IEA on PKI and NAS(Kerberos) for z/OS V2R3

Element/Component: PKI Services and NAS

Agenda

- Trademarks
- Session Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Migration & Coexistence Considerations
- Installation
- Session Summary
- Appendix

Trademarks

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

Session Objectives

- Digital certificates has been growing. Provide continuous enhancements to fulfill customer requirements
- Fulfill product FIPS Certification for PKI Services and Kerberos (NAS)
- At the end of this presentation, you should have an understanding of the support from:
  - PKI Services:
    - PKI DB2 Enhancement
    - PKI Liberty Support
    - PKI SCEP enhancement
    - PKI FIPS Support
  - NAS:
    - NAS FIPS Support

PKI DB2 Enhancement

Overview

- Problem Statement / Need Addressed
  - PKI Services maintains two databases, object store (OST) and issued certificate list (ICL) containing information about certificate requests issued certificates.
  - The databases can be implemented using the VSAM datasets or the DB2 tables.
  - When PKI Services starts, it will check if DB2 is available. It will stop initialization if DB2 is not available. But after the initialization PKI Services is not aware of the unavailability of DB2 and keeps on processing with failure.
- Solution
  - In this release we will enable PKI Services to shut down when DB2 is not available or to wait for DB2 to come back to resume its functions.

Overview

- Benefit / Values
  - Enable PKI to report DB2 issues ASAP and resume operation automatically once the DB2 issue is solved.

Usage & Invocation

- Update the configuration option DBWaitTime in pkiserv.conf
- For example, configure PKI Services to wait for 30 mins for DB2 to resume operation. If DB2 can't resume in 30 mins, PKI Services will shut down itself

```
# How long in days (d),  hours (h) or minutes (m) should PKI wait for

# DB2 to be available before it shuts down?

# The default value is 0m which indicates PKI does not wait. It stops

# when DB2 is not available. The maximum wait time is 1 day.

# This keyword will be ignored if DBType is not DB2.

DBWaitTime=30m
```

Interactions & Dependencies

- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - PKI customers who use DB2 as backend stores

Migration & Coexistence Considerations

None

Installation

None

PKI Liberty Support

Overview

- Problem Statement / Need Addressed
  - PKI Services provides web interface through two different approaches:
    - Rexx CGI execs supported by HTTP server
    - JavaServer pages (JSPs) supported by WebSphere Application Server (WAS). Some advantages:
      - Uses Java, a popular and flexible language
      - Uses XML, more familiar to web programmers
  - WAS is capable of hosting very sophisticated full-function applications but it consumes a lot of resources.
  - Original implementation in WAS relies on Enterprise JavaBeans (EJB). And restricts PKI Services from running multiple instances in one instance of WAS
- Solution
  - A light weight version called Liberty Profile is provided with WAS since WAS 8.5, which provides a subset of WAS functions.

Overview

- Benefit / Values
  - Lightweight - loading of functions is optimized to achieve an smaller footprint
  - Fast – server starts faster and application runs faster
  - Enable PKI Services to run multiple instances of CA domains with different sets of Java Server pages (JSP)
  - Good fit for PKI Services since it does not need the full traditional WAS capabilities and Liberty provides all the needed functions

Usage & Invocation

- Install Liberty server 8.5 or above
- Set the PKISERV_ENABLE_JSP environment variable to TRUE
- Copy the XML template file, pkitmpl.xml, and XML schema file, PKIServ.xsd to your runtime directory and customize them
- Update the generated server.xml according to the sample and customize it
- Authorize the Liberty users by specifying the roles in the server.xml or through the SAF EJBROLE class profiles <profile prefix>.<application name>.<role name> like
  - BBGZDFLT.PKI.PKIAdmin
  - BBGZDFLT.PKI.SAFuser
- Authorize the Liberty sever ID, PKI surrogate ID to use the PKI functions through the FACILITY class profiles IRR.RPKISERV.<PKI function>.<CA domain>
- Customize JSP files

Interactions & Dependencies

- Software Dependencies
  - Liberty 16.0.0.3 or higher
- Hardware Dependencies
  - None
- Exploiters
  - PKI customers who use JSPs for web interface

Migration & Coexistence Considerations

None

Installation

None

PKI SCEP Enhancement

Overview

- Problem Statement / Need Addressed
  - The Simple Certificate Enrollment Protocol (SCEP) allows you to securely issue certificates to large numbers of network devices using an automatic enrollment technique.
  - The network devices such as Cisco routers, must be SCEP-enabled and preregistered first.
  - To request certificates using SCEP, a SCEP requestor, eg, the Cisco router, must be preregistered to the CA with a client name and a passphrase and other optional information.
  - The original design for the SCEP request was to make use of the alternate index on the Requestor field for searching, just like the regular certificate requests.
  - The SCEP request contains a transaction ID which are used as the Requestor field in the certificate request.
  - The client name of the preregistration record is not saved.

Overview

- This creates a problem for the customers who have a lot of preregistration records with different SCEP clients.
- The client name is lost in the certificate request and subsequently lost in the certificate record .

- Solution
  - Retain the client name of the preregistration record in the SCEP request and SCEP certificate.

Overview

- Benefit / Values
  - This function will benefit PKI Services customers who needs a large number of SCEP certificates.

Usage & Invocation

- For VSAM backend – new instance
  - Run IKYCVSV1 to create the new VSAM datasets with additional alternate index for the SCEP transID field
  - Specify DBVersion= 1 in pkiserv.conf
  - Start PKI
- For DB2 backend – new instance
  - Run IKYCDBV1 to create the new DB2 ObjectStore and ICL tables
  - Run IKYSBIND to build the new package
  - Specify DBVersion= 1 in pkiserv.conf
  - Start PKI

Usage & Invocation

- For VSAM backend – existing instance
  - Run IKYCVSV1 to create the new VSAM datasets with additional alternate index for the SCEP transID field
  - Stop PKI
  - Run the conversion utility vsamconv
  - Update pkiserv.conf to specify the DBVersion to 1 and point to the new VSAM datasets
  - Start PKI
- For DB2 backend – existing instance
  - Run IKYCDBV1 to create the new DB2 ObjectStore and ICL tables
  - Run IKYSBIND to build the new package with a new name
  - Stop PKI
  - Run the conversion utility db2conv
  - Update pkiserv.conf to specify the DBVersion to 1
  - Start PKI

Interactions & Dependencies

- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - PKI customers who needs to create a lot of SCEP certificates

Migration & Coexistence Considerations

- List any toleration/coexistence APARs/PTFs.
  - OA52427
- Migration involves only those actions required to make the new system behave as the old one did.
  - None
- Coexistence applies to lower level systems which coexist (share resources) with latest z/OS systems.
  - z/OS 2.1, z/OS 2.2

Installation

None

PKI FIPS Support

Overview

- Problem Statement / Need Addressed
  - As of V2R2, System SSL supports FIPS140-2. The APIs can operate in FIPS mode 140-2 or non-FIPS mode.
  - In V2R3 System SSL item FP1188 is to enforce algorithm and key length restrictions in FIPS mode, as specified by NIST Special Publication SP800-131A
  - PKI Services uses most of the cryptographic functions from System SSL APIs and ICSF PKCS#11 APIs for the key generation related processing.
- Solution
  - PKI Services will provide the capability to execute securely in a mode that is designed to meet the NIST FIPS level supported by System SSL and ICSF PKCS#11 with their most current support as of V2R3.
  - A new environment variable _PKISERV_FIPS_LEVEL will be used in the pkiserv.envars file. This value will be utilized in all the System SSL calls implicitly and explicitly in the ICSF PKCS#11 key generation calls.

Overview

- Benefit / Values
  - This function will benefit customers who wants to run PKI Services in FIPS mode.

Usage & Invocation

- Start ICSF
- Specify the _PKISERV_FIPS_LEVEL value in the pkiserv.envars file corresponds to the System SSL FIPS level it supports:
  - _PKISERV_FIPS_LEVEL = 0, non FIPS mode (default)
  - _PKISERV_FIPS_LEVEL = 1, FIPS140-2
  - _PKISERV_FIPS_LEVEL = 2, SP800-131A with exception (Key generation, signature creation and encryption need to be performed with the required strength; digital signature verification, decryption can be performed with lower key strength)
  - _PKISERV_FIPS_LEVEL = 3, SP800-131A without exception (All operations have to be performed with the required strength)

Interactions & Dependencies

- Software Dependencies
  - ICSF
- Hardware Dependencies
  - None
- Exploiters
  - PKI customers who wants to run PKI Services in FIPS mode

Migration & Coexistence Considerations

None

Installation

None

NAS FIPS Support

Overview

- Problem Statement / Need Addressed
  - As of V2R2, System SSL supports FIPS140-2. The APIs can operate in FIPS mode 140-2 or non-FIPS mode.
  - In V2R3 System SSL item FP1188 is to enforce algorithm and key length restrictions in FIPS mode, as specified by NIST Special Publication SP800-131A
  - Currently Network Authentication Services uses cryptographic functions from
    - its own implementation
    - ICSF CCA APIs
    - System SSL APIs
  - Maintaining multiple implementation of the cryptographic functions is difficult and hard to obtain certifications needed
  - ICSF CCA APIs are not FIPS evaluated

Overview

- Solution
  - Remove internal software implementation and calls to the ICSF CCA callable services to use the ICSF PKCS#11 callable services for encrypt/decrypt/hashing when running in FIPS mode

Overview

- Benefit / Values
  - This will allow Network Authentication Service to run with FIPS evaluated cryptographic functions and remove the burden of maintaining multiple implementations of the cryptographic functions on the platform

Usage & Invocation

- Start ICSF
- For KDC
  - Specify the SKDC_FIPSLEVEL value in the envar file corresponds to the System SSL FIPS level it supports:
    - SKDC_FIPSLEVEL = 0, non FIPS mode (default)
    - SKDC_FIPSLEVEL = 1, FIPS140-2
    - SKDC_FIPSLEVEL = 2, SP800-131A with exception (Key generation, signature creation and encryption need to be performed with the required strength; digital signature verification, decryption can be performed with lower key strength)
    - SKDC_FIPS_LEVEL = 3, SP800-131A without exception (All operations have to be performed with the required strength)

Usage & Invocation

- For Kerberos client
  - Specify the fipslevel value in the krb5.conf file corresponds to the System SSL FIPS level it supports:
    - fipslevel = -1, FIPS mode not to be set (default)
    - fipslevel = 0, non FIPS mode
    - fipslevel = 1, FIPS140-2
    - fipslevel = 2, SP800-131A with exception (Key generation, signature creation and encryption need to be performed with the required strength; digital signature verification, decryption can be performed with lower key strength)
    - fipslevel = 3, SP800-131A without exception (All operations have to be performed with the required strength)

Interactions & Dependencies

- Software Dependencies
  - ICSF
- Hardware Dependencies
  - None
- Exploiters
  - Customers who want to run Kerberos in FIPS mode

Migration & Coexistence Considerations

None

Installation

None

Session Summary

- V2R3 provides continuous enhancements on PKI Services to fulfill customer requirements and fulfill product FIPS Certification for PKI Services and Kerberos (NAS)
- Now, you should have an understanding of the support from:
  - PKI Services:
    - PKI DB2 Enhancement
    - PKI Liberty Support
    - PKI SCEP enhancement
    - PKI FIPS Support
  - NAS:
    - NAS FIPS Support

Appendix

- Publication references
  - Cryptographic Services PKI Services Guide and Reference (*SA22-7693*)
  - Integrated Security Services Network Authentication Service Administration (SC23-6786)
  - Integrated Security Services Network Authentication Service Programming (SC23-6787)
- Websites
  - http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf
  - http://csrc.nist.gov/groups/STM/cmvp/standards.html
  - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1