

ibm.com



e-business



PKI Services for z/OS V1R5



Redbooks

International Technical Support Organization

© Copyright IBM Corp. 2003. All rights reserved.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

ibm.com®
z/OS®
IBM®
MVS™
Perform™
RACF®

The following terms are trademarks of other companies:

Intel, Intel Inside (logos), MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

PKI Services Overview

Complete Certificate Authority (CA) package

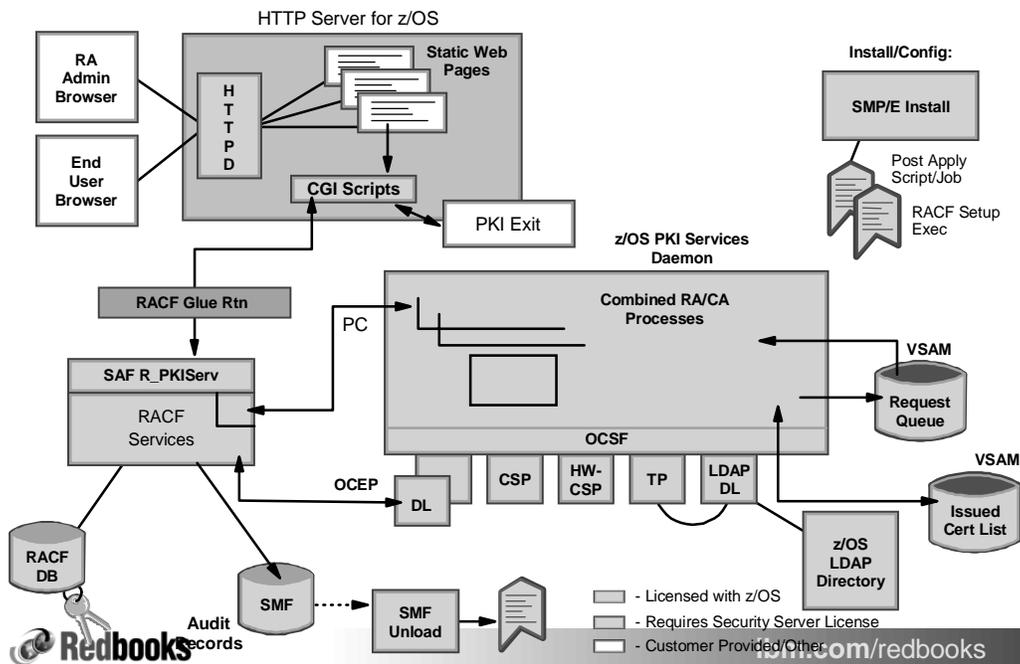
- Full certificate life cycle management
 - User request driven via customizable Web pages
 - Browser or server certificates
 - Automatic or administrator approval process
 - Administered using the same Web interface
 - End user/administrator revocation process
- Certificate validation service for z/OS applications



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

z/OS PKI Services Architecture



© Copyright IBM Corp. 2003. All rights reserved.

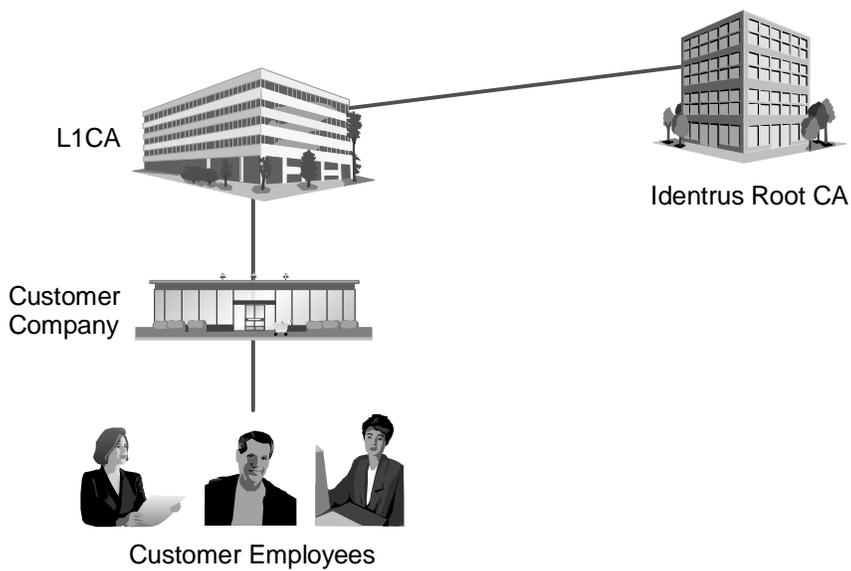
Support for Identrus Compliance



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

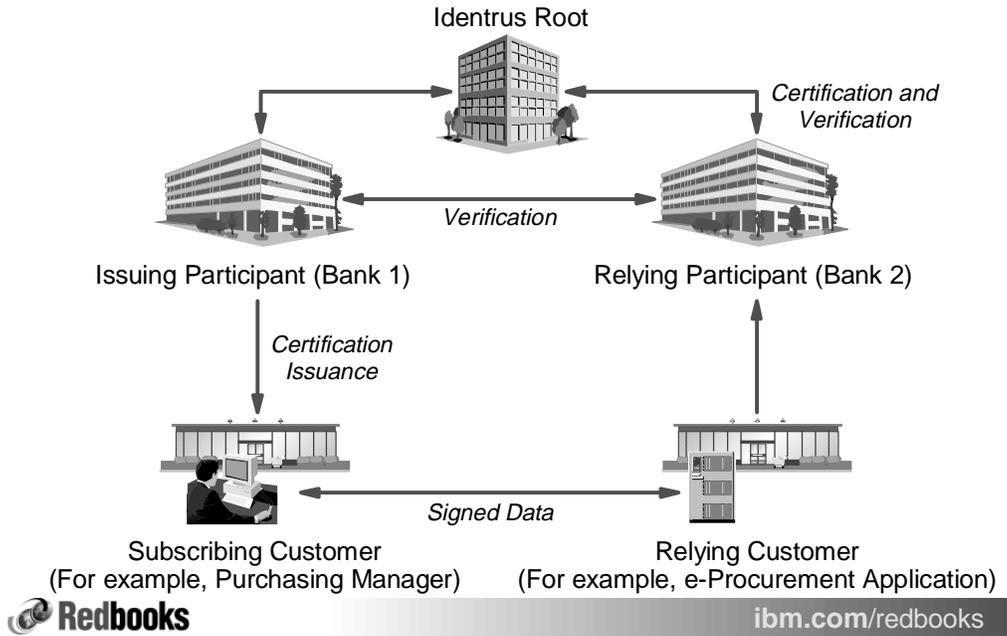
Identrus PKI - Providing Credentials



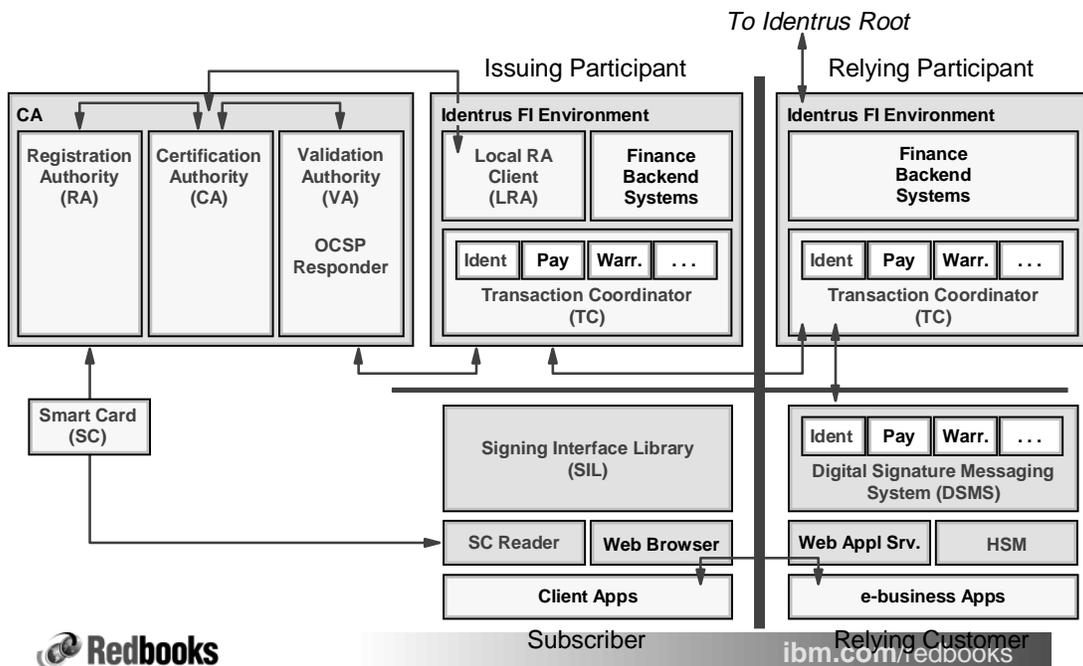
ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

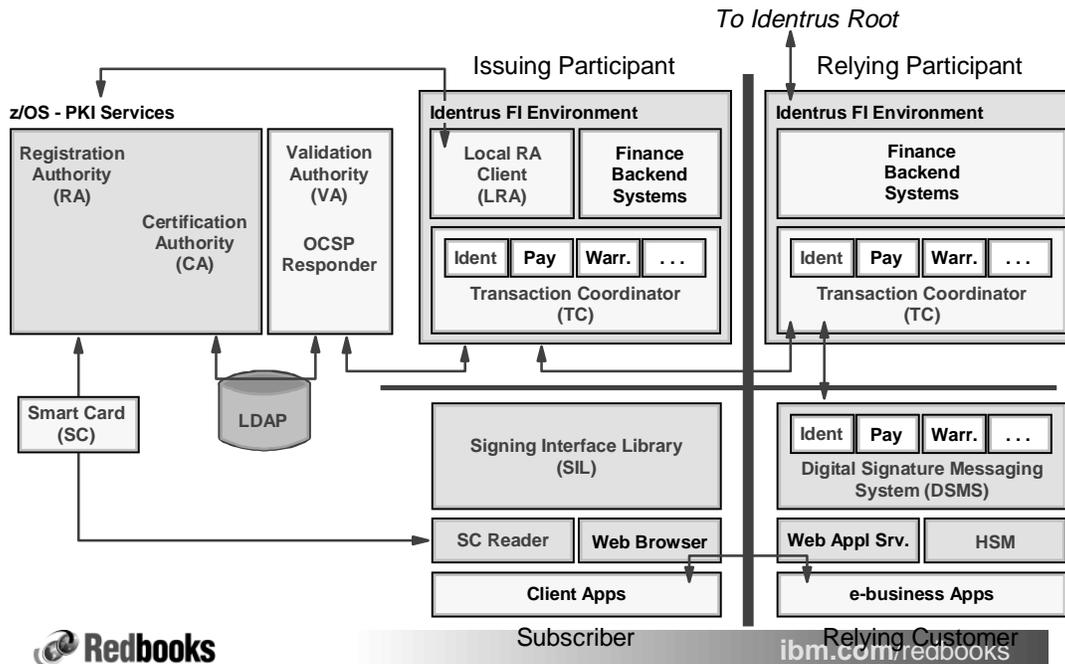
The Identrus Four Corner Model



Identrus PKI



Where PKI Services Fits



© Copyright IBM Corp. 2003. All rights reserved.

PKI Services/RACF Support for Identrus

New/enhanced certificate extensions

- KeyUsage - Support all RSA related flags as defined by RFC2459
- For example, digitalSignature/keyEncipherment vs. handshake

ExtKeyUsage - Allows additional key usages to be defined serverauth, clientauth, codesigning, emailprotection, timestamping and ocsp signing

AuthorityInfoAccess - Needed for vendor VA support (OCSP)

Marking extensions critical - Support on a per template basis

- ExtKeyUsage, CertPolicies, HostIdMappings, SubjectAltName

■ Sample template file directives

```
%%KeyUsage=digitalSig%%
%%ExtKeyUsage=clientauth%%
%%AuthInfoAcc=IdentrusOCSP,URL=https://IV.TC.BankXYZ.com%%
%%Critical=ExtKeyUsage%%
```

Redbooks

ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Certificate Policies

CertificatePolicies – Support on a per template basis

- R4 PKI supports one global set of policies for all certificate types
- Identrus requires unique policies for each certificate type

Individual policies defined in configuration file

```
identrusIdentityPolicy=1.2.840.114021.1.4.1
```

```
Policy used for Identrus End-Entity Identity and  
Server Signing Certificates
```

```
policyName4=IdentrusIdentityPolicy
```

```
serverNoticeText4=This certificate is for the sole use of Identrus,  
its Participants and their customers. Identrus accepts no liability  
for any claim except as expressly provided in its Operating Rules  
IL-OPRUL.
```

- Template file directive specifies policy use

```
%%CertPolicies=4%%
```



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Predefined Identrus Certificate Types

New certificate templates (models) for Identrus

- Included in template file

End-Entity Identity - Used to sign legally binding transactions

- KeyUsage - digitalSignature, nonRepudiation
- CertificatePolicies - The Identrus "signing" policy
- AuthInfoAccess - OCSP information
 - Standard OCSP protocol
 - Identrus enhanced OCSP

End-Entity Utility - Used for SSL client auth and S/MIME data encryption

- KeyUsage - digitalSignature, keyEncipherment, dataEncipherment, keyAgreement
- ExtKeyUsage - Client authentication, Email protection
- CertificatePolicies - The Identrus "utility" policy
- AuthInfoAccess - Same as Identity certificate
- SubjectAltName – E-mail address



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Predefined Identrus Certificate Types...

End-Entity Server Signing - Used to sign communications

- AuthInfoAccess - Identrus enhanced OCSP
- Other info - same as Identity certificate

End-Entity Server Encipherment - Used for SSL server auth

- KeyUsage - digitalSignature, keyEncipherment
- ExtKeyUsage - Server authentication
- CertificatePolicies - Customer defined policy with Identrus wording
- AuthInfoAccess - Same as Server Signing certificate
- SubjectAltName - E-mail address

Authenticode - Used for code signing

- KeyUsage - digitalSignature, keyEncipherment
- ExtKeyUsage - Code signing
- CertificatePolicies - The Identrus "utility" policy
- SubjectAltName - E-mail address



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Web Pages - INSERTS for KeyUsage/ExtKeyUsage

Modify and Approve Request

Indicate the key usage for the certificate

A screenshot of a web form dropdown menu. The menu is open, showing a list of key usage options. The options are: Protocol handshaking e.g., SSL (digitalSignature, keyEncipherment), Certificate and CRL signing (keyCertSign, cRLSign), Document signing (nonRepudiation), Data encryption (dataEncipherment), Authentication (digitalSignature), Key Transport (keyEncipherment), Key agreement (keyAgreement), Certificate signing (keyCertSign), and CRL signing (cRLSign). The 'Data encryption (dataEncipherment)' option is currently selected and highlighted.

Indicate the extended key usage for the certificate

A screenshot of a web form dropdown menu. The menu is open, showing a list of extended key usage options. The options are: Server side authentication (serverAuth), Client side authentication (clientAuth), Code signing (codeSigning), Email protection (emailProtection), Digital time stamping (timeStamping), and OCSP response signing (OCSPSigning). The 'Code signing (codeSigning)' option is currently selected and highlighted.



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Single Certificate Request or Issued Certificate

Data reformatted. Complete KeyUsage/ExtKeyUsage info displayed.

Single Request

Requestor:	jsweeny@us.ibm.com	Created:	2002/04/29
Status:	Approved	Modified:	2002/04/29
Transaction Id:	1jClzs9OX5QgVknDWBrf3ls+	Passphrase:	mred
Template:	1 Year PKI SSL Browser Certificate	NotifyEmail:	jsweeny@us.ibm.com
Serial #:	<u>5447</u>		
Previous Action Comment: <hr/>			
Subject:	MAIL=jsweeny@us.ibm.com,CN=Michael Sweeny,OU=Class 1 Internet Certificate CA,O=The Firm		
Issuer:	CN=Bank XYZ Identrus Certificate Authority,OU=Bank XYZ Identrus Authority,O=Bank XYZ		
Validity:	2002/04/29 00:00:00 - 2003/04/28 23:59:59		
Usage:	handshake(digitalSignature, keyEncipherment)		
Extended Usage:	clientauth		



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Certificate Suspension

Temporarily revoke a certificate

- End user may suspend own browser certificate via Web page
 - ↳ Requires SSL w/client auth
- PKI Administrator may suspend end user's certificate
- Only PKI Administer may resume end user's certificate

Some possible reasons to suspend a certificate

- On vacation
- Fear private key may have been compromised

Optional suspension "Grace Period"

- Time period after which suspended certificates are permanently revoked
- Configuration file directive
 - # Length of certificate suspension grace period in day
 - # or weeks (d,w). 0d for unlimited.
 - MaxSuspendDuration=120d



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Suspend a Certificate

Requestor:	jsweeny@us.ibm.com	Created:	2002/04/29
Status:	Active	Modified:	2002/04/29
Template:	1 Year PKI SSL Browser Certificate		
Serial #:	5447		
Previous Action Comment:	Issued certificate		
<hr/>			
Subject:	MAIL=jsweeny@us.ibm.com,CN=Michael Sweeny,OU=Class 1 Internet Certificate CA,O=The Firm		
Issuer:	CN=Bank XYZ Identrus Certificate Authority,OU=Bank XYZ Identrus Authority,O=Bank XYZ		
Validity:	2002/04/29 00:00:00 - 2003/04/28 23:59:59		
Usage:	handshake(digitalSignature, keyEncipherment)		
Extended Usage:	LISTDATA.12		

- Revoke the certificate

- Suspend the certificate

- Delete the certificate



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Resume a Certificate

Requestor:	G. W. Bush	Created:	2002/04/29
Status:	Suspended	Modified:	2002/04/29
Template:	1 Year PKI SSL Browser Certificate		
Serial #:	5448		
Previous Action Comment:			
<hr/>			
Subject:	CN=G. W. Bush,OU=Class 1 Internet Certificate CA,O=The Firm		
Issuer:	CN=Bank XYZ Identrus Certificate Authority,OU=Bank XYZ Identrus Authority,O=Bank XYZ		
Validity:	2002/04/29 00:00:00 - 2003/04/28 23:59:59		
Usage:	handshake(digitalSignature, keyEncipherment)		
Extended Usage:	LISTDATA.12		

- Revoke the certificate

- Resume the certificate

- Delete the certificate



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

New Certificate Query

PKI Services Administration

Choose one of the following:

.....

- **Specify search criteria for certificates and certificate requests**

Certificate Requests

- Show all requests
- Show requests pending approval
- Show approved requests
- Show completed requests
- Show rejected requests
- Show rejections in which the client has been notified

Issued Certificates

- Show all issued certificates
- Show revoked certificates
- Show suspended certificates
- Show expired certificates
- Show active certificates (not expired, not revoked, not suspended)
- Show disabled certificates (suspended or revoked, not expired)



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Miscellaneous Support

Internal auditing

- Publishing of CRLs to LDAP is now audited
 - New event unloaded by RACF SMF Unload

Multiple Application Domains

- Way of subdividing your customers
 - Each customer set can have a unique home page and set of certificate templates
 - Defined by adding additional APPLICATION sections in template file
 - Default setup has two application domains: "PKIServ" and "Customers"
 - "Customer" home page is the same as "PKIServ", less the "Go to Administration Page" but

Application domain part of URL. For example,
<http://dceimgun.pdl.pok.ibm.com/Customers/public-cgi/camain.rexx>



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Miscellaneous RACF Support

RACF - 2048 bit RSA key generation

- Old limit (1024) still in effect for software keys
- Up to 2048 bits permitted if generated by ICSF
 - TSO command - RACDCERT GENCERT SIZE(2048) PCICC
 - PCICC keyword requires either PCICC card or z990 with PCIXCC card
- Option for PKI Services to use 2048 bit signing key
 - IKYSETUP REXX exec - ca_keysize="2048"

RACF - New default CA certificates added

- Identrus Interoperability CA
- GTE CyberTrust Root CA
- Entrust.net Secure Server CA



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Performance Improvements



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Additional VSAM Alternate Indexes

Improves performance of data access

- Each VSAM data set (ObjectStore and ICL) now has:
- Status Alternate Index – For background tasks. For example, creating CRLs.
- Requestor Alternate Index – For user queries based on requestor's name
 - Customer should ensure requestor names are meaningful. Should be unique (For example, e-mail address.)

Migration – Customer must create alternate indexes

- Sample JCL provided – SYS1.SAMPLIB(IKYMVSAM)

New configuration file directives for alternate indexes

```
ObjectStatusDSN='pkisrvd.vsam.ost.status'  
ObjectRequestorDSN='pkisrvd.vsam.ost.requestr'  
ICLStatusDSN='pkisrvd.vsam.icl.status'  
ICLRequestorDSN='pkisrvd.vsam.icl.requestr'
```



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Optional VSAM Buffering

Declare DD statements in PKISERVD proc with AMP values

```
//OST DD DSN=PKISRVD.VSAM.OST,DISP=SHR,  
// AMP=('BUFNI=8,BUFND=4')  
//TID DD DSN=PKISRVD.VSAM.OST.PATH,DISP=SHR,  
// AMP=('BUFNI=8,BUFND=4')  
//OSTAT DD DSN=PKISRVD.VSAM.OST.STATUS,DISP=SHR,  
// AMP=('BUFNI=1,BUFND=4')  
//OREQ DD DSN=PKISRVD.VSAM.OST.REQUESTR,DISP=SHR,  
// AMP=('BUFNI=1,BUFND=4')  
//ICL DD DSN=PKISRVD.VSAM.ICL,DISP=SHR,  
// AMP=('BUFNI=8,BUFND=4')  
//ISTAT DD DSN=PKISRVD.VSAM.ICL.STATUS,DISP=SHR,  
// AMP=('BUFNI=1,BUFND=4')  
//IREQ DD DSN=PKISRVD.VSAM.ICL.REQUESTR,DISP=SHR,  
// AMP=('BUFNI=1,BUFND=4')
```

Configuration file directives specify the DD statements

```
ObjectDSN=DD:OST  
ObjectTidDSN=DD:TID  
ObjectStatusDSN=DD:OSTAT  
  
ObjectRequestorDSN=DD:OREQ  
  
ICLDSN=DD:ICL  
ICLStatusDSN=DD:ISTAT  
  
ICLRequestorDSN=DD:IREQ
```

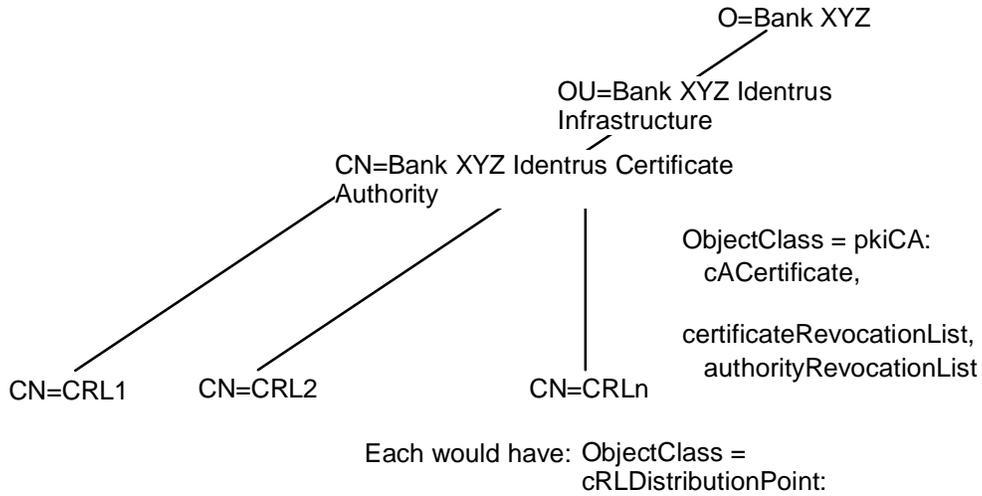


ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

CRL Distribution Points (DPs)

Mechanism to keep the size of CRLs small



© Copyright IBM Corp. 2003. All rights reserved.

ibm.com/redbooks

CRL Distribution Points...

User certificates subdivided into CRL DPs

- Subdivision based on serial number
 - For example, Certificates 1-500 go in CRL DP 1, 501-1000 go in CRL DP 2, etc.
- `CRLDistributionPoints` extension specifies the correct DP CRL
- PKI Services does not use CRL DPs for CA certificates

Configuration file directives for CRL DPs

```
# Maximum number of certificates that may appear on one
# distribution point CRL. 0 for no CRL DPs.
CRLDistSize=500

# Constant portion of the CRL distribution point leaf-
# node relative distinguished name. The distribution
# point number is appended to this value to form the
# common name. The default value is "CRL".
CRLDistName=CRL
```



© Copyright IBM Corp. 2003. All rights reserved.

ibm.com/redbooks

Miscellaneous Performance Support

Replaced OCSF Crypto with System SSL

- In PKI Services daemon only
 - Certificate validation API (pktp) still uses OCSF crypto
- No directives to control this. Should be an invisible change

ICL cleanup

- Option to removed expired certificate from the ICL after a given time period
 - Controlled by configuration file directive
 - # How many days (d) or weeks (w) should expired
 - # certificates remain in the ICL? Specify 0d to
 - # indicate expired certificates should not be removed
- `RemoveExpiredCerts=26w`



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Sysplex Considerations



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Sysplex Considerations - R4 and R5 PKI Services

R4 and R5 PKI Services may coexist

- VSAM Record Level Sharing (RLS) maintains alternate indexes across both releases

Avoid using R5 features when shared with R4

- Suspended certificates appear as revoked on R4
- Do not use any of the following:
 - CRL Distribution Points
 - Template specific Certificate Policies
 - New extension support (For example, ExtKeyUsage.)
 - New Identrus certificate types



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Session Summary

You should now have an understanding of...

- PKI Services prior to R5
- Enhancements made for R5 to:
 - PKI Services itself, and...
 - Related RACF changes



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Notices

This information was developed for products and services offered in the U.S.A.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.