# IBM Education Assistance for z/OS V2R2

Item:  PKI OCSP Currency
Element/Component:  PKI Services

Material current as of May 2015

# Agenda

- Trademarks
- Presentation Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Presentation Summary
- Appendix

# Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.

# Presentation Objectives

- Digital certificates usage has been growing
- Continuous enhancements to fulfill customer requirements
- Components on certificate support:
  - PKI Services
  -
- At the end of this presentation, you should have an understanding of the support from PKI Services for OCSP currency.

# Overview

- Problem Statement / Need Addressed
  - In RFC 2560, the Online Certificate Status Protocol (OCSP) requires server responses to be signed but does not specify a mechanism for selecting the signing algorithm to be used.
  - Currently z/OS PKI Services uses the same signing algorithm used for certificate and Certificate Revocation List (CRL) signing specified in the configuration file to sign the OCSP response.
  - RFC 6277 is an update to RFC 2560. It addresses the deficiency of the original design which may lead to interoperability failure when the server and the client support different signing algorithms
  - Support OCSP client implemented with System SSL

# Overview

- Solution
  - In the V2R2 release, PKI Services will be able to sign the OCSP response with the client specified signing algorithm through an extension in the request in the way documented by RFC 6227
  - PKI will choose the signing algorithm to sign the response as follows:
    - If the request contains the Preferred Signature Algorithms extension, PKI will pick the first one on the list.
    - If it is not on PKI's supported list or it does not meet the contemporary standards, eg. md-2WithRSAEncryption, md-5WithRSAEncryption, the next one will be used, so on and so forth.
    - If none of the specified algorithms is supported by PKI Services or meet the contemporary standard, PKI will use the one specified in the configuration file.

# Overview

- Benefit / Value
  - Facilitate interoperability between OCSP server and client in case they support different signing algorithms

# Usage & Invocation

- Specify the desire signing algorithm in the request created by the OCSP client sending to PKI Services to check for certificate revocation status
- Can use the enhanced System SSL support to create the OCSP client application

# Interactions & Dependencies

- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - OCSP clients, eg. System SSL applications

# Presentation Summary

- At the end of this presentation, you should have an understanding of the PKI Services support for OCSP currency.

# Appendix

- Publication references
  - Cryptographic Services PKI Services Guide and Reference (*SA22-7693*)
  - Security Server RACF Command Language Reference *(SA22-7687)*
  - Security Server RACF Administrator's Guide (SA22-7683)
  - Integrated Security Services Network Authentication Service Administration (SC23-6786)
  - Integrated Security Services Network Authentication Service Programming (SC23-6787)
- RFCs
  - RFC4120 – The Kerberos Network Authentication Service V5
  - RFC4556 - Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)
  - RFC2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
  - RFC6277 - Online Certificate Status Protocol Algorithm Agility