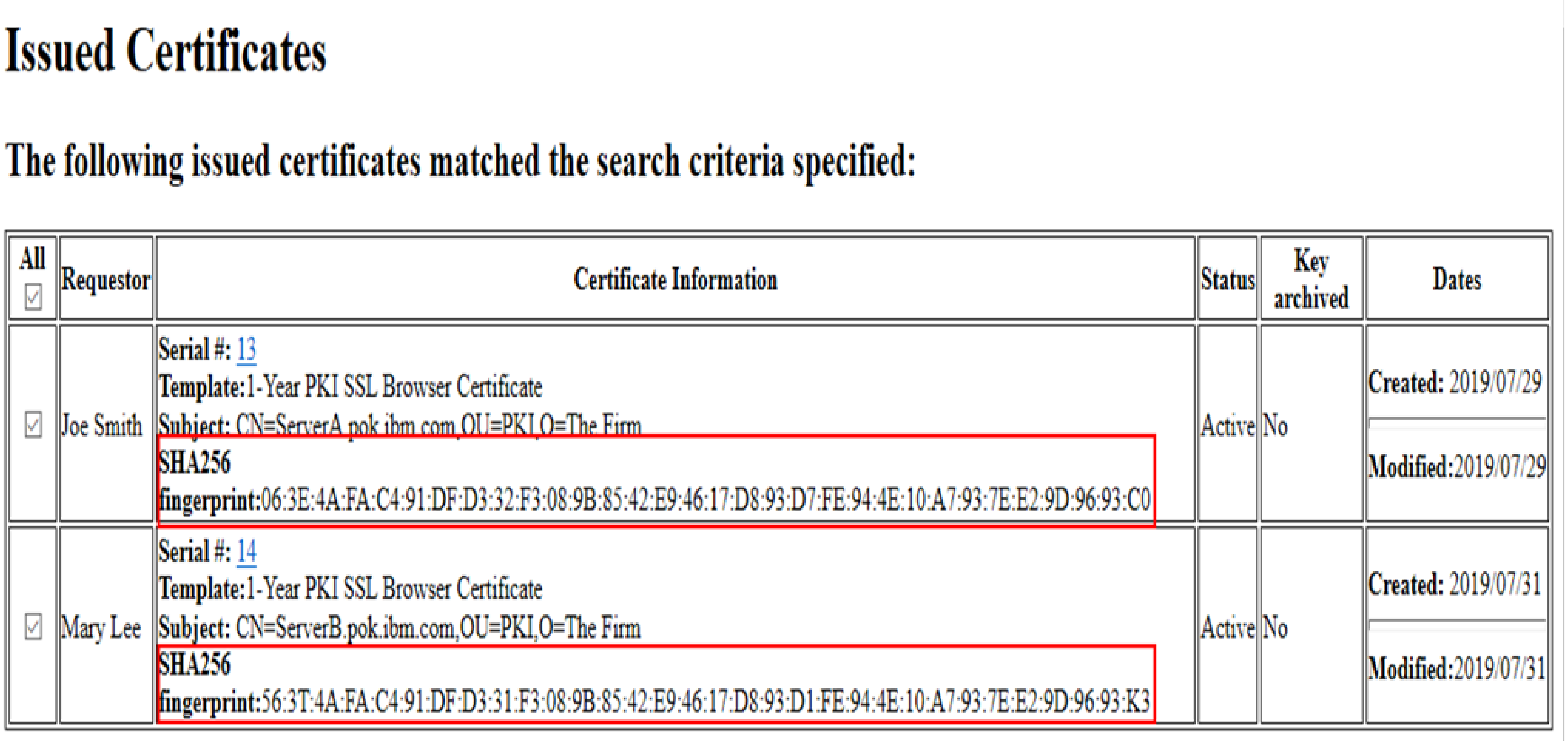
- To know the inventory of the certificates and know how they are being used are two of the many pain points from the customers
- Fingerprint is a HASH value over the entire certificate, it is a unique representation of a certificate
- We can make use of it to track the whole life cycle of the certificate in a z/OS system and see if the same certificate is being used on the other applications or platforms
- It involves all the major components that handle certificates. PKI Services is one of them.

Overview

- Who (Audience)
  - z/OS customers from various certificate enhancement requirements
- What (Solution)
  - PKI Services stores certificate fingerprint, a SHA256 HASH value, in:
    - its certificate backend store's (ICL) header
    - SMF records for PKI functions that generate, revoke (suspend), renew and export a certificate
  - Provide the capability to query a certificate created by PKI Services using the fingerprint as input
- Wow (Benefit / Value, Need Addressed)
  - The number of certificates exist on z/OS is growing. The same certificate may exist across different applications or platforms. Administrator needs a way to identify them
  - Having a clear view on the certificate inventory and understanding what certificates are being used helps the better implementation on security policy based on certificates

Usage & Invocation

- Fingerprint is displayed with the other existing information from the result page of the query



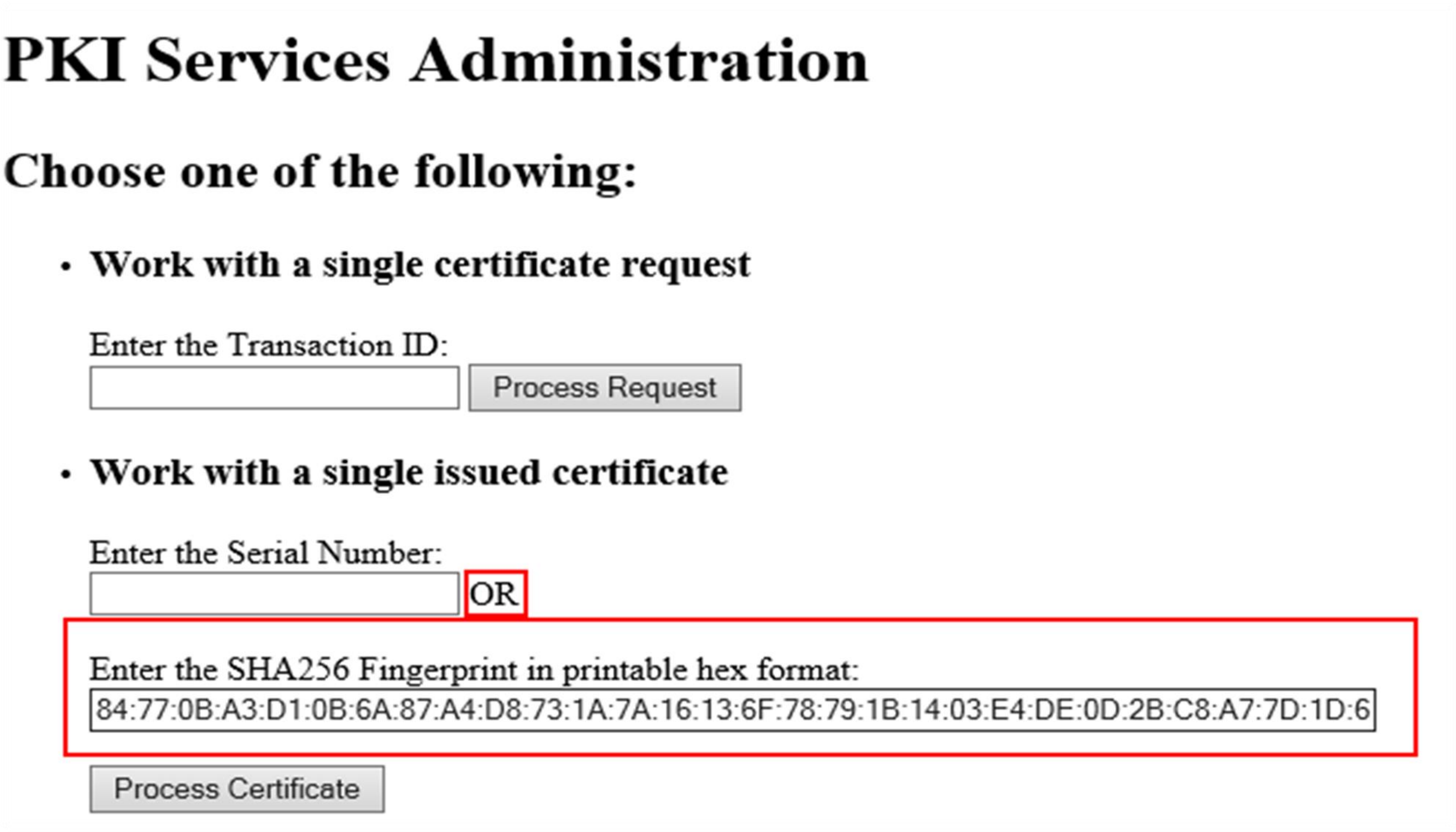
Issued Certificates

The following issued certificates matched the search criteria specified:

All ☑	Requestor	Certificate Information	Status	Key archived	Dates
☑	Joe Smith	**Serial #:** 13 **Template:**1-Year PKI SSL Browser Certificate **Subject:** CN=ServerA.pok.ibm.com,OU=PKI,O=The Firm **SHA256** **fingerprint:**06:3E:4A:FA:C4:91:DF:D3:32:F3:08:9B:85:42:E9:46:17:D8:93:D7:FE:94:4E:10:A7:93:7E:E2:9D:96:93:C0	Active	No	**Created:** 2019/07/29 **Modified:**2019/07/29
☑	Mary Lee	**Serial #:** 14 **Template:**1-Year PKI SSL Browser Certificate **Subject:** CN=ServerB.pok.ibm.com,OU=PKI,O=The Firm **SHA256** **fingerprint:**56:3T:4A:FA:C4:91:DF:D3:31:F3:08:9B:85:42:E9:46:17:D8:93:D1:FE:94:4E:10:A7:93:7E:E2:9D:96:93:K3	Active	No	**Created:** 2019/07/31 **Modified:**2019/07/31

Usage & Invocation

- Fingerprint can be used as a search input



PKI Services Administration

Choose one of the following:

- Work with a single certificate request

Enter the Transaction ID:

- Work with a single issued certificate

Enter the Serial Number:

OR

Enter the SHA256 Fingerprint in printable hex format:

84:77:0B:A3:D1:0B:6A:87:A4:D8:73:1A:7A:16:13:6F:78:79:1B:14:03:E4:DE:0D:2B:C8:A7:7D:1D:6

Usage & Invocation

- Enable SMF recording to store the certificate fingerprint
  - For R_PKIServ callable service
    - RPKIGENC (event code 69)
    - RPKIEXPT (event code 70)
    - RPKIUPDC (event code 74)
    - RPKISCEP (event code 83)
    - PKIAURNW (event code 85)

Usage & Invocation

- **Use utility iclview to view the fingerprint in ICL, for example**

```
Iclview –d \'pkisrvd.vsam.icl\'
```

```
Cert 2: Joe Smith
    ISSUED (Issued certificate)
    Issued at 2019-07-29 18:09:46
    Last changed 2019-07-29 18:09:46
    Subject: CN=ServerA.pok.ibm.com,OU=PKI,O=The Firm
    Issuer: OU=Master CA,O=IBM,C=US
    Requester: Joe Smith
```

```
ApplData: 1YBSSL
   Serial Number: 13
   Email flag: Off
   AutoRenew flag: Not Set
   Additional flags Set:
   KeyID:
   Validity: 2019/07/29 00:00:00 - 2020/07/27 23:59:59
   Revocation Information Location: Distribution Point 1
   SHA256 Fingerprint: 06:3E:4A:FA:C4:91:DF:D3:32:F3:08:9B:85:42:E9:46:
                       17:D8:93:D7:FE:94:4E:10:A7:93:7E:E2:9D:96:93:C0
```

Interactions & Dependencies

- Software Dependencies
  - No
- Hardware Dependencies
  - No
- Exploiters
  - PKI Services customers

Upgrade & Coexistence Considerations

- If you want to upgrade PKI Services from an older release to exploit the fingerprint support, you need to perform the following actions based on the backend type:
  - VSAM backend
    - Run IKYCVSV2 to create the new VSAM datasets with additional alternate index for the certificate fingerprint field
    - Stop PKI after all the requests are completed*
    - Run the conversion utility vsamconv
    - Update pkiserv.conf to specify the DBVersion to 2 and point to the new VSAM datasets*
    - Start PKI*
  - DB2 backend
    - Run IKYCDBV2 to create the new DB2 ObjectStore and ICL tables
    - Run IKYSBIND to build the new package with a new name
    - Stop PKI after all the requests are completed*
    - Run the conversion utility db2conv
    - Update pkiserv.conf to specify the DBVersion to 2*
    - Start PKI*

* If running in sysplex, make sure the action is performed on all the members

Installation & Configuration

- Update pkiserv.conf to use the fingerprint support

```
[ObjectStore]
# …
# Specify one of the following:
#      DBVersion=0
#      DBVersion=1
#      DBVersion=2
DBVersion=2
 …
# If DBType is VSAM, configure the following
additional keywords:
#      ObjectDSN                  ICLDSN
#      ObjectStatusDSN            ICLStatusDSN
#      ObjectRequestorDSN         ICLRequestorDSN
#      ObjectSCEPTidDSN           ICLSCEPTidDSN
#      ObjectTidDSN               ICLCertFprintDSN
# Data set name of the VSAM object store PATH for the requestor
# alternate index
#
ObjectRequestorDSN='pkisrvd.vsam.ost.requestr'

# Data set name of the VSAM object store PATH for the SCEP Transaction
# ID alternate index
#
#ObjectSCEPTidDSN='pkisrvd.vsam.ost.sceptid'
```

```
# Data set name of the VSAM issued certificate list
(ICL) base CLUSTER
#
ICLDSN='pkisrvd.vsam.icl'

# Data set name of the VSAM ICL PATH for the status
alternate index
#
ICLStatusDSN='pkisrvd.vsam.icl.status'

# Data set name of the VSAM ICL PATH for the
requestor alternate index
#
ICLRequestorDSN='pkisrvd.vsam.icl.requestr'

# Data set name of the VSAM ICL PATH for the SCEP
Transaction ID
# alternate index
#
ICLSCEPTidDSN='pkisrvd.vsam.icl.sceptid'
# Data set name of the VSAM ICL PATH for the
Certificate Fingerprint
# alternate index
#
ICLCertFprintDSN='pkisrvd.vsam.icl.fprt'
```

PKI Services Trust Policy Plugin Removal

Overview

- Follow IBM’s announced decision in V2R4 RFA: z/OS V2.4 is planned to be the last release to support OCSF(Open Cryptographic Services Facility) and its plug-ins, PKITP(PKI Services Trust Policy) is one of them
- z/OS PKI Services will no longer include any of the Trust Policy codes starting from V2R5

Overview

- Who (Audience)
  - z/OS customers who have programs calling PKI Trust Policy for certificate validation
- What (Solution)
  - Remove the Trust Policy code from PKI Services
  - There is better alternative to perform the same functionality provided by System SSL's APIs
- Wow (Benefit / Value, Need Addressed)
  - Have a simpler validation program through System SSL APIs without installing any CDSA framework

Usage & Invocation

- N/A

Interactions & Dependencies

- Software Dependencies
  - N/A
- Hardware Dependencies
  - N/A
- Exploiters
  - N/A

Upgrade & Coexistence Considerations

- Make sure you replace the Trust Policy calls in the certificate validation program

Installation & Configuration

- N/A

Summary

- Now you should understand the support from:
  - RACF Fingerprint support
  - PKI Services Fingerprint support
  - PKI Services Trust Policy Plugin Removal

Appendix

- Publication references
  - Security Server Command Language Reference
  - Security Server Callable Services
  - Security Server Macros and Interfaces
  - Cryptographic Services PKI Services Guide and Reference