



zSeries Explorers



IBM @server zSeries

PKI Services

Como economizar dinheiro explorando este novo componente do z/OS Security Server

Vicente Ranieri Júnior

IBM Senior Certified Consulting IT Specialist

ranieri@br.ibm.com



IBM @server zSeries

zSeries Explorers

IBM

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

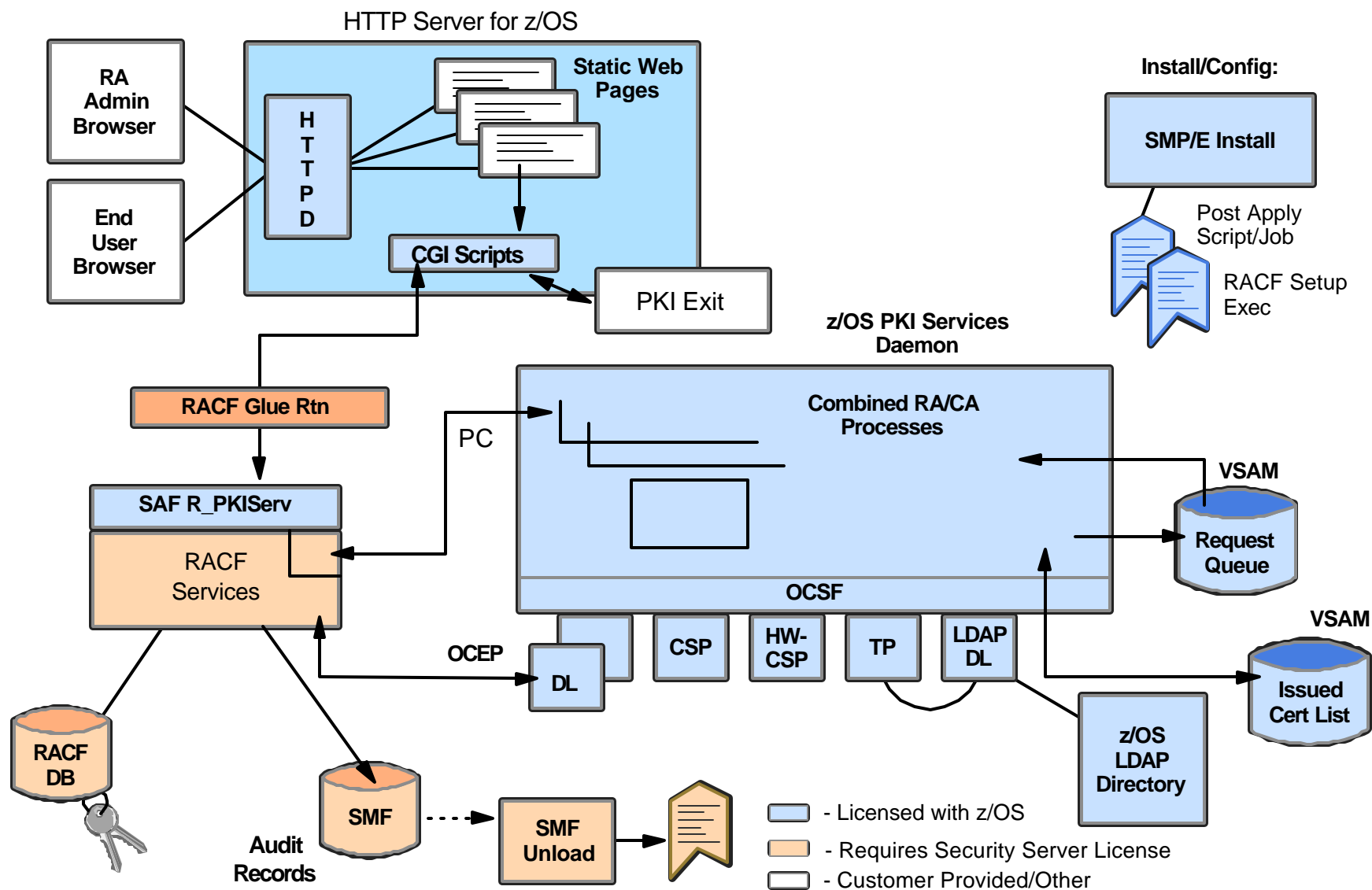


IBM @server zSeries

zSeries Explorers

IBM

z/OS PKI Services Architecture





IBM @server zSeries

zSeries Explorers

IBM

z/OS PKI Services System Components

■ HTTP Server

- ▶ Provides browser/CGI interface for end-users and administrators
 - Web page logic defined in certificate templates file
 - CGIs - Read template file, control flow

■ R_PKIServ - SAF callable service backed by RACF (or other)

- ▶ End-user functions - Request, retrieve, verify, revoke, or renew a certificate
- ▶ Administrator functions - Query, approve, modify, or reject certificate requests, query and revoke issued certificates
- ▶ Interface to call PKI Services
- ▶ SMF auditing

■ PKI Services Daemon

- ▶ Services threads for incoming requests
- ▶ Background threads for certificate approval/certificate revocation list (CRL) issuance
- ▶ VSAM DBs for requests (ObjectStore) and issued certificate list (ICL)



IBM @server zSeries

zSeries Explorers

IBM

z/OS PKI Services System Components (continued)

- **Open Cryptographic Services Facility (OCSF) and Open Cryptographic Enhanced Plug-in (OCEP)**
 - ▶ Provided the crypto facilities for PKI Services
 - OCEP - Access to CA certificate and private key in RACF
 - OCSF - BSAFE or ICSF (Hardware) crypto engines
- **LDAP Directory**
 - ▶ Publication of issued certificates and CRLs



IBM @server zSeries

zSeries Explorers

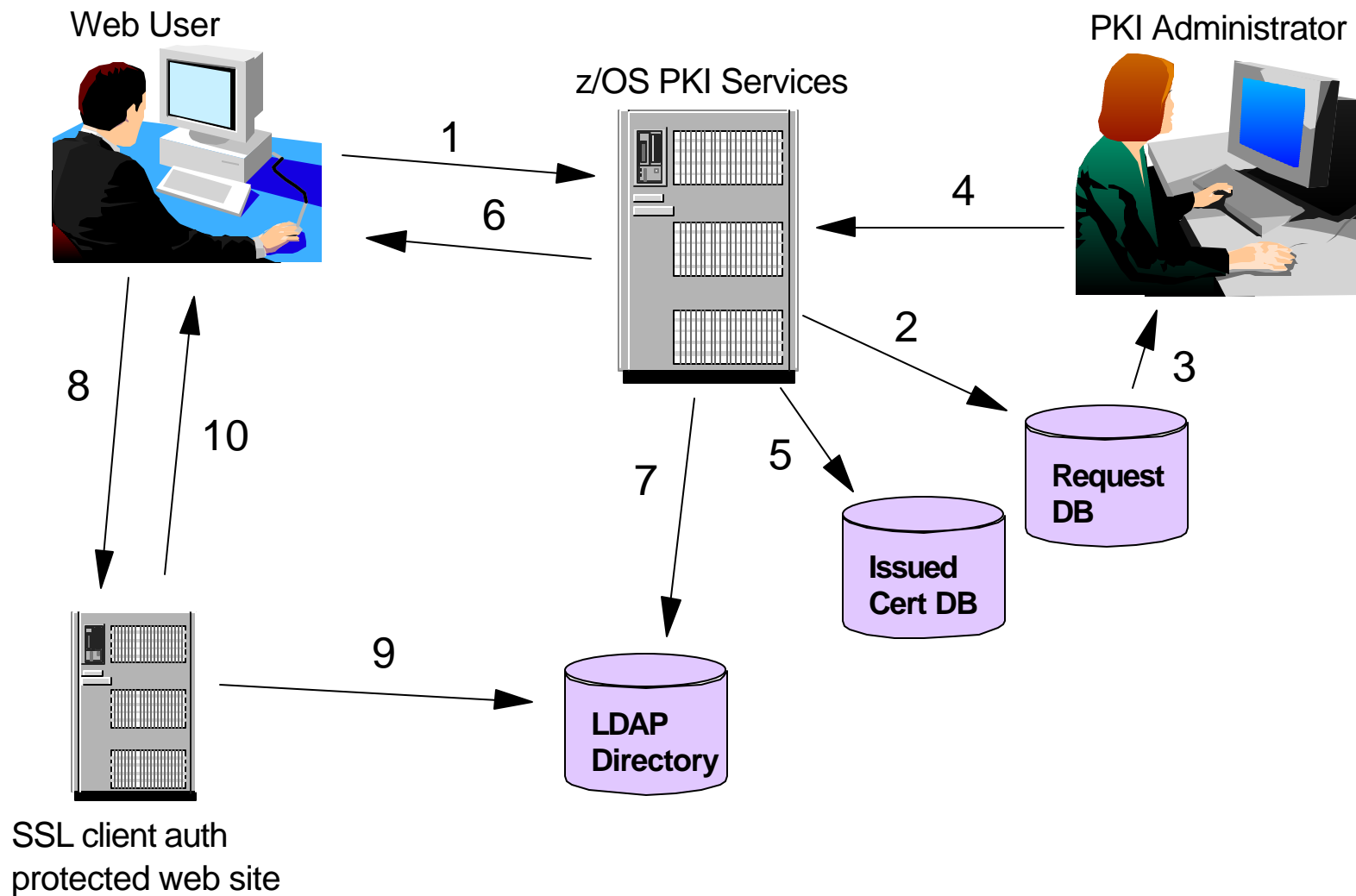
IBM

Uses For Certificates

- Servers (devices) on z/box or elsewhere
 - ▶ Server authentication, data encryption
 - SSL Webservers
 - VPNs -
 - Internet Routers
- Clients (workstations)
 - ▶ SSL client authentication
 - e.g., accessing protected web sites
 - ▶ Message encryption and/or signing (S/MIME E-mail)
 - ▶ File encryption

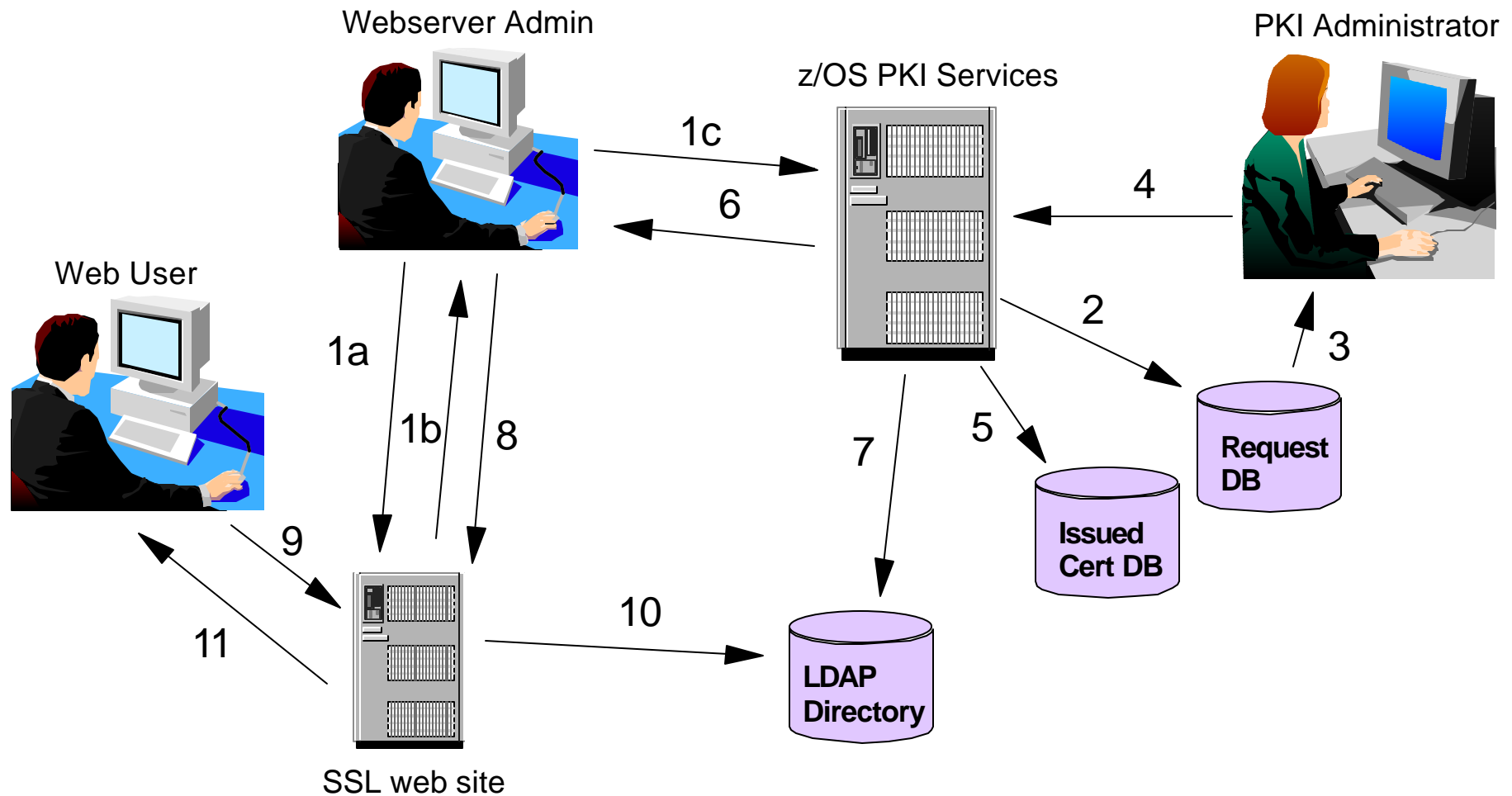


Browser Certificates





Server Certificates





IBM @server zSeries

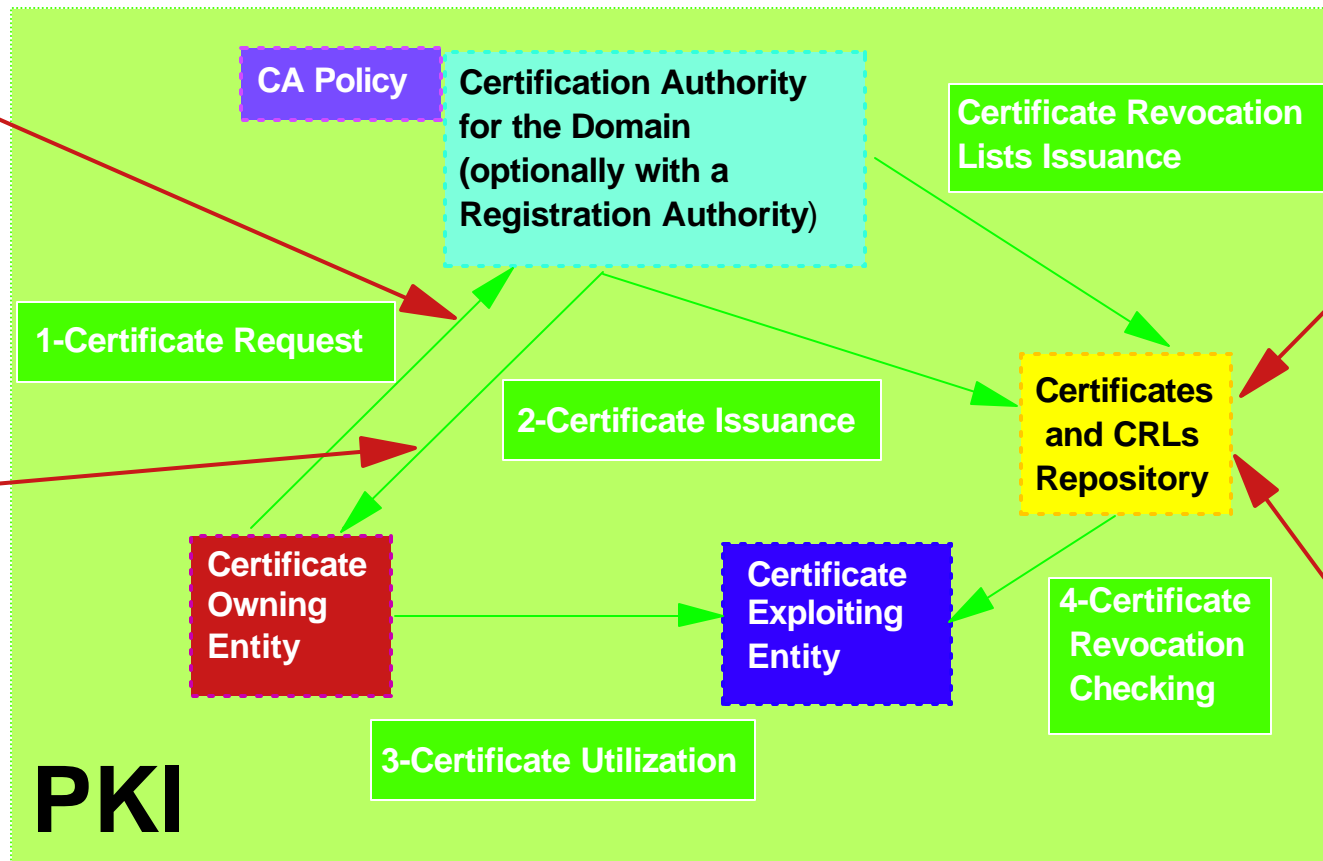
zSeries Explorers

IBM

Compliant with PKIX Architectural Model

PKIX:
Certificate
Request in
PKCS#10
format

PKIX:
Format of
Certificate
is X.509 V3



PKIX:
Format of
Certificate
Revocation
List is
X.509 V2

PKIX:
CRL
repository
(LDAP
directory)

<http://www.ietf.org/internet-drafts/draft-ietf-pkix-roadmap-06.txt>



IBM @server zSeries

zSeries Explorers

IBM

z/OS V1R4 PKI Services Enhancements

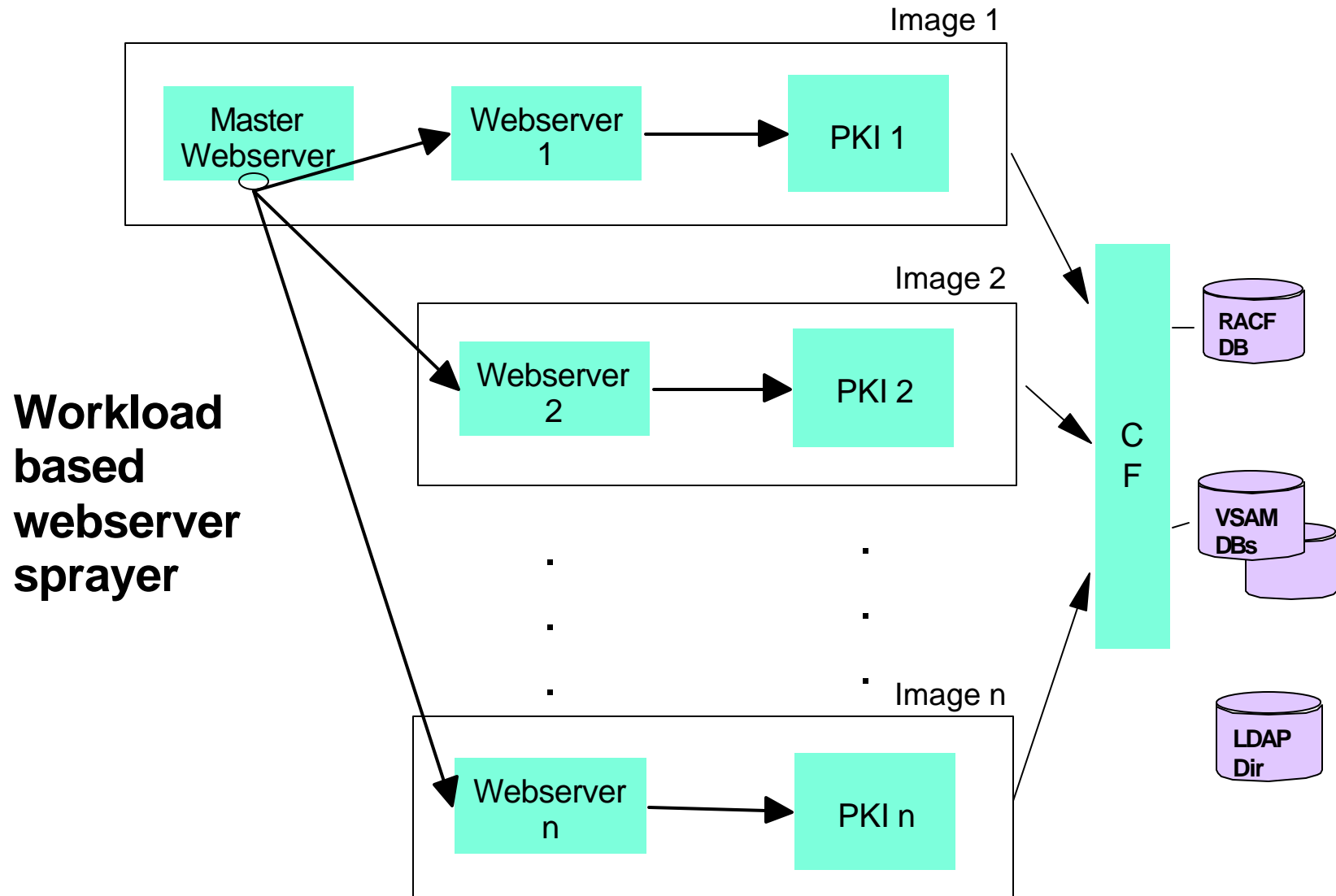


Sysplex Support

- R3 - no parallel Sysplex support
 - ▶ Multiple instances of PKI Services in a plex would all be independent, ie., separate databases (VSAM data sets)
- R4 - multiple instances can share databases
 - ▶ Access via VSAM record level sharing (RLS)
 - Requires - CF, couple data sets, storage class
 - See DFSMS manuals
 - IDCAMS STORCLAS keyword in create JCL
 - New sample JCL (IKYMVVSAM) to migrate existing data sets to new storage class
 - ▶ Configuration setting (SharedVSAM=T) tells PKI Services to use VSAM RLS



Sysplex Support Configuration





Event Notification via Email

- New request named field, "NotifyEmail"
 - ▶ Allows end-users to supply a notification email address
 - Notified when request is complete (ready or rejected)
 - Notified when certificate is about to expire
- NotifyEmail addr stored in LDAP directory as MAIL attribute
- Comm Server's sendmail utility used to send email message
- Customer supplies message forms - Pathnames specified via configuration settings:
 - ▶ ReadyMessageForm=/etc/pkiserv/readymsg.form
 - ▶ RejectMessageForm=/etc/pkiserv/rejectmsg.form
 - ▶ ExpiringMessageForm=/etc/pkiserv/expiringmsg.form
- Sample message forms shipped in samples directory



IBM @server zSeries

zSeries Explorers

IBM

Sample Ready Message

PKI Services recognizes 4 variables and will substitute accordingly - transactionid, requestor, dn, and notafter:

From:dime-o-cert PKI

Subject:Certificate Ready For Pick Up

Attention - Please do not reply to this message as it was automatically sent by a service machine.

Dear %%requestor%%,

Thank you for choosing dime-o-cert PKI. The certificate you requested for subject %%dn%% is now ready for pickup. Please visit <http://www.dimeocert.com/PKIServ/camain.rexx> to retrieve your certificate. You will need the transaction ID listed below and your passphrase that you entered when you submitted the request.

%%transactionid%%



Additional DN Qualifiers

- Subject's distinguished name (DN) is specified via qualifier name/value pairs when the request is submitted.
e.g., CN=Jim Sweeny,O=IBM,C=US
 - ▶ Qualifiers are named fields in the web pages
 - Can be user supplied or hardcoded
- In R3, the following DN qualifiers were supported:
 - ▶ CommonName, Title, OrgUnit, Org, Locality, StateProv, and Country
- In R4, the following qualifiers are added:
 - ▶ Email, PostalCode, and Street
 - If both Email and NotifyEmail are specified, they must be equal.



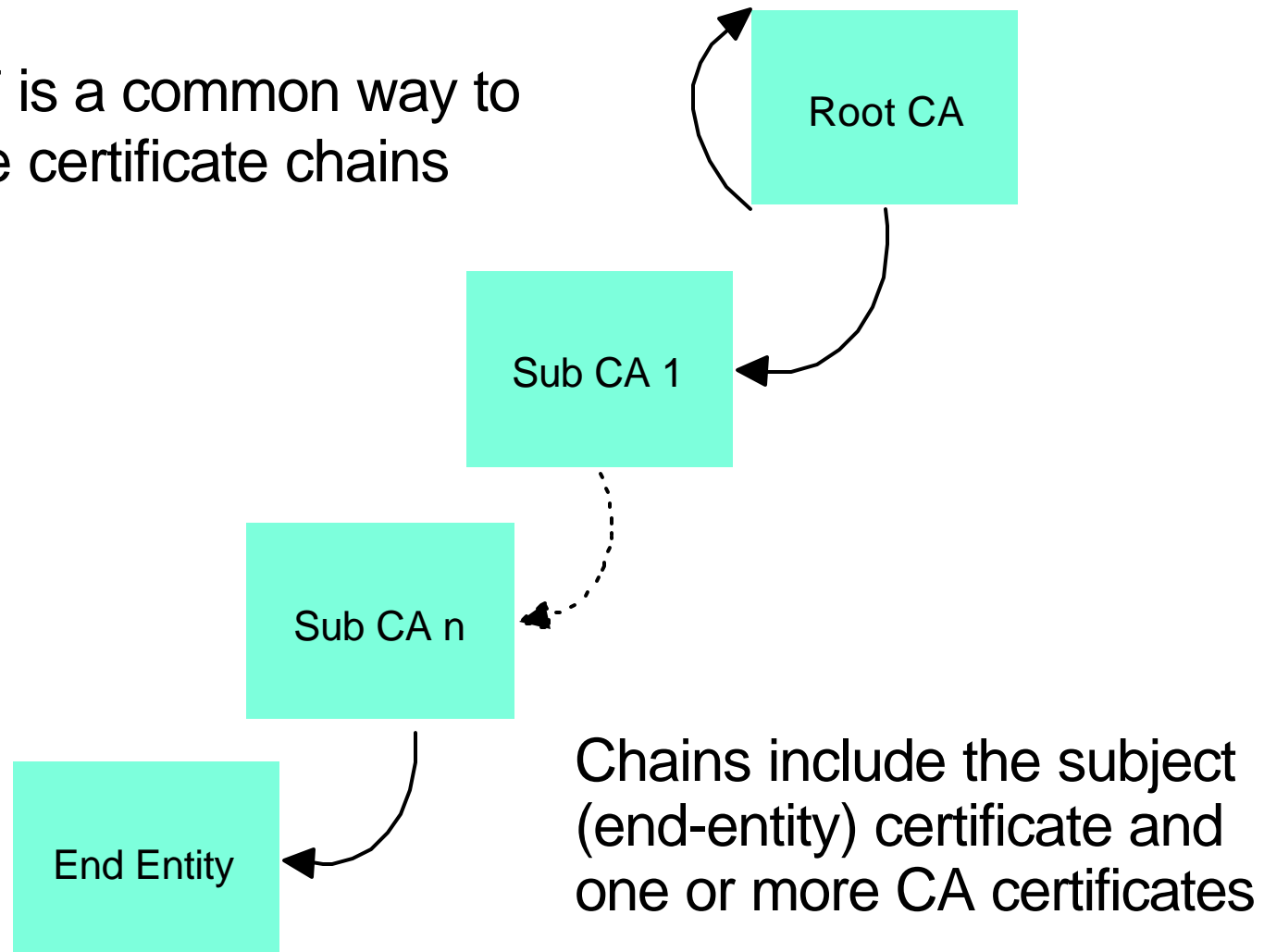
LDAP Password Encryption

- PKI Services posts information to LDAP
 - ▶ Needs bind dn and password to do so
- In R3, bind password specified in the clear as configuration setting AuthPWDn
- In R4, server name, port, bind dn, and pwd may be specified in PROXY segment of RACF profile
 - ▶ Create profile using RDEFINE ... PROXY command
 - ▶ LDAPBIND Class - Used to hold these binding profiles
 - Name specified via configuration setting BindProfilen
 - ▶ Or, IRR.PROXY.DEFAULTS in FACILITY Class to use same default as the LDAP Proxy
 - ▶ Password is encrypted by RACF when profile is created



PKCS#7 Certificate Chains

PKCS#7 is a common way to distribute certificate chains





PKCS#7 Certificate Chains (continued)

- Prior to R4:
 - ▶ RACDCERT ADD - Would ignore the CA certificates
 - ▶ RACDCERT EXPORT - Could not build a PKCS#7 cert chain
 - ▶ R_PKIServ EXPORT - Would only return a single certificate
- R4 - Full support for PKCS#7
- RACDCERT ADD - Will now add CA certificates to CERTAUTH if user authorized
 - ▶ Requires CONTROL authority to FACILITY class profile IRR.DIGTCERT.ADD or RACF SPECIAL
 - ▶ No new keywords to support this
 - ▶ Specified trust value used to prime top cert
 - Trust inherited down chain until inconsistency found
 - Subject certificate added with specified trust value



IBM @server zSeries

zSeries Explorers

IBM

PKCS#7 Certificate Chains Encoding

- RACDCERT EXPORT can now locate CERTAUTH certificates to build complete PKCS#7 chain
- New PKCS7* values for FORMAT keyword
 - ▶ PKCS7DER - DER (binary) encoded PKCS7 chain
 - ▶ PKCS7B64 - Same DER encoding with additional base64 encoding
 - ▶ Requires CONTROL authority to FACILITY class profile IRR.DIGTCERT.EXPORT or RACF SPECIAL
 - ▶ New informational message if constructed chain is incomplete



PKCS#7 Certificate Chains (continued...)

- R_PKIServ EXPORT can also locate CERTAUTH certificates to build complete PKCS#7 chain
- No parameter to ask for this. Controlled by caller's authority to IRR.DIGTCERT.EXPORT
 - ▶ CONTROL or higher or RACF SPECIAL
 - PKCS#7 built if at least one CA cert found in RACF
 - ▶ All other cases
 - Single certificate returned as in R3
 - ▶ For PKI Services web pages, the surrogate user ID is the ID whose authority is checked
 - Default setup enables return of PKCS#7 chains



Key Generation via PCICC

- Prior to R4, RACDCERT GENCERT generated RSA key pair using software
- R4, PCI Cryptographic Coprocessor (PCICC) used for generation if new PCICC keyword specified:
 - ▶ <no keyword specified> - key generated in software, then stored in RACF DB
 - ▶ ICSF specified - key generated in software, then stored in PKDS
 - Now fails if ICSF's PKA features not active (instead of saving as a software key as in R3)
 - ▶ PCICC specified - key generated using PCICC, then stored in PKDS
 - Fails if ICSF PKA features and/or PCICC not active



IBM @server zSeries

zSeries Explorers

IBM

Default CERTAUTH Certs

- Three new CERTAUTH certificates added to the default list:
 - ▶ Verisign Class 1 Individual CA
 - ▶ Verisign Class 2 Individual CA
 - ▶ Verisign International Svr CA
- Two expiring CERTAUTH certificates replaced:
 - ▶ Verisign Class 2 Primary CA
 - ▶ Verisign Class 3 Primary CA
- Defunct CERTAUTH certificate no longer added
 - ▶ IBM World Registry CA



IBM @server zSeries

zSeries Explorers



z/OS V1R5 PKI Services Enhancements

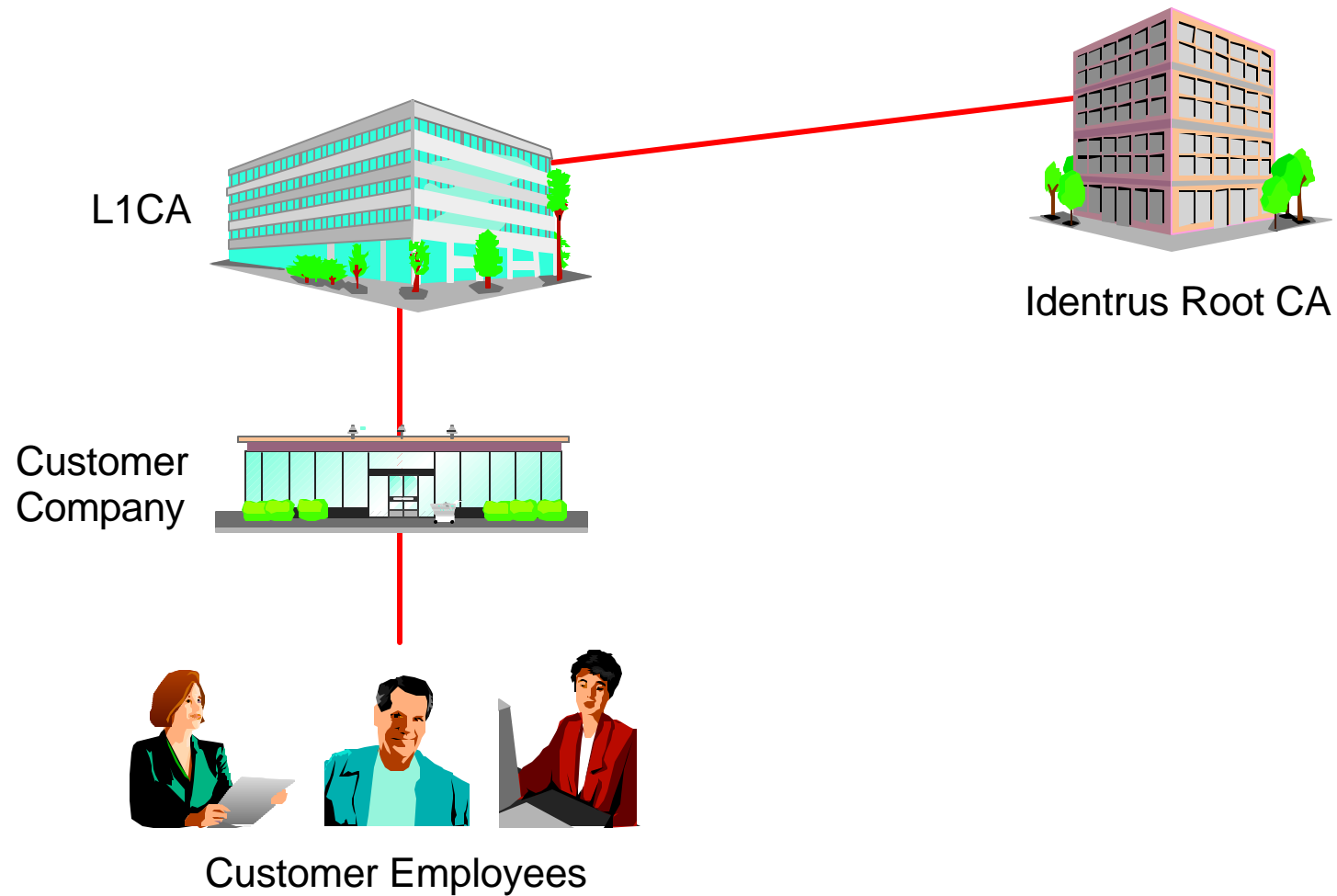


IBM @server zSeries

zSeries Explorers

IBM

Identrus PKI - Providing Credentials



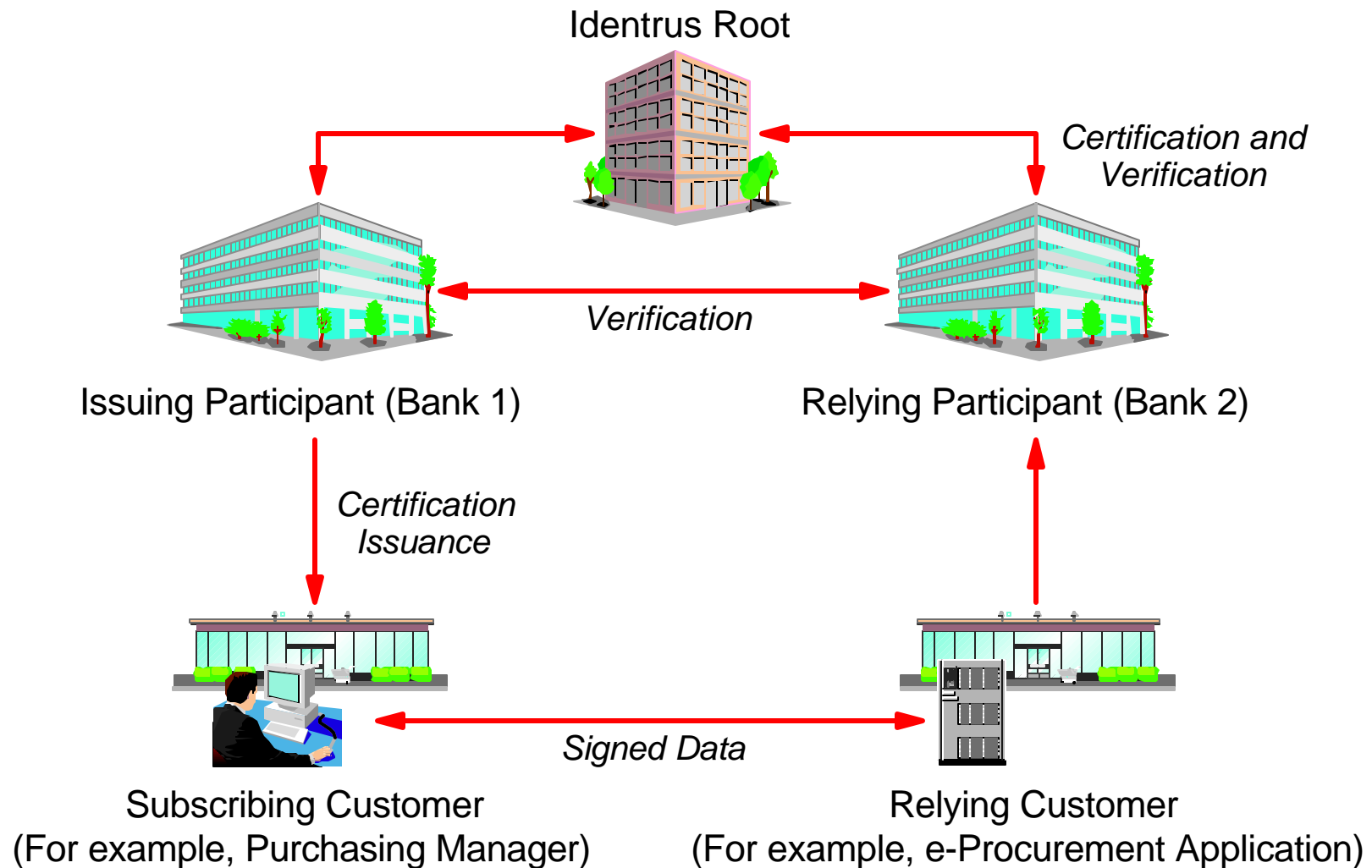


IBM @server zSeries

zSeries Explorers

IBM

The Idenrus Four Corner Model



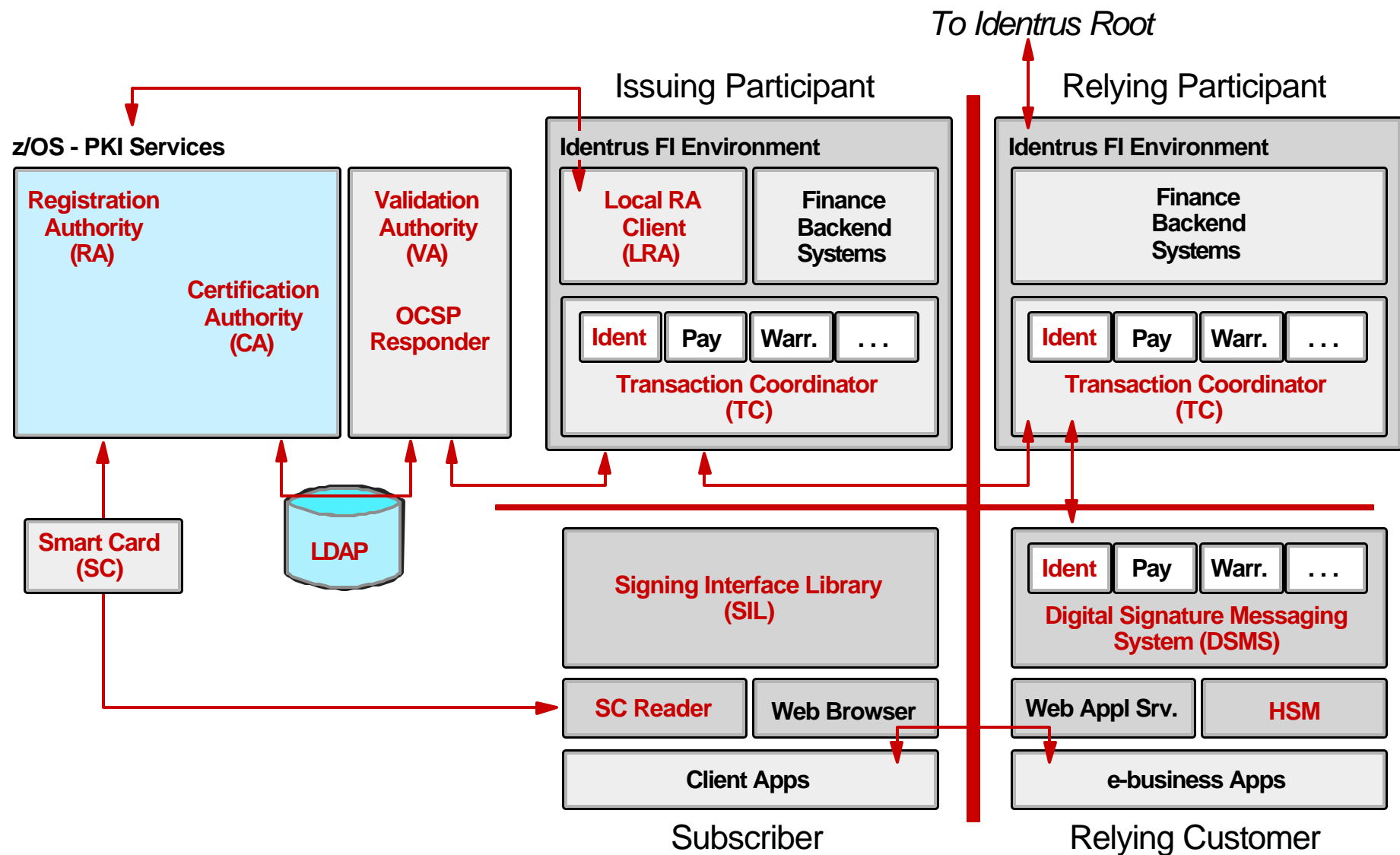


To Identrus Root





Where PKI Services Fits





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 @server zSeries

zSeries Explorers

IBM

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		

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 @server zSeries

zSeries Explorers

IBM

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 - Revoke the certificate

Resume - Resume the certificate

Delete - Delete the certificate



IBM @server zSeries

zSeries Explorers

IBM

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 @server zSeries

zSeries Explorers

IBM

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



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

Performance Improvements



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='pkisrzd.vsam.ost.status'`
 - `ObjectRequestorDSN='pkisrzd.vsam.ost.requestr'`
 - `ICLStatusDSN='pkisrzd.vsam.icl.status'`
 - `ICLRequestorDSN='pkisrzd.vsam.icl.requestr'`



Optional VSAM Buffering

- Declare DD statements in PKISERVDD proc with AMP values

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



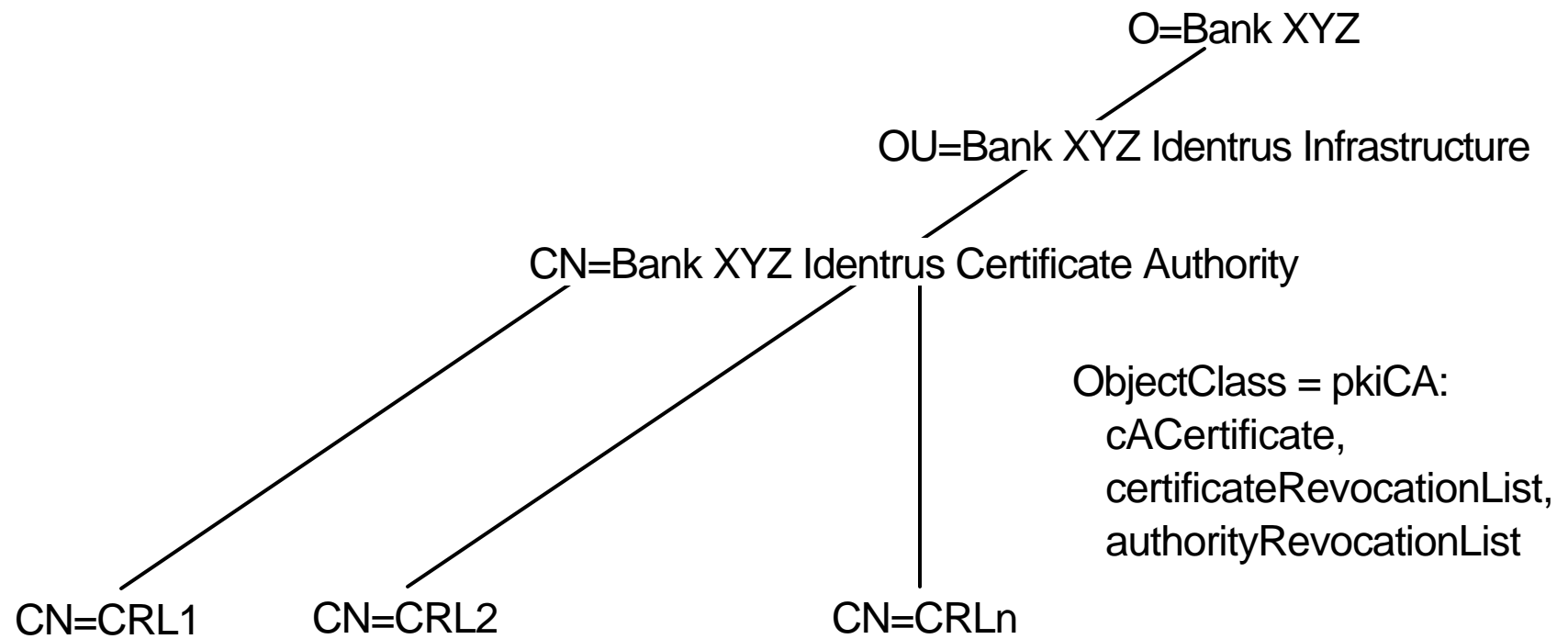
IBM @server zSeries

zSeries Explorers

IBM

CRL Distribution Points (DPs)

Mechanism to keep the size of CRLs small



Each would have: ObjectClass = cRLDistributionPoint:
certificateRevocationList



CRL Distribution Points (continued)

- 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
```



Miscellaneous Performance Support

- Replaced OCSF Crypto with System SSL
 - ▶ In PKI Services daemon only
 - Certificate validation API (pkitp) 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 @server zSeries

zSeries Explorers

IBM

Performance

z900 model 2064-104 with hardware encryption and VSAM buffering.

- ▲ Maximum ETR for synchronous certificate creates was **19.20 sec.**
- ▲ (PKI Services can create 19.2 certificates a second which includes the storage of the certificates in VSAM.)
- ▲ With 1+ million certificates created, queries with a requestor value specified as criteria returned in less than 1 second.
- ▲ With 1+ million certificates created and 5% revoked. CRL refreshing in LDAP (using 3055 CRL distribution points) took on average 3 minutes.



IBM @server zSeries

zSeries Explorers

IBM

Appendix



PKISERV Certificate Generation Application

[Install our CA certificate into your browser](#)

Choose one of the following:

- Request a new certificate using a model

Select the certificate template to use as a model

Same pull-down for requesting a certificate of a certain type (template)

- Pickup a previously requested certificate

Enter the assigned transaction ID

Select the certificate return type

New shortcut to pickup certificate with return template pull-down

- Renew or revoke a previously issued browser certificate

Link for renew/revoke forces SSL client authentication

- Administrators click here

Admin link is either userid/pw protected or forces SSL client authentication



IBM @server zSeries

zSeries Explorers



1 Year SSL Browser Certificate

Choose one of the following:

- **Request a New Certificate**

Enter values for the following field(s)

Common Name

Your name for tracking this request (optional)

Pass phrase for securing this request. You will need to supply this value when retrieving your certificate

Reenter your pass phrase to confirm

Select a key size

- **Pick Up a Previously Issued Certificate**

This is the certificate request page. The dialogs that appear on this page depends on the certificate template chosen.

When the submit button is pressed, the data entered by the user and the data hardcoded for this certificate template are sent to PKI Services for processing



IBM @server zSeries

zSeries Explorers

IBM

Request Submitted Successfully

Here's your transaction ID. You will need it to retrieve your certificate. Press 'Continue' to retrieve the certificate.

1jx6t3cYpU2/VkndWBrf3ls+

Continue

The request is queued to PKI Services request database for approval. The result is the return of a transaction ID



IBM @server zSeries

zSeries Explorers

IBM

Retrieve Your 1 Year PKI SSL Browser Certificate

Please bookmark this page

Since your certificate may not have been issued yet, we recommend that you create a bookmark to this location so that when you return to this bookmark, the browser will display your transaction ID. This is the easiest way to check your status.

Enter the assigned transaction ID

If you specified a pass phrase when submitting the certificate request, type it here, exactly as you typed it on the request form

Retrieve and Install Certificate

To check that your certificate installed properly, follow the procedure below:

Netscape V6 - Click Edit->Preferences, then Privacy and Security-> Certificates. Click the Manage Certificates button to start the Certificate Manager. Your new certificate should appear in the Your Certificates list. Select it then click View to see more information.

Netscape V4 - Click the Security button, then Certificates-> Yours. Your certificate should appear in the list. Select it then click Verify.

Internet Explorer V5 - Click Tools->Internet Options, then Content, Certificates. Your certificate should appear in the Personal list. Click Advanced to see additional information.

Home page



IBM @server zSeries

zSeries Explorers

IBM

Internet Explorer Certificate Install

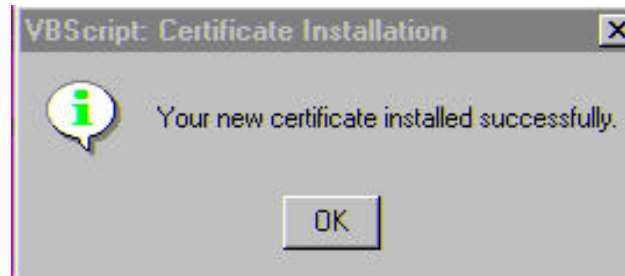
Click "Install Certificate" to store your new certificate into your browser

Install Certificate

Home page

If the certificate has been issued, it may be installed.

This page shows how it would look for Microsoft's IE browser





IBM @server zSeries

zSeries Explorers



5 Year PKI SSL Server Certificate

Choose one of the following:

- Request a New Certificate

Enter values for the following field(s)

Pass phrase for securing this request. You will need to supply this value when retrieving your certificate

Reenter your pass phrase to confirm

Selecting a server certificate template from the main page presents a dialog to enter a PKCS#10 request

Base64 encoded PKCS#10 certificate request

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBfTCB5wIBADAOMQwwCgYDVQQDEwNKaW0wgZ8wDQYJKoZIhvcNAQEBBQADgYOA
MIGJAoGBANVudl7GpgE83s80S7cNBqignYpS0rClrrNQ1ArhMKjRNRvE5Mb5scR3
/n7S5doPGhioXrLWEstNia9QbPaQ2RHf0S791lm0/nRrQTdbAjmPyz8SAbl1cpZR
ElSf9F/2Plxs54AuPh8YfPK0bpjLN3o8jQAMC7LG4fvw+cYivuIJAgMBAAGgMDAu
BgkqhkiG9w0BCQ4xITAfMBOGA1UdDgQWBBQivwx39S/oc4MbD/1YxNexaWAZMzAN
BgkqhkiG9w0BAQUFAA0BgQBulYhQTfxyRvjf1BQM01QXV9Ud0jLjDgefeyexfg/
CsP75FqFp/E3SndZHjHX9kF9YOH0cEEVnkFSCK0w6pnTQnCHDoIz0BZ13zHHX5oC
ljn7NdBpcsgZiuMC/kZBmcxv2PkCbK0lt7kaRvvXOCegKB+vOu4lu0sCMgM/khls
7E==
-----END NEW CERTIFICATE REQUEST-----
```

Submit certificate request

Clear



Here's Your Certificate. Cut and Paste it to a File

```
-----BEGIN CERTIFICATE-----
MIICFTCCAX6gAwIBAgIBeDANBgkqhkiG9w0BAQUFADBQMwswCQYDVQQGEwJVUzEM
MAoGA1UEChMDSUJNMS4wLAYDVQQLEyVidWlhb3BzZXNvdXJjZXNMGQ2VydGlmawNh
dGUgQXV0aG9yaXR5MB4XDTAxMDkyNDAAQMDAwMFoXDTA2MDkyMzAzNTk1OVowDjEM
MAoGA1UEAxMDSmltMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDVbndexqYB
PN7PDku3DQaooJ2KUjqwta6zUJQK4TC0TUbX0TG+bHEd/5+0uXaDxoYqF6ylhLL
TSGvUGz2kNkR39Eu/ddZjv50a0E3WwI5j8s/EgG5ZXKWURNUn/Rf9j9cb0eALj4f
GHzyjm6Yyzd6PIOADuYxuH78PnGlr7iCQIDAQAB0YwRDA0BgNVHQ8BAf8EBAMC
BaAwEQYDVRO0BAoECCK/DHf1L+gEMB8GA1UdIwQYMBaAFAFBGj9gTEPz4l5s5a8yge
4hdHQZ15MA0GCSqGSIb3DQEBBQUAA4GBAIVxewxfSgAIB8xQNYZ0c9v0jd0i3aCy
PXEjduxTl8/4mmbi7BD02eFX8G5tyhCjpZyf44KzMx7pszjnZGYWdwef4tLW8XGF
zVpfu2hl+esYnCFPPFM/3jBJ+BNn4qaPi/LfZ7IshMz8u6PEalC6WQw2DjuPzYOC
UjHxeIRq2xsY
-----END CERTIFICATE-----
```

Server certificates are returned in base64 encoded form.



Renew or Revoke a Browser Certificate

Here is the certificate you selected:

Requestor	Serial #/Certificate Names / Validity	Usage	Status	Date
Joe Coffee	Serial #: 12345 Template: 1 Year PKIX Browser Certificate	handshake dataencrypt	Active	Created: 2000/04/20
	Subject: CN=Joe Coffee,OU=S390,O=IBM,C=US Issuer: OU=RACF CA,O=IBM,C=US Validity: 2000/04/20 00:00:00 - 2001/04/20 23:59:59			Modified: 2000/04/22

Field Name	Field Value
HostIdMap	jcoffee@plpsc.pok.ibm.com
HostIdMap	joc@S390vm.pok.ibm.com
AltIpAddr	9.117.35.14

If this is the correct certificate, choose one of the following:

- Renew this certificate

- Revoke this certificate

If the renew/revoke button is pressed on the main page, client authentication will drive the browser dialogs to select a certificate. If the one selected was created by this PKI CA and is not revoked, it's information will be displayed so that the user may confirm and proceed.



IBM @server zSeries

zSeries Explorers

IBM

PKISERV Certificate Generation Application

[Install our CA certificate into your browser](#)

Choose one of the following:

- Request a new certificate using a model

Select the certificate template to use as a model

The default setup has the Admin link
userid/pw protected

- Pickup a previously requested certificate

Enter the assigned transaction ID

Select the certificate return type

- Renew or revoke a previously issued browser certifi

- Administrators click here

Enter Network Password

Please type your user name and password.

Site: dceimgun.endicott.ibm.com

Realm: AuthenticatedUser

User Name

Password

☐ Save this password in your password list



IBM @server zSeries

zSeries Explorers

IBM

PKI Services Administration

Choose one of the following:

- Work With a Single Certificate Request

- Work With a Single Issued Certificate

- Specify Search Criteria For Certificates and Certificate Requests

Certificate Requests

- ☐ Show All Requests
- ☒ Show Requests Pending Approval
- ☐ Show Approved Requests
- ☐ Show Completed Requests
- ☐ Show All Rejected Requests
- ☐ Show Rejections in Which the Client Has Been Notified

Issued Certificates

- ☐ Show All Issued Certificates
- ☐ Show All Revoked Certificates
- ☐ Show All Expired Certificates
- ☐ Show Non-Expired Non-Revoked Certificates Only
- ☐ Show Non-Expired Certificate Revocations Only

Additional Search Criteria (Optional)

Requestor's Name

Show Recent Activity Only

Work with one request or certificate directly by entering its transaction ID or serial number. Or

Query requests or issued certificates based on some criteria

Requestor's name and/or time period may be used as additional search criteria.



IBM @server zSeries

zSeries Explorers



Certificate Requests

The following certificate requests matched the search criteria specified:

Select	Requestor	Certificate ID / Certificate Names / Validity	Usage	Status	Date
<input checked="" type="checkbox"/>	Joe Coffee	Trans ID: b2b1le/cRqZDsb2b1le/cRq Previous Serial #: 732686 Subject: CN=Joe Coffee,OU=S390,O=IBM,C=US Issuer: OU=RACF CA,O=IBM,C=US Validity: 2000/04/20 00:00:00 - 2001/04/20 23:59:59			
<input checked="" type="checkbox"/>	Peter Jones	Trans ID: YA0znG2JvMbvysb2b1le/cRq Template: 1 Year PKIX Browser Certificate Serial #: 00945686 Subject: CN=Peter Jones,OU=S390,O=IBM,C=US Issuer: OU=RACF CA,O=IBM,C=US Validity: 2000/04/20 00:00:00 - 2001/04/20 23:59:59			Modified: 2000/04/22
<input checked="" type="checkbox"/>	Sam Smith	Trans ID: sitncG2JvMbvysb2b1le/cRq Template: 1 Year PKIX Browser Certificate Subject: CN=Sam Smith,OU=S390,O=IBM,C=US Issuer: OU=RACF CA,O=IBM,C=US Validity: 2000/04/21 00:00:00 - 2001/04/21 23:59:59	handshake	Approve	
<input checked="" type="checkbox"/>	John Q. Public	Trans ID: YA0znGasncwyc1b2b1le5cRq Template: 1 Year PKIX Browser Certificate Serial #: 00945692 Subject: CN=John Q. Public,OU=S390,O=IBM,C=US	handshake	Approve	

Querying requests would produce a list of requests with some summary data displayed for each. A maximum of ten requests would be displayed on one page. (scroll to see more...)

Presence of previous serial # indicates renewal

Presence of serial # indicates certificate has been created.

These are hypertext links

Select button used to select multiple requests

Choose on



IBM @server zSeries

zSeries Explorers

IBM

		Issuer: OU=RACF CA,O=IBM,C=US Validity: 2000/04/21 00:00:00 - 2001/04/21 23:59:59	
<input checked="" type="checkbox"/>	John Q. Public	Trans ID: YA0znGasncwyc1b2b1le5cRq Template: 1 Year PKIX Browser Certificate Serial #: 00945692 Subject: CN=John Q. Public,OU=S390,O=IBM,C=US Issuer: OU=RACF CA,O=IBM,C=US Validity: 2000/04/21 00:00:00 - 2001/04/21 23:59:59	h

(After scrolling...)

To obtain more information for a particular request or certificate, administrator would click the link

Presence of template name indicates request is not a renewal

Choose one of the following:

- Click on a transaction ID to see more information or to modify individually
- Select and take action against multiple requests at once

Action Comment (Optional)

Note - The "all requests selected above that are" actions should not be displayed unless there is at least 1 request that can be altered by such an action, e.g., don't display Approve all requests selected above that are "Pending Approval" unless there are some requests pending approval

- Approve without modification all requests selected above that are "Pending Approval"

- Reject all requests selected above that are "Pending Approval"

Links provided to display the next set of ten requests or redo the search

To take a global action against multiple requests such as "approve", user would select the requests then click the action



IBM @server zSeries

zSeries Explorers



Modify and Approve Request

Requestor	Certificate ID	Dates
Joe Coffee	Trans ID: b2b1le/cRqZDsb2b1le/cRqa Previous Serial #: 732686	Created: 2000/04/20 Modified: 2000/04/22

You may modify the following fields by providing new values. To remove a field simply blank it out.

Common Name

Organizational Unit

Organization

Country

Date certificate becomes valid Date certificate expires (at end of day)

2000 04 20 2001 04 20

Indicate the intended purpose for the certificate

Protocol handshaking (e.g., SSL)
Data encryption
Certificate signing
Document signing (nonrepudiation)

The modify action allows "Pending Approval" requests to be approved with modifications. HTML controls for each admin modifiable field will be presented with current values if any.

List of modifiable fields is customizable in certificate templates file

(scroll to see more...)



IBM @server zSeries

zSeries Explorers

IBM

Date certificate becomes valid Date certificate expires (at end of day)

2000 04 20 2001 04 20

Indicate the intended purpose for the certificate

Protocol handshaking (e.g., SSL)
Data encryption
Certificate signing
Document signing (nonrepudiation)

HostIdMappings Extension value(s) in subject-id@host-name form

jcoffee@plpsc.pok.ibm.com
joec@s390vm.pok.ibm.com

IP address in dotted decimal form

9.117.35.14

Action Comment (Optional)

Approve

- Approve the request with the modifications specified above

Reset Modified Fields

(after scrolling...)

HostId Mappings can
also be specified or
modified

User clicks on "Approve"
to commit changes



IBM @server zSeries

zSeries Explorers



Issued Certificates

The following issued certificates matched the search criteria specified:

Select	Requestor	Certificate Names / Validity	Usage	Status	Date
<input checked="" type="checkbox"/>	Joe Coffee	Serial #: 12345 Template: 1 Year PKIX Browser Certificate Subject: CN=Joe Coffee,OU=S390,O=IBM,C=US Issuer: OU=RACF CA,O=IBM,C=US Validity: 2000/04/20 00:00:00 - 2001/04/20 23:59:59	handshake dataencrypt	Active	Created: 2000/04/20 Modified: 2000/04/22
<input checked="" type="checkbox"/>	Sam Smith	Serial #: 732686 Template: 1 Year PKIX Browser Certificate Subject: CN=Sam Smith,OU=S390,O=IBM,C=US Issuer: OU=RACF CA,O=IBM,C=US Validity: 2000/04/21 00:00:00 - 2001/04/21 23:59:59	handshake	Revoked	Created: 2000/04/20 Modified: 2000/04/22

Choose one of the following:

- Click on a serial number to see more information or to revoke or delete certificate
- Select and take action against multiple certificates at once

Action Comment (Optional)

Note - Action for "Revoke" should only be displayed if at least 1 cert has status "Active"

Revoke

No Reason

- Revoke all certificates selected above that are "Active"

Delete

- Delete all certificates selected above

Get Next 10 Matching Certificates

Hypertext links take you straight to the certificate where more information is displayed

Select button used to select multiple certificates



IBM @server zSeries

zSeries Explorers

IBM

Reference

✓ **Security Server Manuals:**

- ✓ PKI Services Guide and Reference (SA22-7693)
- ✓ RACF Command Language Reference (SC28-1919)
- ✓ RACF Security Administrator's Guide (SC28-1915)
- ✓ RACF Callable Services Guide (SC28-1921)
- ✓ LDAP Administration and Use (SC24-5923)
- ✓ OCEP Application Programming (SC24-5925)

✓ **Cryptographic Services**

- ✓ OCSF Service Provider Developer's Guide and Reference (SC24-5900)
- ✓ ICSF Administrator's Guide (SA22-7521)

✓ **IBM HTTP Server Manuals:**

- ✓ Planning, Installing, and Using (SC31-8690)

✓ **Other Sources:**

- ✓ PKIX - <http://www.ietf.org/html.charters/pkix-charter.html>
- ✓ **ITSO Redbook SG24-6968 in preparation**



zSeries Explorers



IBM @server zSeries

PKI Services

Como economizar dinheiro explorando este novo componente do z/OS Security Server

Vicente Ranieri Júnior

IBM Senior Certified Consulting IT Specialist

ranieri@br.ibm.com