SHARE
Technology • Connections • Results

Managing Certificate Cost Effectively

Anaheim,CA
8644

Jonathan M. Barney, CISSP
IBM Corporation
STG Lab Services and Training
e-mail: jmbarney@us.ibm.com

Trademarks

SHARE
Technology · Connections · Results

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

- CICS*
- DB2*
- IBM*
- IBM (logo)*
- OS/390*
- RACF*
- Websphere*
- z/OS*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Identrus is a trademark of Identrus, Inc
VeriSign is a trademark of VeriSign, Inc
Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the 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.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

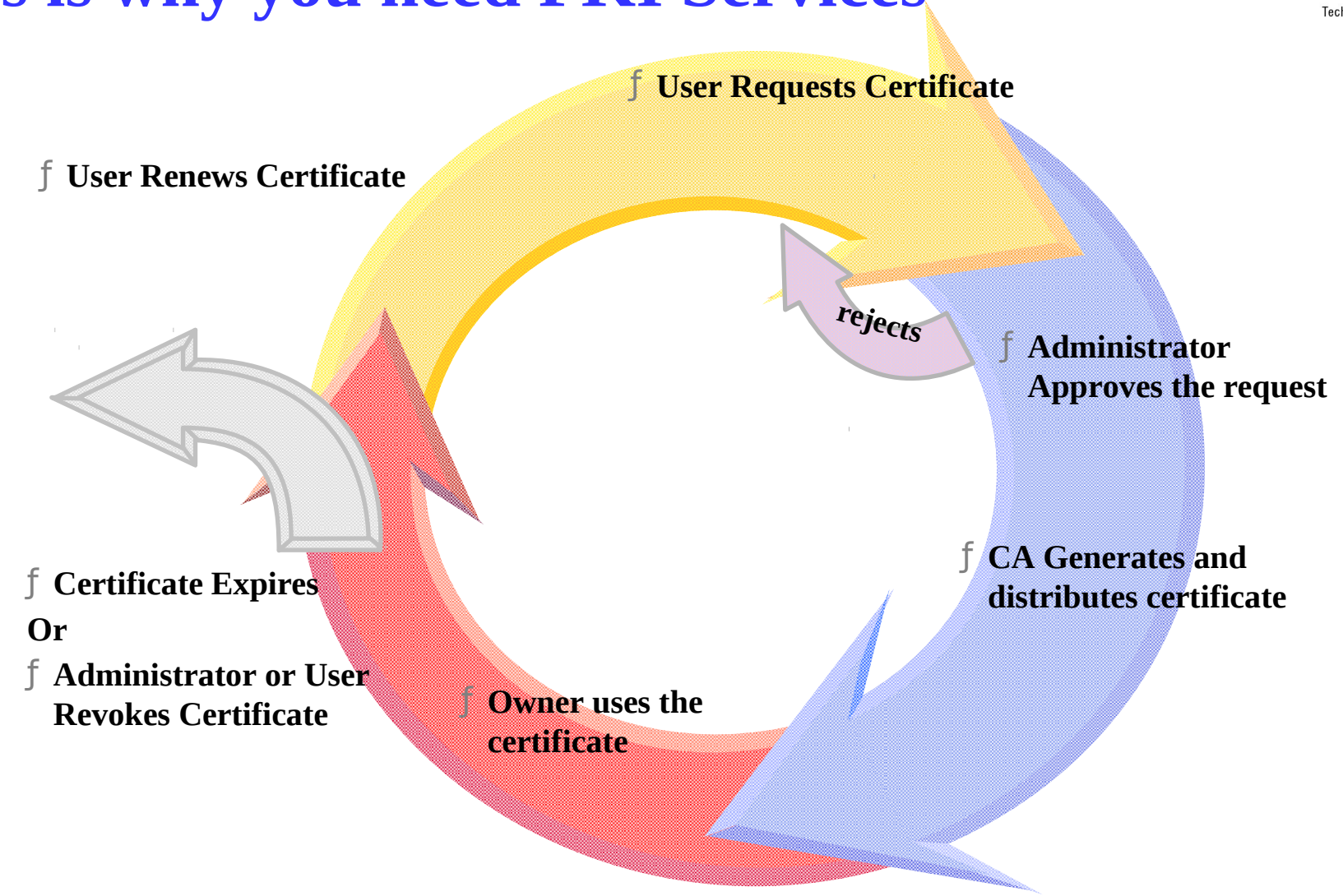
Z/OS PKI Services review

Certificate Authority on z/OS

- PKI Services
  - Request, create, renew, revoke certificate
  - Provide certificate status through Certificate Revocation List(CRL) and Online Certificate Status Protocol (OCSP)
  - Generation and administration of certificates via customizable web pages
  - Support Simple Certificate Enrollment Protocol (SCEP) for routers to request certificates automatically

Certificate Life Cycle –

This is why you need PKI Services



Overview

- A component on z/OS since V1R3
- Closely tied to RACF
  - The CA cert must be installed in RACF's key ring
  - Authority checking goes through RACF's callable service
- **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
  - Support multiple revocation checking mechanisms
    - Certificate Revocation List (CRL)
    - Online Certificate Status Protocol (OCSP)
  - Certificates and CRLs can be posted to LDAP

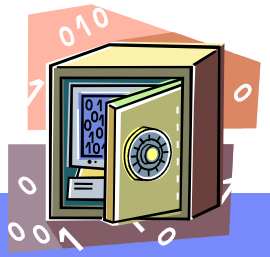
Overview (contd)

- Provides email notification
  - to notify end user for completed certificate request and expiration warnings
  - to notify administrator for pending requests
  - to send the automatic renewed certificate

Benefits of using PKI Services on z/OS

SHARE
Technology · Connections · Results

- Not a priced product. Licensed with z/OS. An alternative to purchasing third party certificates
- IdenTrust™ compliant
  - ensures adherence to a common standard to provide a solid foundation for trust between financial institutions and their customers
- Relatively low mips to drive thousands of certificates
- Leverage existing z/OS skills and resources
- Cost efficient for banks, government agencies to host Digital Certificate management
- Run in separate z/OS partitions (integrity of zSeries® LPARs)
- Scalable (Sysplex exploitation)
- Secure the CA private key with zSeries cryptography



Customization

- **Configuration file** - pkiserv.conf (used by the PKI Services daemon)
  - Contains mainly setup information for PKI Services
  - May contain certificate information applies to all types of certificates that PKI Services creates
- **Template file** - pkiserv.tmpl (used by the PKI Services CGIs)
  - pkitmpl.xml (used by PKI Services JSPs)
  - Provides different types of certificate template
    - Browser certificate – key generated by browser
    - Server certificate – key generated by server
    - Key certificate – key generated by PKI CA
  - Each template contains certificate information that is specific to a certain type of certificate
    - S/MIME, IPSEC, SSL, CA, Windows Logon…

A Customer Implementation Example

Goals of the Implementation

SHARE
Technology · Connections · Results

- **Deploy a new internal PKI infrastructure (CA/RA)**
- **Manage the lifecycle for certificates issued internally**
- **Support X.509 authentication and identify verification for various authentication mechanisms**
- **Explore methods for delivering CA Root certificate chain to users**
- **Create security policies around certificate usage to encompass the new system**
- **Augment existing Asset Management and governance**
- **Create a business case/Cost reduction**
- **Improve Security by removing barriers to obtaining signed certificates and enforcing stricter certificate usage policies**

Issues

- **Chicken and Egg- How to test internal Certificate Authority pilot when users don't have Root certificates?**
- **How to deploy new trusted root certificates in an enterprise?**
- **How to validate certificate requests for various certificate types?**
- **How to set and enforce new certificate policies**
- **Automation**
  - **Certificate trust and issuance**
  - **Certificate deployment**

Certificate Policies

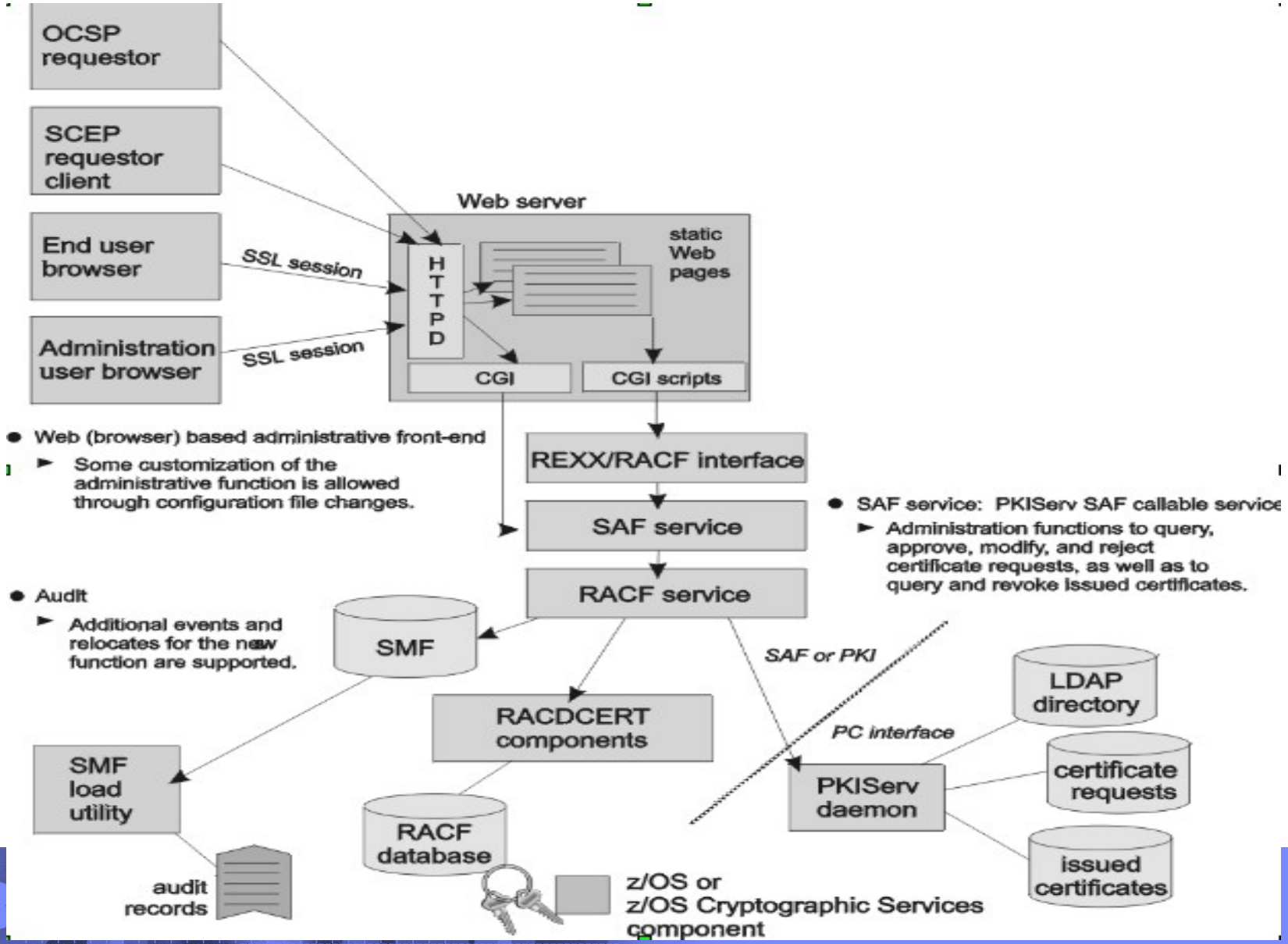
- How will the certificate be used? What are acceptable uses?
- What are acceptable certificate stores?
- Who will be the certificate authority?
- What is the identity's subject name?
- What are the size of the public/private keys?
- Whether additional identity information is to be added to the certificate?
- What label or nickname will the certificate be known by?
- How to enforce these policies?
- How to save time through automation?
- What credentials, proofs of identity and secondary approvals are required by the Registration Authority

Public Key Infrastructure

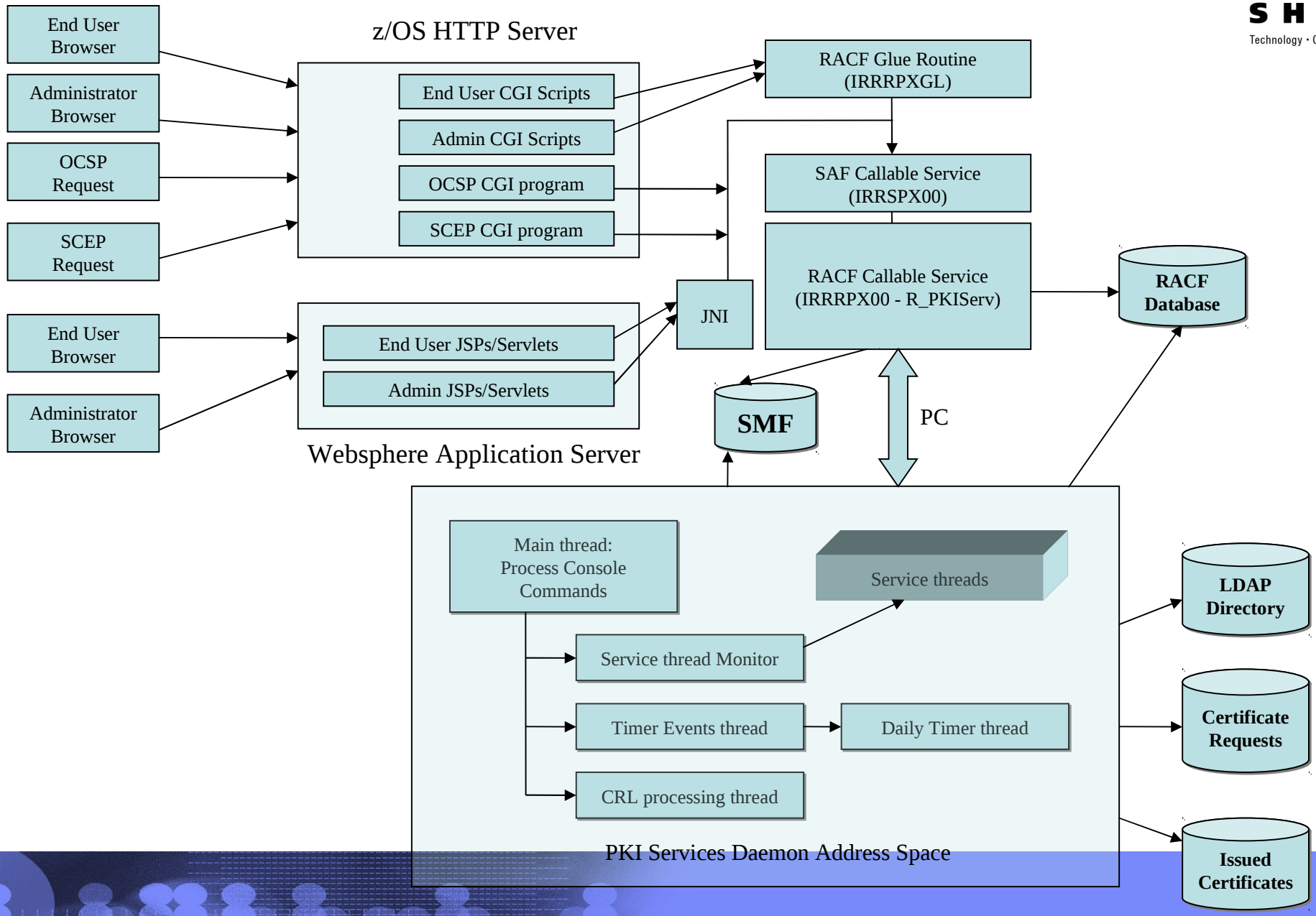
SHARE
Technology • Connections • Results

- **“Personal Certificates” are issued to any user in the Enterprise Directory LDAP and can be used for Wireless client access and SSL Client Authentication**
- **“Server Certificates” are issued to internal Websites and BSO Firewalls for use as SSL Server Certificates**
- **“Middleware Certificates” are issued to WebSphere MQ Queue Managers**
- **“Application Certificates” are issued to individual applications that require Certificates for a variety of purposes that do not include SSL client or server authentication**
- **“Web Services Certificates” are issued to applications hosting WS-Security enabled Web services**
- **Code signing**
- **Server to server proxy**

zPKI Services Architecture – Out of the box



zPKI Services Architecture

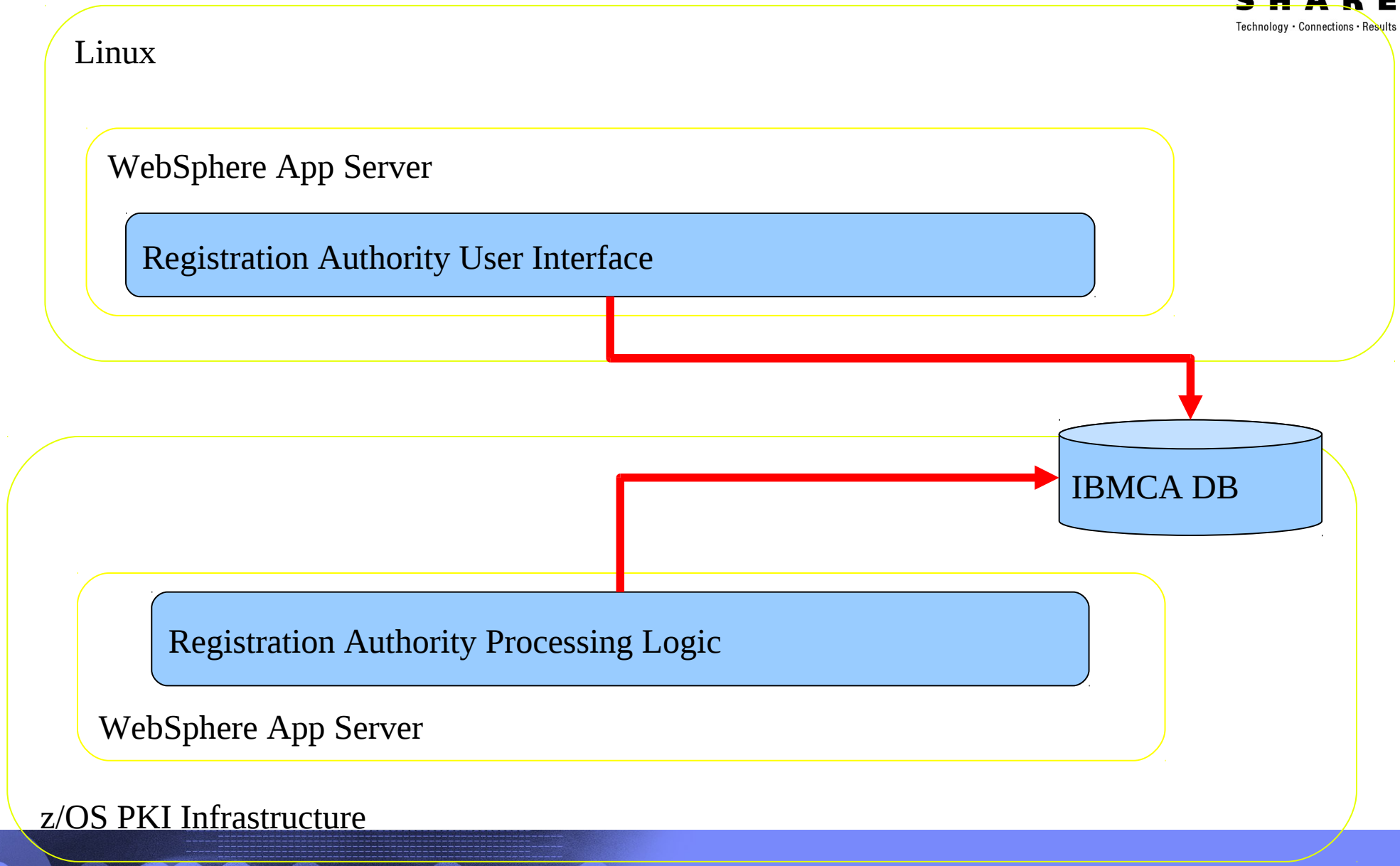


IBM CA Pilot

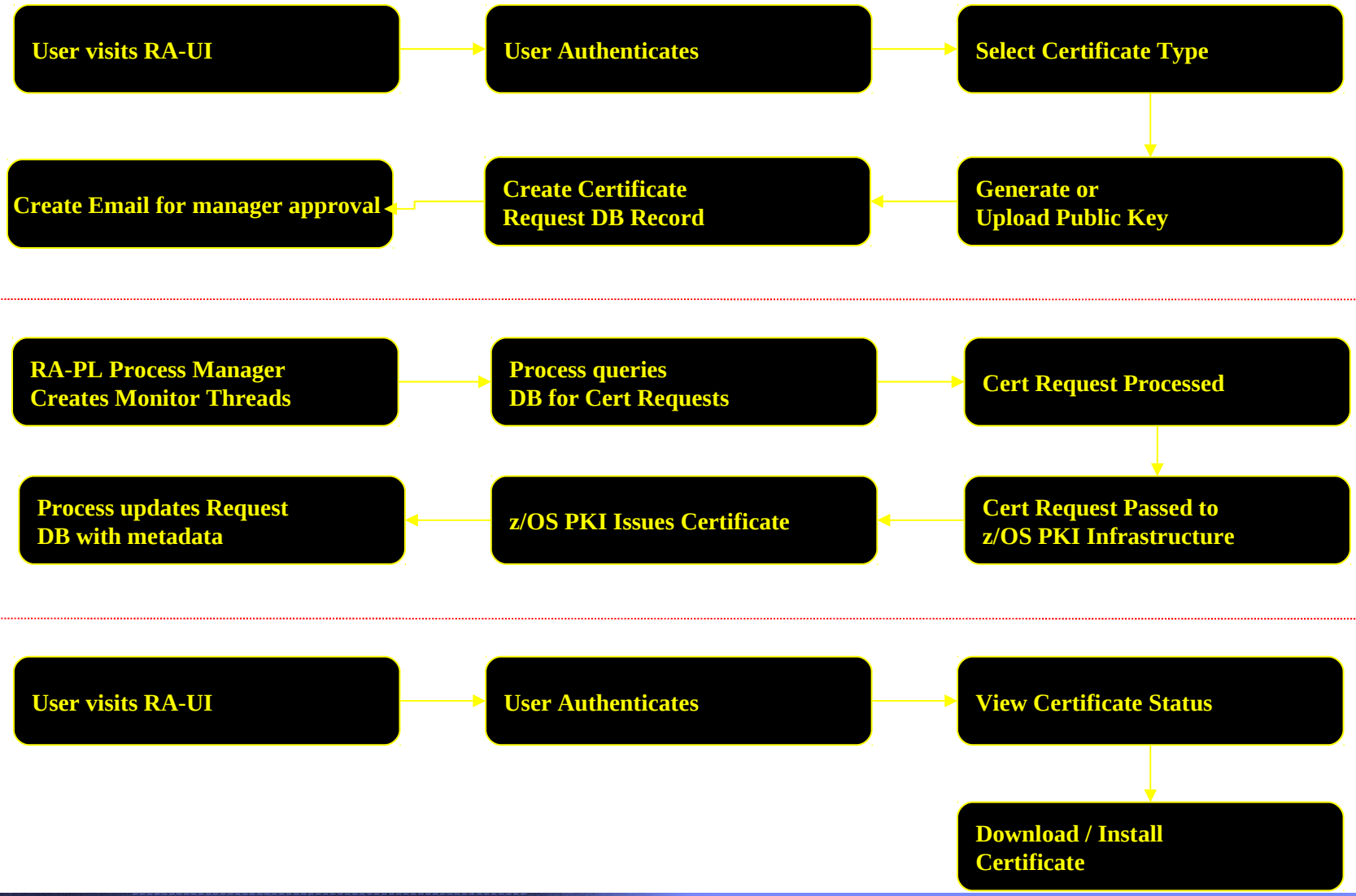
SHARE
Technology · Connections · Results

- **The application is split into three distinct components**
  - The RA User Interface
  - The RA Processing Logic
  - The RA Metadata Database
- **There is no direct communication between the RA User Interface and the Processing Logic. The application is essentially a State machine.**
- **When a certificate request is created, a new record is created in the RA Metadata Database with a State of "CREATED"**
- **Worker processes in the RA Processing Logic monitors the database for CREATED requests, then validates those requests based on criteria specific to each type of certificate**
- **Another Worker process monitors the database for SUBMITTED requests, and will send those to the z/OS PKI infrastructure via the z/OS PKI Java Native Interface API.**
- **Once the certificate is issued, a copy of the certificate is stored in the Metadata Database.**
- **Users can go to the RA User Interface to monitor request status and download the certificate when it is available.**

The IBMCA Pilot



The IBMCA Pilot



IBM CA Pilot

SHARE
Technology · Connections · Results

- **The application allows for three distinct methods of generating public/private key pair**
  - Users can use their Web Browser's built-in key generation support to generate keys
  - Users can use an external tool such as Java's keyman or OpenSSL to generate Certificate Signing Requests
  - Users can ask the z/OS PKI Infrastructure to generate and manage the public/private key pairs

- **Most modern Web browsers support the ability to generate public/private keys using either built-in tags (e.g. <keygen />) or, in the case of Microsoft Internet Explorer, using a special ActiveX control. The public and private keys are stored in an encrypted store that is specific to that browser instance which means the Digital Certificate must be installed into that specific browser or else it is useless. Once the cert is installed, it can be exported with the private key to a file that can be used with other applications.**

- **If users use iKeyman,OpenSSL,RACDCERT etc. to generate certificate signing requests, they can either upload or cut-and-paste the CSR into the RA-UI interface. It is up to the user to manage their public/private key pair**

- **If the z/OS infrastructure is asked to create the key pair, special handling is required to export the certificate and the private key securely. This option is not desirable because it means that the private key is shared by more than one individual (the user and the PKI Infrastructure)**

PKI is about Trust

Question: Why would you trust a certificate issued from IBMCA ?

- **CA root certificates are protected by FIPS1402-3 crypto hardware**
- **Personal Certificates**
  - Authentication for certificate request is through Enterprise Director
  - Certificate request is populated through RA business logic
  - Certificate requests are management approved
- **CA Registry: a repository of profiles.**
- **Authentication to the Registry is through Enterprise director**
- **Validation of profiles is through manager approval**
- **Each profile is composed with:**
  - A Distinguished Name.
  - A type of resource: WebServer, Boundary Firewall, Queue Manager, Application, Web Service, Other.
  - An extended list of owners.

What we tested with “personal” certificates

SHARE
Technology · Connections · Results

- **WAS Clientauth – replacement for authentication with intranet id/password**
- **WAS with TAI – Clientauth if personal certificate is present, fail back to id/pw if not**
- **Wireless authentication**
- **BSO authentication**
- **Server to server proxy**
- **VPN authentication**

"Server" certificates

- Apache – openssl keystore
- OPEN VPN – Openssl Keystore
- IBM HTTPD web server -CMS, RACF keystore
- WAS – PKCS12 , RACF, JCEKS
- LDAP-RACF
- MQUEUE- RACF, CMS
- iNotes

Deploying Root Certificates

- Manually though download
- Included on new system images
- Through update rules
- Bundled as Firefox extension package
- PKCS7b

Shipped sample reques

PKI Services Certificate Generation Application

Install our CA certificate into your browser

Shipped sample

Choose one of the following:

- **Request a new certificate using a model**

  Select the certificate template to use as a model 1-Year PKI SSL Browser Certificate

  Request Certificate

- **Pick up a previously requested certificate**

  Enter the assigned transaction ID

  Select the certificate return type PKI Browser Certificate

  Pick up Certificate

- **Renew or revoke a previously issued browser certificate**

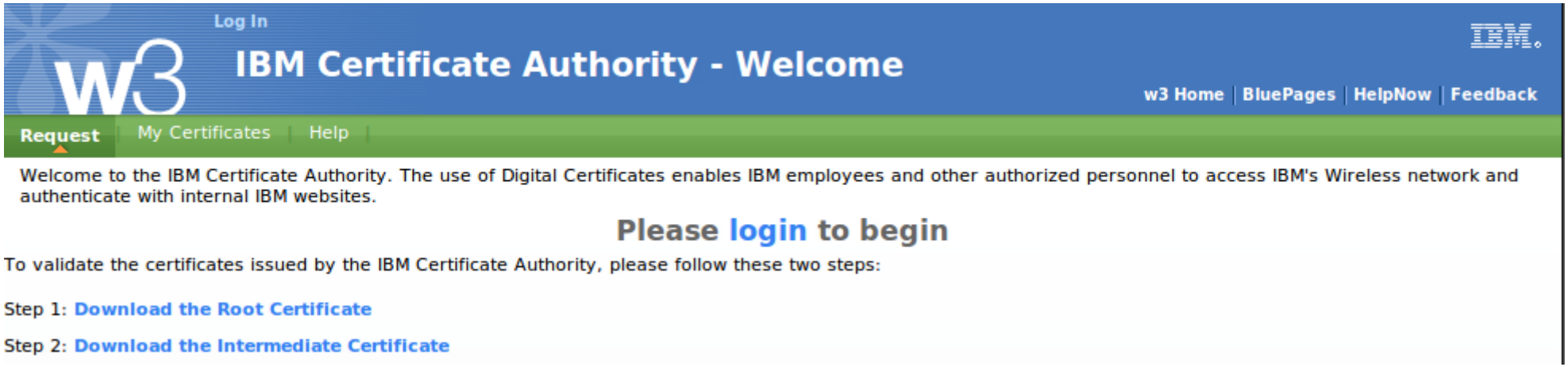
  Renew or Revoke Certificate

- **Administrators click here**

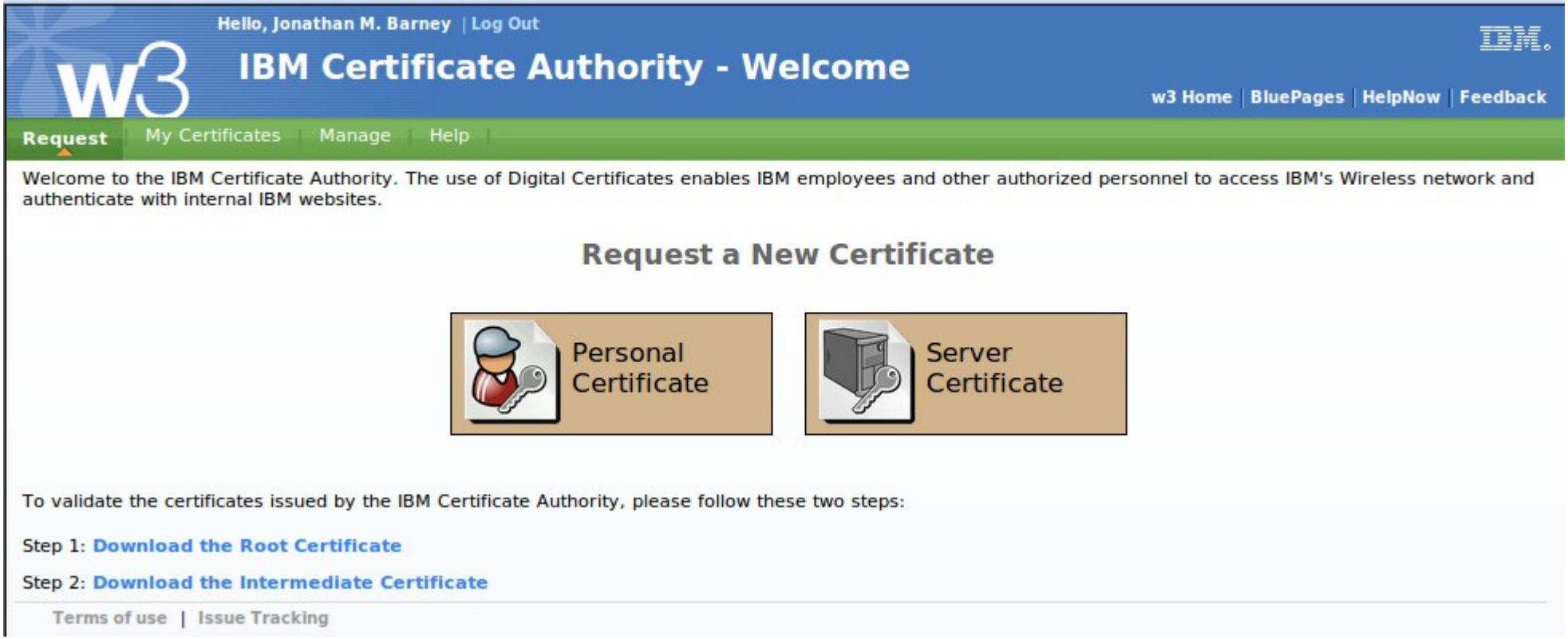
  Go to Administration Page

email: webmaster@your-company.com

IBM Custom RA



Request



Request a Personal Certificate

SHARE
Technology · Connections · Results

Hello, Jonathan M. Barney | Log Out

IBM Certificate Authority - Personal Certificate

w3 Home | BluePages | HelpNow | Feedback

Request | My Certificates | Manage | Help

Personal Certificate

Personal Certificates are used to provide both SSL/TLS Client Authentication as an alternative to the IBM Intranet ID and Password and for use with the IBM Internal Wireless infrastructure.

Key Generation

To request a certificate, a public and private key pair must be generated. The **private** key must be kept secret by the user requesting the certificate. The **public** key must be sent to the IBM Certificate Authority to be used in the creation of the Digital Certificate. There are several methods available for creating the private and public keys. The determination of which method to use depends entirely on your requirements. Please select from one of the three key generation options below.

- (●) Use the browser to generate the public/private key pair. If you select this option, your Web browser will generate keys and store the private key in an encrypted database managed by the browser. The public key will be sent to the server to process the certificate request. The resulting Digital Certificate **must** be downloaded and installed on the same machine, and in the same browser that was used to submit the request or the private key cannot be recovered and the certificate will not be usable. Please select the key strength from the options below.

  Key Strength: 2048 (High Grade)

- ( ) Use a tool such as Java's Keyman utility or OpenSSL to generate a Certificate Signing Request and use the form below to upload it to the server for processing.

  CSR: Choose File No file chosen

- ( ) As an alternative to uploading the Certificate Signing Request file, you can cut and paste the Base64-encoded Certificate Signing Request into the text box below.

  CSR:

- ( ) Have the backend PKI Infrastructure generate and store the public/private keys. The Private key will be encrypted and protected in a highly secure storage environment. Use of this option is discouraged as it requires the private key to be stored in a location that is not under the direct control of the Certificate owner. To use this option, you must provide a PIN that will be used to secure the private key. You will be required to provide the PIN when attempting to download the issued certificate.

  PIN:

Submit | Cancel

Terms of use | Issue Tracking

Request a Server Cert

SHARE
Technology · Connections · Results

Hello, Jonathan M. Barney | Log Out

IBM Certificate Authority - Server Certificate

w3 Home | BluePages | HelpNow | Feedback

Request | My Certificates | Manage | Help

Server Certificate

Server Certificates are used to provide SSL/TLS Server Authentication for secure websites deployed within the protected IBM Intranet Environment, as well as for WebSphere MQ middleware instances. Such systems must be registered with the **Profile Registry** before a certificate can be requested and issued.

Below is a listing of profiles in the System Registry for which you are marked as either a Business or Security owner.

To request a Server Certificate, select the Profile from the list, then select a Key Generation method, and press "Submit".

Select a Server

Profile: test 2 (CN=test 2 name,OU=CIO,L=NEW YORK,ST=NEW YORK,C=SM)

Don't see the Profile you want? **Create a new one.**

Key Generation

To request a certificate, a public and private key pair must be generated. The **private** key must be kept secret by the user requesting the certificate. The **public** key must be sent to the IBM Certificate Authority to be used in the creation of the Digital Certificate. There are several methods available for creating the private and public keys. The determination of which method to use depends entirely on your requirements. Please select from one of the three key generation options below.

- Use a tool such as Java's Keyman utility or OpenSSL to generate a Certificate Signing Request and use the form below to upload it to the server for processing.

  CSR: Choose File No file chosen

- As an alternative to uploading the Certificate Signing Request file, you can cut and paste the Base64-encoded Certificate Signing Request into the text box below.

  CSR:

- Have the backend PKI Infrastructure generate and store the public/private keys. The Private key will be encrypted and protected in a highly secure storage environment. Use of this option is discouraged as it requires the private key to be stored in a location that is not under the direct control of the Certificate owner. To use this option, you must provide a PIN that will be used to secure the private key. You will be required to provide the PIN when attempting to download the issued certificate.

  PIN:

Submit | Cancel

Retrieve a cert

Hello, Jonathan M. Barney | Log Out

IBM Certificate Authority - Certificate Detail

w3 Home | BluePages | HelpNow | Feedback

Request | My Certificates | Manage | Help

Certificate Detail

Type / Status	Subject / Serial	Created	Issued	Expires	Revoked	Actions
Personal / Issued	Jonathan M. Barney / 01:33	03-03-2010	03-03-2010	03-02-2011		Select »

Fingerprint: 3d:53:83:34:c8:d1:30:92:56:b2:48:df:fc:ed:9d:86

Processing History

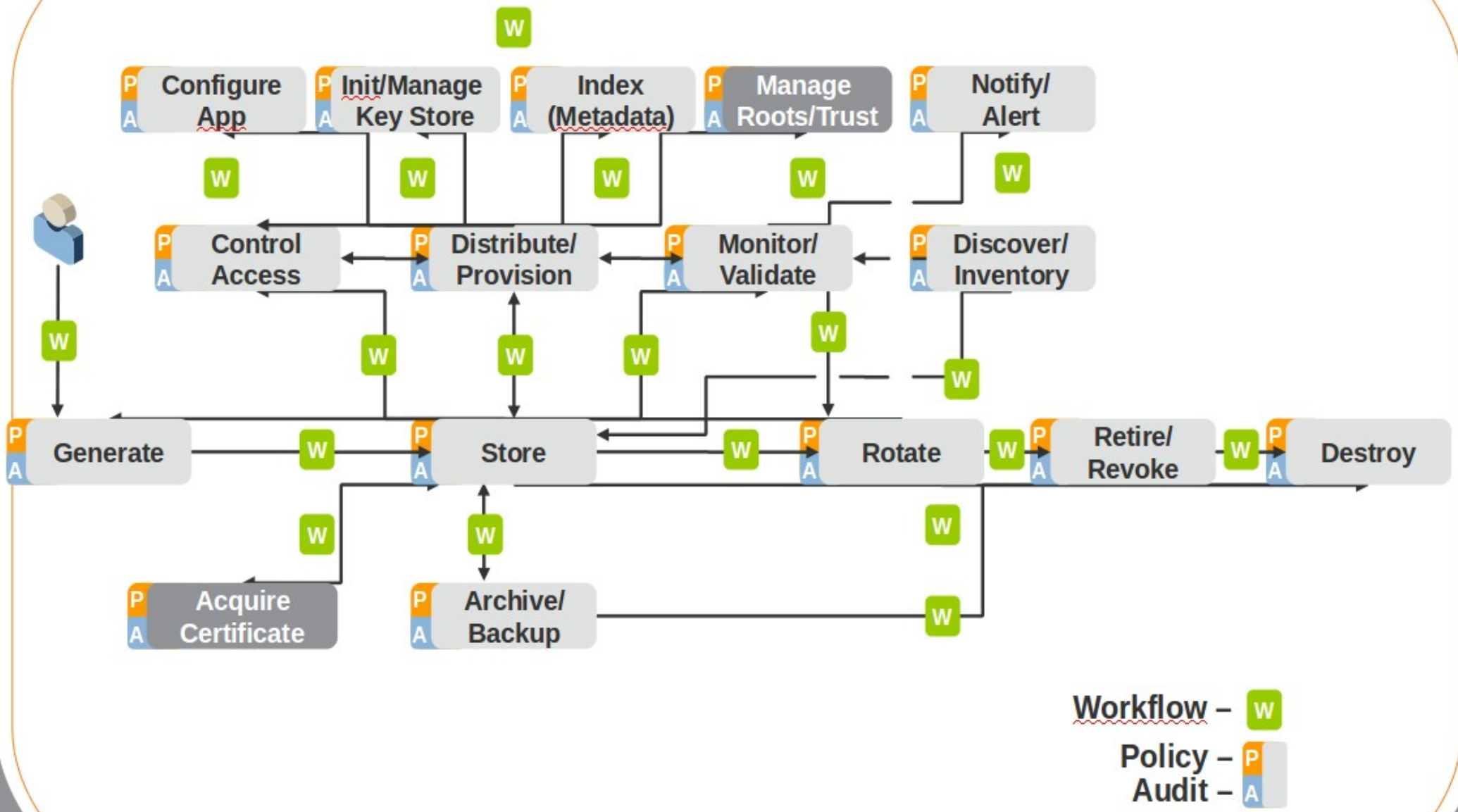
When	Status	Who	Notes
03-03-2010	Issued	ZOSPKI	
03-03-2010	Submitted	SYSTEM	
03-03-2010	Approved	SYSTEM	
03-03-2010	Pending	SYSTEM	
03-03-2010	Created	Jonathan M. Barney	

Base64-encoded X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIINxgYJKoZIhvcNAQcCoIINtzCCDbMCAQExADALBgkqhkiG9w0BBwGggg2bMIIF
xzCCA6+gAwIBAgICATMwDQYJKoZIhvcNAQEFBQAwSzEQMA4GA1UEChMHaWJtLmNv
bTETMBEGA1UECxMKQ01PIE9mZmljZTEiMCAGA1UEAxMZSUJNIE1udGVybWVkaWF0
ZSBDQSBQaWxvdDAeFw0xMDAzMDMwNTAwMDBaFw0xMTAzMDMwNDU5NTlaMG8xEDAO
```

Traditional Key Certificate Management

The Operational Reality Management



Business case

To create a business case, the current “certificate story” must be understood

In a complex enterprise how can certificates be tracked?

Venafi Encryption Director was used for certificate discovery

Next steps

Production

Deeper business logic

Integrated asset management, federation

SCEP

CMP

REST

CLOUD

Clients that were tested

References

- **PKI Services web site:**

http://www.ibm.com/servers/eserver/zseries/zos/pki

- **PKI Services Red Book:**

http://www.redbooks.ibm.com/abstracts/sg246968.html

References (Continued)

- Cryptographic Services
  - PKI Services Guide and Reference (SA22-7693)
  - OCSF Service Provider Developer's Guide and Reference (SC24-5900)
  - ICSF Administrator's Guide (SA22-7521)
  - System SSL Programming (SC24-5901)
- IBM HTTP Server Manuals:
  - Planning, Installing, and Using (SC31-8690)
- Other Sources:
  - PKIX - http://www.ietf.org/html.charters/pkix-charter.html

Disclaimer

- The information contained in this document is distributed on as "as is" basis, without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in its own operational environment.
- In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used. Functionally equivalent programs that do not infringe IBM's intellectual property rights may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.
- It is possible that this material may contain references to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.
- IBM retains the title to the copyright in this paper as well as title to the copyright in all underlying works. IBM retains the right to make derivative works and to republish and distribute this paper to whomever it chooses.