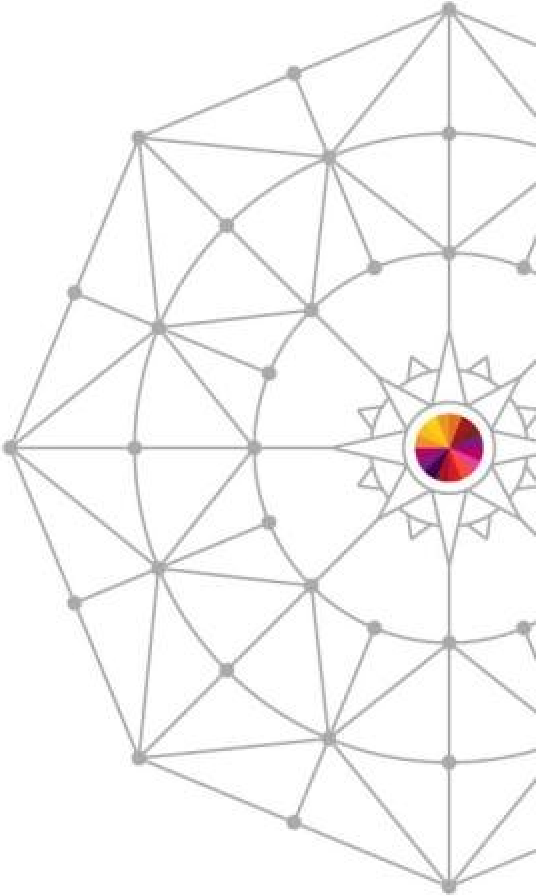
z/OS PKI Services Hands-on Lab

Ross Cooper, CISSP®
IBM Corporation

March 13th, 2014
Session: 14964



Trademarks

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

AIX*
BladeCenter*
BookManager*
CICS*
DataPower*
DB2*
DFSMS
DFSMSdss
DFSMShsm
DFSMSrmm
DFSORT
Domino*
DS6000
DS8000*
FICON*
IBM*
IBM eServer
IBM logo*
IMS
InfinBand
Language Environment*
MVS
Parallel Sysplex*
ProductPac*
RACF*
Redbooks*
REXX
RMF
ServerPac*
SYSREXX
System Storage
System x*
System z
System z9
System z10
System z10 Business Class
Tivoli*
WebSphere*
z10
z10 BC
z10 EC
zEnterprise*
zSeries*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds 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.

Windows Server and the Windows logo are trademarks of the Microsoft group of countries.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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

Java and all Java based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

* Other product and service names might be trademarks of IBM or other 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.

This information provides only general descriptions of the types and portions of workloads that are eligible for execution on Specialty Engines (e.g, zIIPs, zAAPs, and IFLs) ("SEs"). IBM authorizes customers to use IBM SE only to execute the processing of Eligible Workloads of specific Programs expressly authorized by IBM as specified in the “Authorized Use Table for IBM Machines” provided at www.ibm.com/systems/support/machine_warranties/machine_code/aut.html (“AUT”). No other workload processing is authorized for execution on an SE. IBM offers SE at a lower price than General Processors/Central Processors because customers are authorized to use SEs only to process certain types and/or amounts of workloads as specified by IBM in the AUT.

Agenda

- **PKI Services Overview**
- PKI Services **Lab**

Digital Certificate support on z/OS

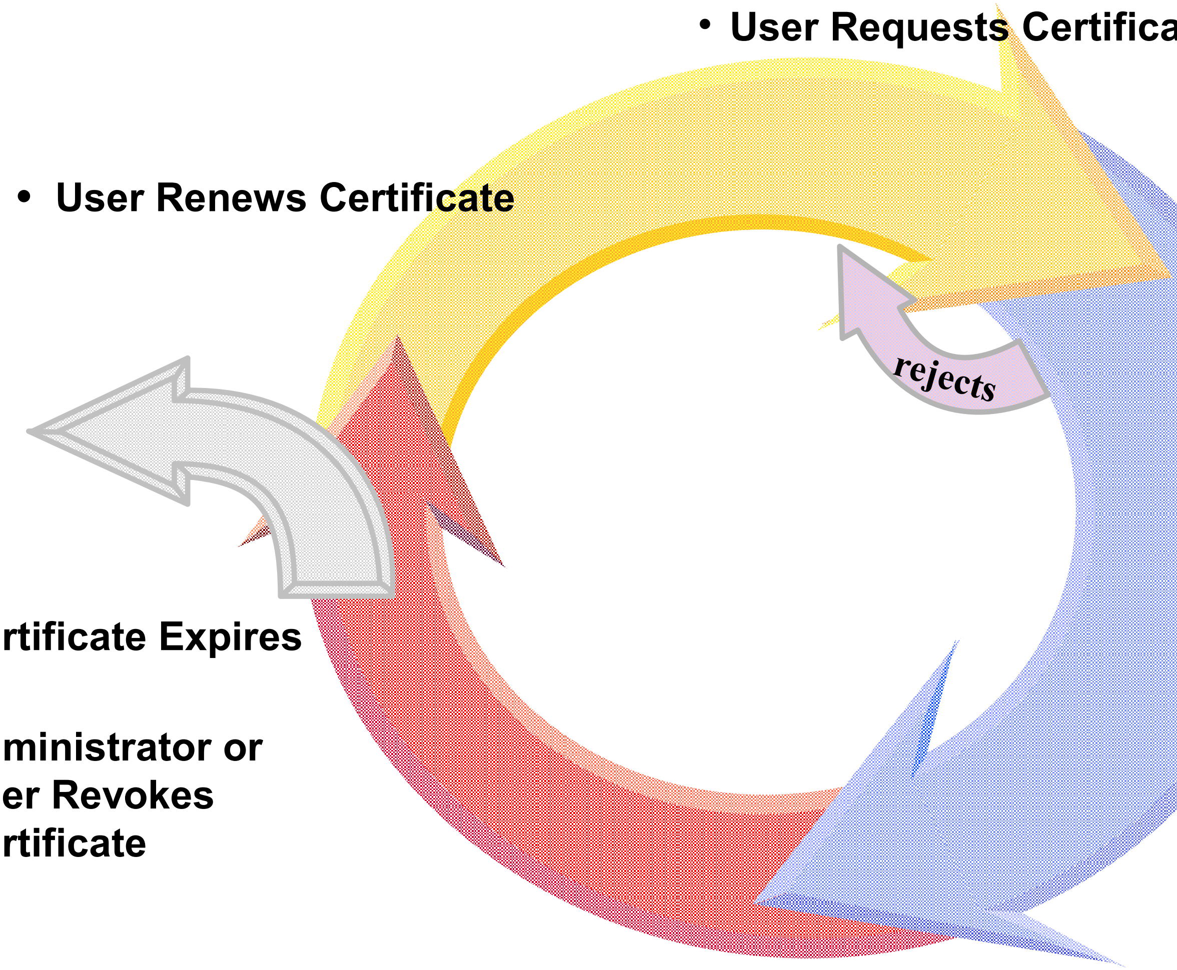
- Two main components delivering Digital Certificate support:
  - **RACF:**
    - **RACDCERT Commands** – Provides basic Digital Certificate generation and Key Ring management
    - **R_DataLib SAF Callable Service** – Provides API for accessing certificates in SAF Key rings
  - **z/OS PKI Services:**
    - Provides a fully functional Certificate Authority
    - Much more robust than a simple certificate utility like RACDCERT

PKI Services
Certificate Authority on z/OS

- PKI Services provides a full functioning **Certificate Authority**
  - Allows a organization to issue certificates signed by their own trusted CA certificate

- Provides for the full certificate life cycle:
  - End users can create a certificate **request**
  - PKI Administrators can **approve** / **modify** / **reject** requests
  - Certificates can be **revoked**
  - Certificates can be **renewed**

Certificate Life Cycle



- User Requests Certificate
- Administrator Approves the request
- CA Generates and distributes certificate
- Owner uses the certificate
- Certificate Expires

Or

- Administrator or User Revokes Certificate
- User Renews Certificate

PKI Services – Features

- Compared with RACDCERT, PKI Services can create certificates with many more fields in the Distinguished Names, and more extensions, including customizable ones
- Supports multiple certificate revocation mechanisms:
  - **Certificate Revocation Lists** (CRL) – List of certificates which can no longer be trusted
  - **Online Certificate Status Protocol** (OCSP) – dynamic checking on certificate status
- **SCEP Support:**
  - Simple Certificate Enrollment Protocol – automatic fulfillment on certificate request from network devices
- **CMP Support:**
  - Certificate Management Protocol – enable PKI functions through standard transport protocol

PKI Services – Features

- Certificates and CRLs can be posted to **LDAP** and/or stored in an HFS file for HTTP server

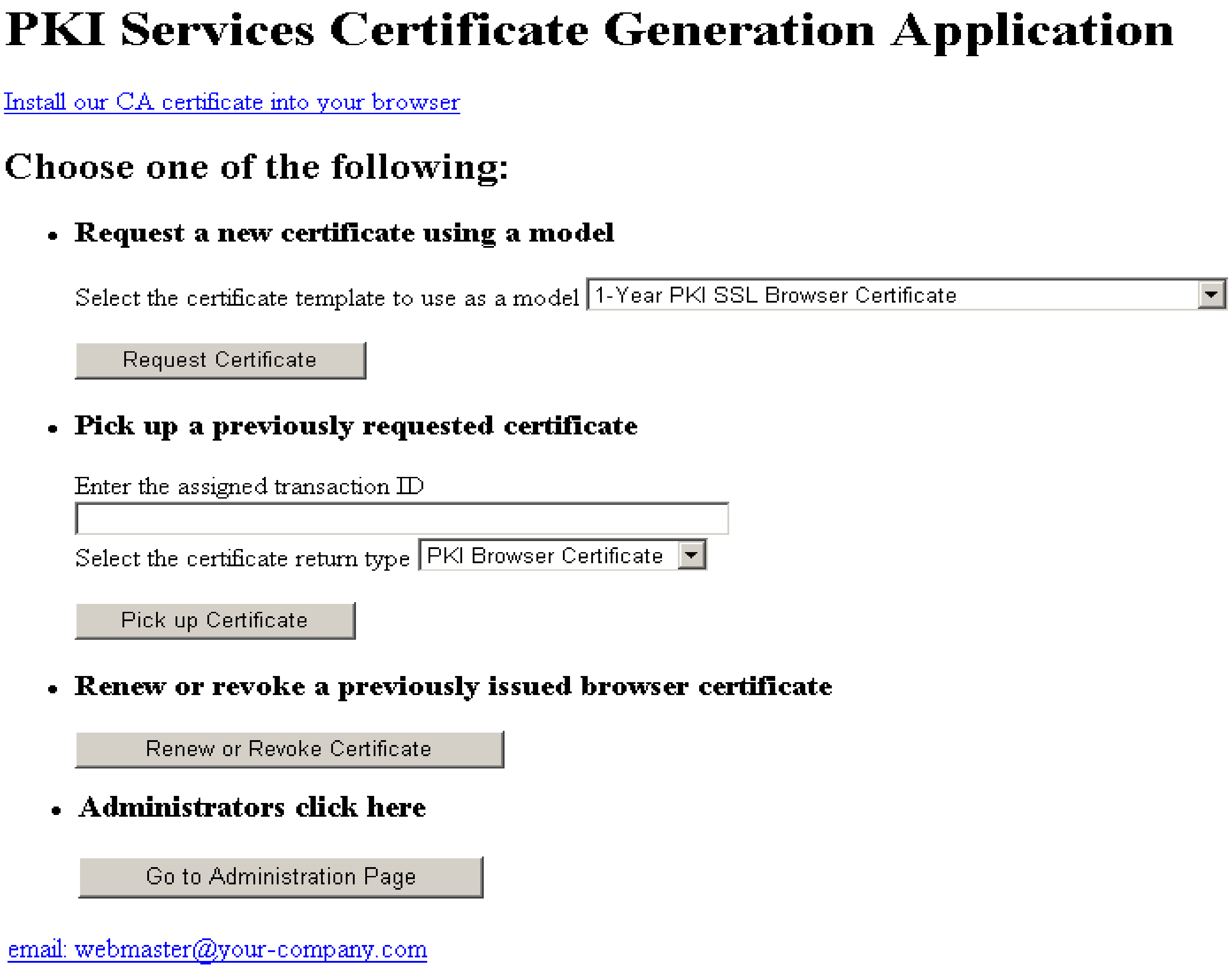
- Provide options for requestor to **generate his own key pair** or request the **PKI CA to generate it**

- Provides email notification:
  - Notify administrator for **pending requests**
  - Notify end user for **completed** certificate request and
  - Notify users for certificate **expiration** warnings
  - Send the **automatic renewed** certificate

PKI Services – Features

- Can issue many different types of certificates though customizable certificate templates
  - S/MIME, IPSEC, SSL, CA, Windows Logon
- Smart-card support
- Support **automatic** or **administrator approval** process
- Certificates can be picked up from the requestor’s machine
- Generation and administration of certificates via **customizable web pages**

PKI Services Webpages: Sample



PKI Services 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: 1-Year PKI SSL Browser Certificate

- **Pick up a previously requested certificate**

  Enter the assigned transaction ID

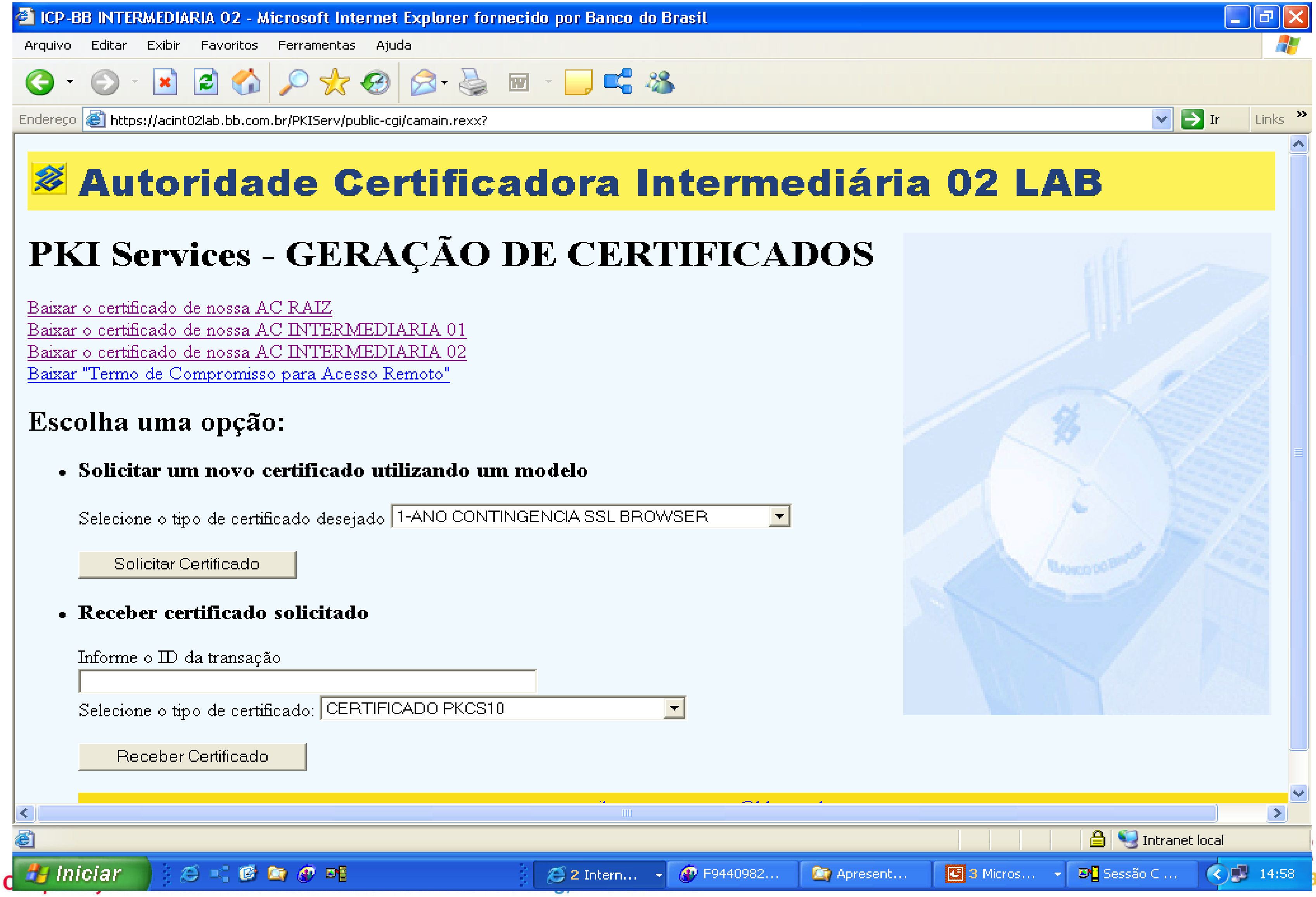
  Select the certificate return type: PKI Browser Certificate

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

- **Administrators click here**

email: webmaster@your-company.com

PKI Services Webpages: Customized



https://acint02lab.bb.com.br/PKIServ/public-cgi/camain.rexx?

Autoridade Certificadora Intermediária 02 LAB

PKI Services - GERAÇÃO DE CERTIFICADOS

Baixar o certificado de nossa AC RAIZ
Baixar o certificado de nossa AC INTERMEDIARIA 01
Baixar o certificado de nossa AC INTERMEDIARIA 02
Baixar "Termo de Compromisso para Acesso Remoto"

Escolha uma opção:

- **Solicitar um novo certificado utilizando um modelo**

  Selecione o tipo de certificado desejado: 1-ANO CONTINGENCIA SSL BROWSER

  Solicitar Certificado

- **Receber certificado solicitado**

  Informe o ID da transação

  Selecione o tipo de certificado: CERTIFICADO PKCS10

  Receber Certificado

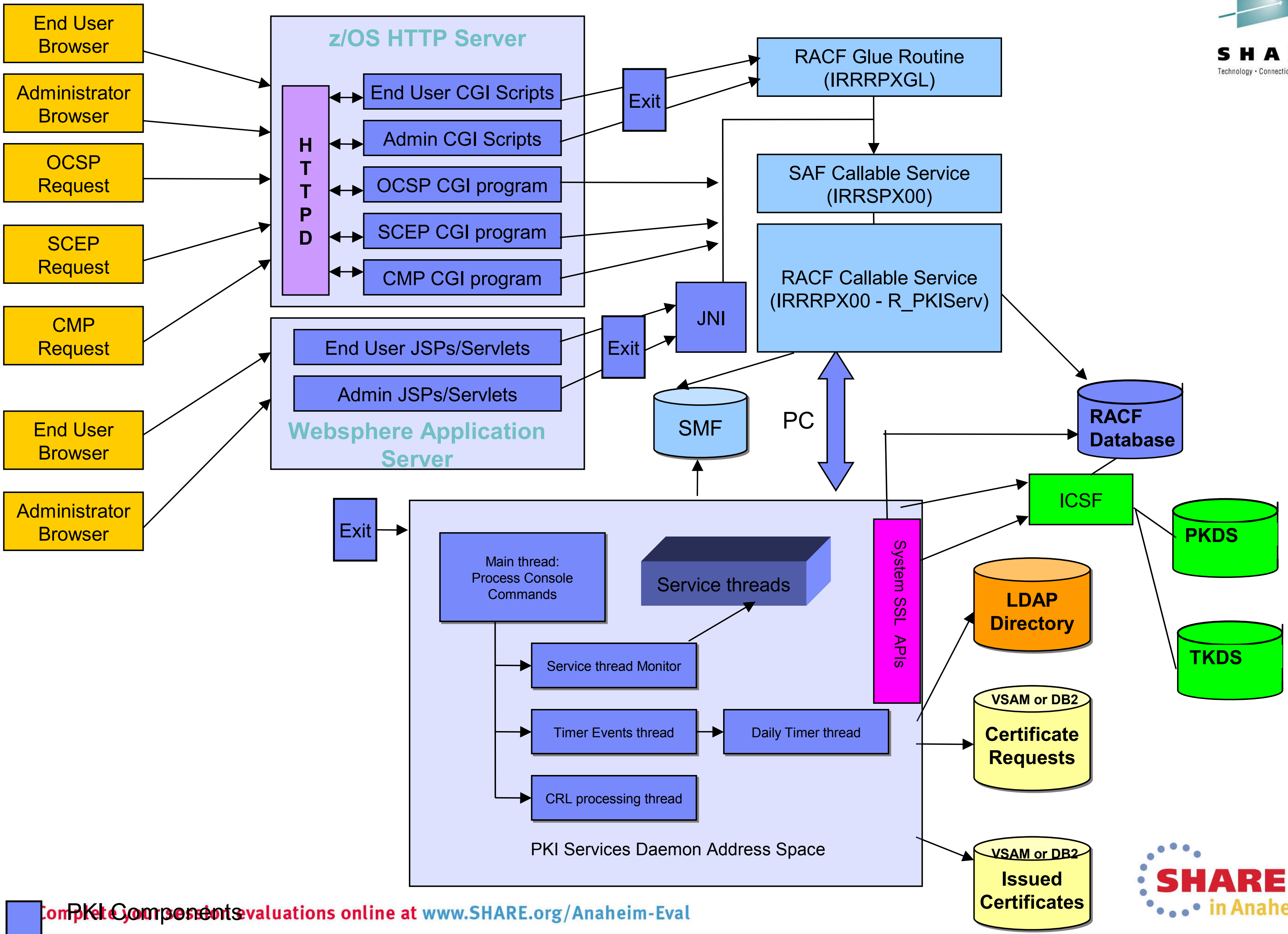
PKI Services Customization

- **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…

Why PKI Services on z/OS?

- Feature rich:
  - Responsive to customer requirements
- Cost effective:
  - Not a priced product - Licensed and *integrated* within z/OS
  - Alternative to purchasing third party certificates
- Scalable:
  - Scalable and available with z/OS Sysplex exploitation
  - Customers issue thousands and millions of certificates
- Secure:
  - CA's private key can be protected using System z Crypto hardware
  - Authority checking and Auditing though a SAF callable service - R_Pkiserv



End User Browser

Administrator Browser

OCSP Request

SCEP Request

CMP Request

End User Browser

Administrator Browser

z/OS HTTP Server

HTTPD

End User CGI Scripts

Admin CGI Scripts

OCSP CGI program

SCEP CGI program

CMP CGI program

End User JSPs/Servlets

Admin JSPs/Servlets

Websphere Application Server

Exit

Exit

JNI

RACF Glue Routine (IRRRPXGL)

SAF Callable Service (IRRSPX00)

RACF Callable Service (IRRRPX00 - R_PKIServ)

SMF

PC

RACF Database

ICSF

PKDS

TKDS

Exit

Main thread: Process Console Commands

Service threads

Service thread Monitor

Timer Events thread

Daily Timer thread

CRL processing thread

System SSL APIs

PKI Services Daemon Address Space

LDAP Directory

VSAM or DB2

Certificate Requests

VSAM or DB2

Issued Certificates

🟦 PKI Components

Major Prerequisite Products

- **RACF (or equivalent)**
  - For storing PKI CA certificate
  - For authorization
- **IBM z/OS HTTP Server / Websphere Application Server**
  - For web page interface
- **LDAP Directory (z/OS or other platforms)**
  - For publishing issued certificates and CRLs
  - For email notification
- **ICSF (optional)**
  - For more secure CA private key
  - For PKI CA to generate key pair
- **z/OS Communications Server (optional)**
  - For email notification
- **DB2 (optional)**
  - An alternative implementation for backend stores

z/OS PKI Services Hands-on Lab

Ross Cooper, CISSP®
IBM Corporation

March 13th, 2014
Session: 14964