zSeries Security Update 2005

z/OS V1R7 Security Server

PKI Services
Certificate Extensions Improvement

Redbooks

International Technical Support Organization

Session Objectives

- Provide a quick overview of PKI Services prior to R7
- Understand the benefits of the new support
  - Digital Signature Algorithm (DSA) Key Support
  - Online Certificate Status Protocol (OCSP) Support
  - Enhanced CRL/ARL Distribution Point
  - Trust Policy Plugin Enhancement
  - New format in Subject Alternate Name Extension
  - Usability Enhancements
- Explain the enhancements made for R7

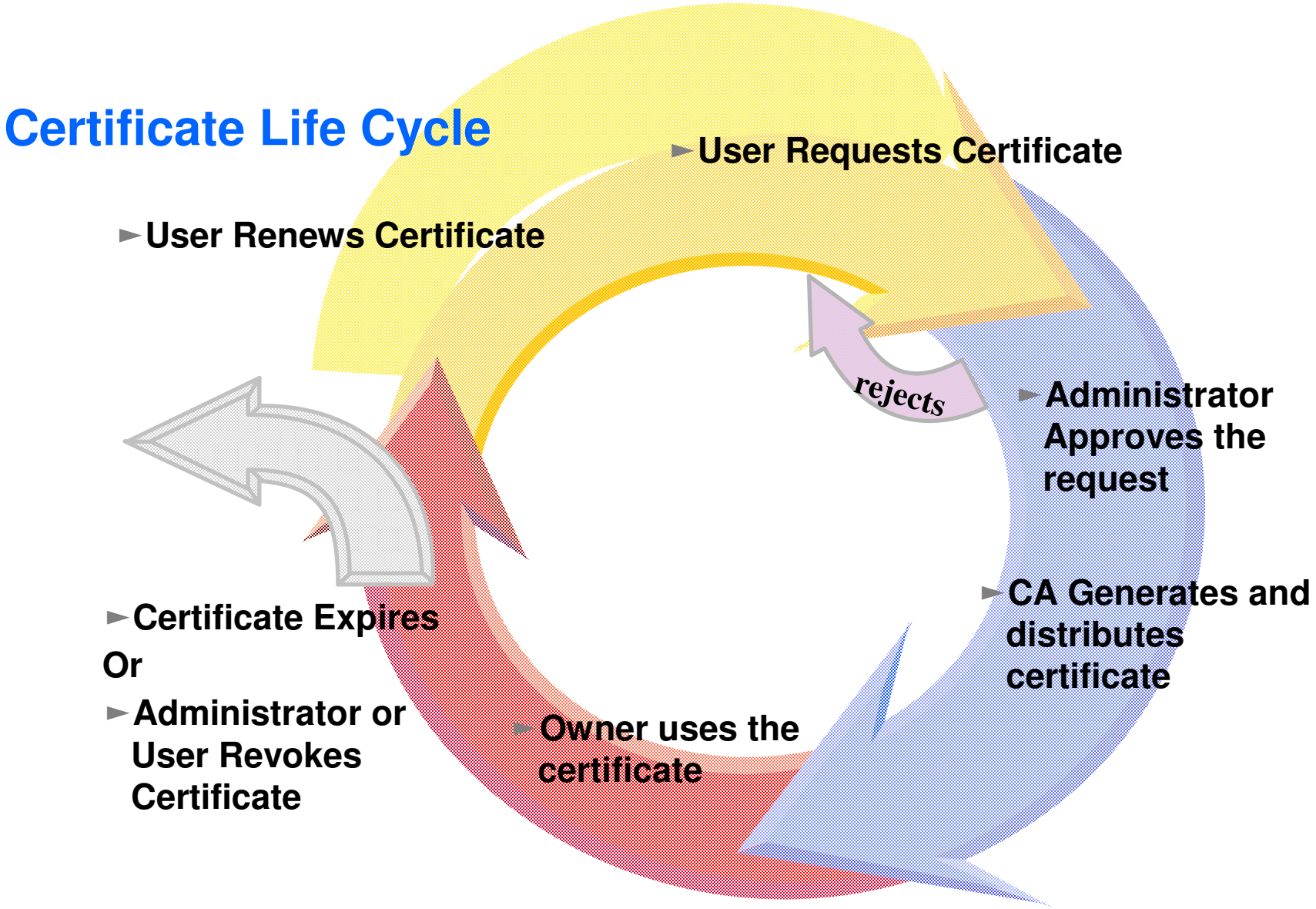
PKI Services Overview

- New component on z/OS since V1R3
- PKI Services allows customers to act as their own certificate authority (CA)
- Closely tied to RACF, but supports more functions than RACDCERT
- Full certificate life cycle management: request, create, renew, revoke
- Generation and administration of certificates via customizable web pages
- Support automatic or administrator approval process

PKI Services Overview…

- Create Certificate Revocation Lists (CRLs)
- Certificates and CRLs can be posted to LDAP
- Provides email notification for completed certificate request and expiration warnings
- Provides Trust Policy Plug-in as certificate validation service for z/OS applications

PKI Services Overview…



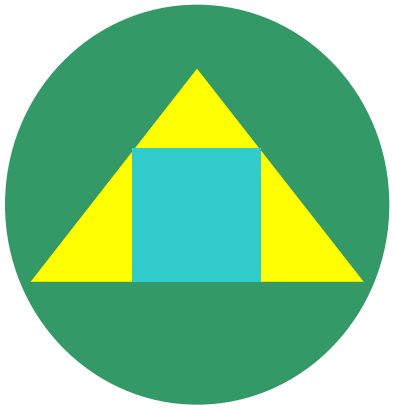
PKI Services Overview…

What's inside a Certificate?

Certificate Info

- version
- serial number
- signature algorithm ID
- issuer's name
- validity period
- subject's name
- subject's public key
- extensions

Certificate Signature

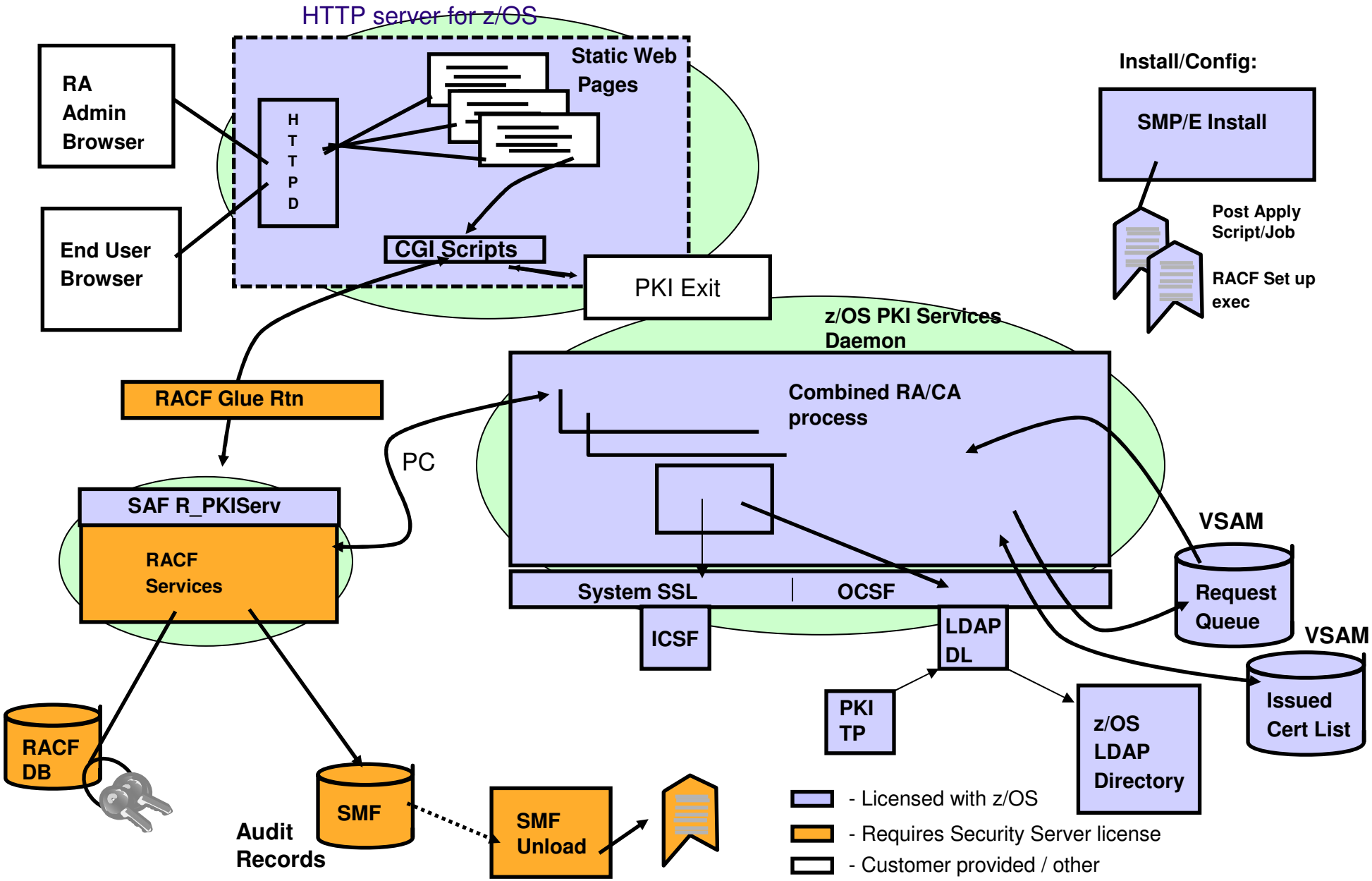


This is the hash/encrypt algorithm used in the signature

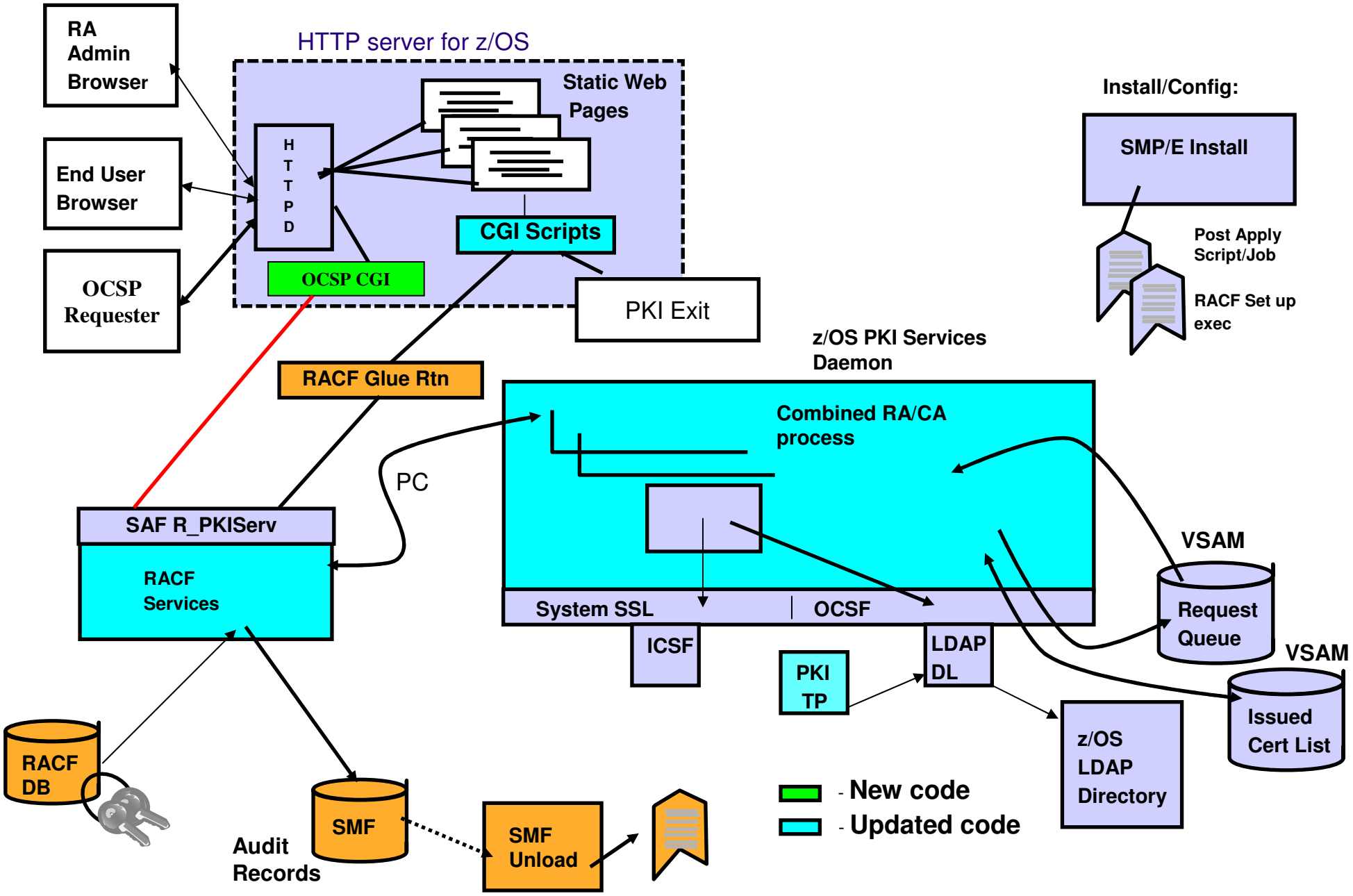
The certificate binds a public key to a subject

CA signs the above cert info by encrypting the hash with its private key

z/OS PKI Services Architecture prior to R7



z/OS V1R7 PKI Services Architecture



Usage & Invocation

- **For PKI Services**
  - Use the new configuration file and template file to get the new / enhanced certificate extensions support
- **For RACF**
  - Use the new keyword DSA in the RACDCERT GENCERT command

New / Enhanced support from R7

- **Requirement from Websphere J2EE**
  - Digital Signature Algorithm (DSA) Key Support
- **More competitive with other Certificate Authority products**
  - Enhanced CRL/ARL Distribution Point
  - Online Certificate Status Protocol (OCSP) Support
  - New format in Subject Alternate Name Extension
  - Trust Policy Plugin Enhancement
- **Easier to use**
  - Usability Enhancements

DSA Key Support

- **What is it?**
  - Digital Signature Algorithm is a signing algorithm defined by the US National Institute of Standards and Technology (NIST)

- **Benefit of having this support:**
  - Support products that use DSA keys, (eg. Websphere J2EE test suite)

DSA Key Support…

- **RACF can now generate DSA public/private key pairs for use in certificates**
  - Support through the changes on the RACDCERT Gencert command, RACDCERT ISPF Panels
  - It is mutually exclusive with ICSF and PCICC keywords
  - DSA key pair generation via BSAFE (software, no hardware support)
  - Max keysize for DSA keys is 2048 bits
  - Certificates with DSA keys may only be used for Signing and Signature Verification
- **PKI Services CA key can be a DSA key, and it can generate certificates on requests with DSA keys**
  - Support through the changes on the R_PKIServ callable service, and PKI Services daemon.

Enhanced CRL Distribution Point

- **What is it?**
  - CRL Distribution Point is an extension in the certificate
  - Prior to this release, its format is a Directory Name CN=CRL1,OU=RACF,C=IBM,C=IBM
  - Now it can also be in a URI format with LDAP or HTTP protocol (Secure formats like https or ldaps are not supported)
    - ldap://www.ibm.com/CN=CRL1,OU=RACF,O=IBM, C=IBM?certificateRevocationList
    - >http://www.ibm.com/PKIServ/crllist/CRL1.crl
- **Benefit of having this support:**
  - Certificate validation applications can know where to get the revocation list from the certificate itself.

Enhanced CRL Distribution Point…

- New configuration file keywords added in the [CertPolicy] section
  - **CRLDistURI*n*, CRLDistDirPath,** and **ARLDist**

- **CRLDistURI*n*** indicates the creation of the CRL Distribution Point extension with URI format, and its URI value, n >= 1. (You may have more than 1 URI value)

- **CRLDistDirPath** indicates the HFS directory where the distribution point CRL is stored for the http protocol

- **ARLDist** indicates whether a CRL Distribution Point extension should be created for CA certificates.

Online Certificate Status Protocol (OCSP)

- **What is it?**
  - A dynamic way to check the revoke status of a certificate
  - Certificate Revocation List is a static list of revoked certificates

- **Benefit of having this support:**
  - Certificate validation application can get the live revoke status of a certificate

Online Certificate Status Protocol (OCSP)…

- PKI Services daemon operates as an OCSP Responder for certificates it issued.
- R_PKIServ callable service updated with new function code, RESPOND to invoke PKI Services responder function.
- New CGI program, ***caocsp***, written to field http GET or POST OCSP requests, which calls the new R_PKIServ RESPOND callable service.

Online Certificate Status Protocol (OCSP)…

- Enabled/disabled by new configuration file keyword in the [CertPolicy] section, OCSPType. Acceptable values are ***basic*** or ***none***
  - OCSPType = none : The responder is disabled
  - OCSPType = basic : With basic OCSP responder support, request does not need to be signed
- New audit record will be created when a valid response is generated

PKI Trust Policy Plugin Enhancements

- **What is it?**
  - PKI Trust Policy is a certificate validation application
  - It can validate the certificates issued by PKI Services and other Certificate Authorities
  - In this release, it can make use of the new support of the CRL distribution point URI and OCSP
- **Benefit of having this support:**
  - Trust Policy of PKI Services has competitive validation ability as the other validation applications

PKI Trust Policy Plugin Enhancements

- Instead of checking certificate revocation status just through a CRL from a predefined directory server, the validation sequence is changed to:

1. OCSP responder
   - Indicated in the Authority Information Access Extension in the cert
   - Can go to PKI Services responder or third party's
2. URI format CRL/ARL Distribution Points
   - Indicated in the CRL Distribution Point Extension in the cert, includes server location
3. Distinguished Name format CRL/ARL Distribution Points
   - No server location indicated in the extension
4. Master CRL/ARL

** The original support was only steps 3 and 4

New Subject Alternate Name Format

- **What is it?**
  - Subject Alternate Name is an extension in a certificate
  - Prior to this release, the supported formats are email address, domain sever name, URI and IP address
  - Now an additional format called OtherName is added

- **Benefit of having this support:**
  - Unlike the other formats, the OtherName format is free formed – very flexible to customize to hold any kinds of data

Subject Alternative Name – OtherName

- Enable PKI Services to generate certificates with Subject Alternative Name Extension with 'OtherName' form
- The format of an OtherName is a dotted decimal OID followed by a comma, followed by the data specific to the OID.
- Customers determine the OID and data format to use in the extension and design their own web page dialogs to enable the creation and display of the field(s)

Subject Alternative Name – OtherName…

- R_PKIServ callable service was modified to support the new OtherName form
- The PKI web pages were updated to allow entry of, and display the values of the OtherName

Single Request

Requestor:	For altother	**Created:**	2005/01/05
Status:	Pending Approval	**Modified:**	2005/01/05
Transaction Id:	1jVEqye9Zgk/2SHV++++++++	**Passphrase:**	a
Template:	n-Year PKI Certificate for Extensions Demonstration	**NotifyEmail:**	

Previous Action Comment:

Subject:	CN=Wai,OU=ibm,C=us
Issuer:	CN=new_CA%2,O=ibm,C=us
Validity:	2005/01/05 00:00:00 - 2006/01/04 23:59:59
Usage:	handshake(digitalSignature, keyEncipherment)
Extended Usage:	clientauth
AltIPAddr:	9.56.53.111
AltURI:	http://plpsc.pok.ibm.com
AltEmail:	wchoi@us.ibm.com
AltDomain:	plpsc.pok.ibm.com
AltOther:	Other Name for alternate name: Customer's account number (11 digits) 11111111111
AltOther:	Other Name for alternate name: Customer's driver license number (9 digits) 222222222 Customer's driver license expiration date (yyyymmdd) 20051231
HostIdMap:	wai@pokvmtl4.pok.ibm.com

All these are different forms in the Subject Alternate Name extension

Usability Enhancement

- The PKI-Brazil CA (ICP-Brasil) certificate was added to the list of default CERTAUTH certificates in RACF
- During PKI Services initialization, errors detected in the pkiserv.conf file will be logged as “error” level messages in the job log of the daemon.
- All PKI Services daemon created threads are now managed in the same manner, and will prevent the daemon from “hanging” when a stop command is issued from the console.
- The R_PKIServ callable service, VERIFY, was enhanced to accept PKCS#7 certificate packages as input, in addition to x509 certificates.

Usability Enhancement…

- Debug option for the Web pages can now be set also from the pkiserv template file, not only from the CGI scripts which are not recommended for modification.
  - To Debug a problem in the PKI Web pages, customers had to edit each REXX exec to set the debug flag. In R7, this same option is available, but in addition, a customer can update the pkiserv template file (pkiserv.tmpl) to enable debug for all the web pages.

Session Summary

- You should now have an understanding of...
  - PKI Services prior to R7
  - Benefits of the new support
  - Enhancements made for R7

Publications

- *z/OS Cryptographic Services PKI Services Guide and Reference - SA22-7693*
- *z/OS Security Server RACF Command Language Reference - SA22-7687*
- *z/OS Security Server RACF Security Administrator's Guide - SA22-7683*
- *z/OS Security Server RACF Callable Services - SA22-7691*
- *z/OS Integrated Security Services LDAP Server Administration and Use - SC24-5923*
- *z/OS Security Server Open Cryptographic Enhanced Plug-ins Application Programming - SC24-5925*
- *z/OS OCSF Service Provider Module Developer's Guide and Reference - SC24-5900*
- *z/OS Cryptographic Services System Secure Sockets Layer Programming - SC24-5901*
- *z/OS Cryptographic Services ICSF Administrator's Guide - SA22-7521*
- *z/OS HTTP Server Planning, Installing, and Using - SC34-4826*

Websites

- PKI Services http://www-1.ibm.com/servers/eserver/zseries/zos/pki
- PKIX http://www.ietf.org/html.charters/pkix-charter.html
- Identrus http://www.identrus.com