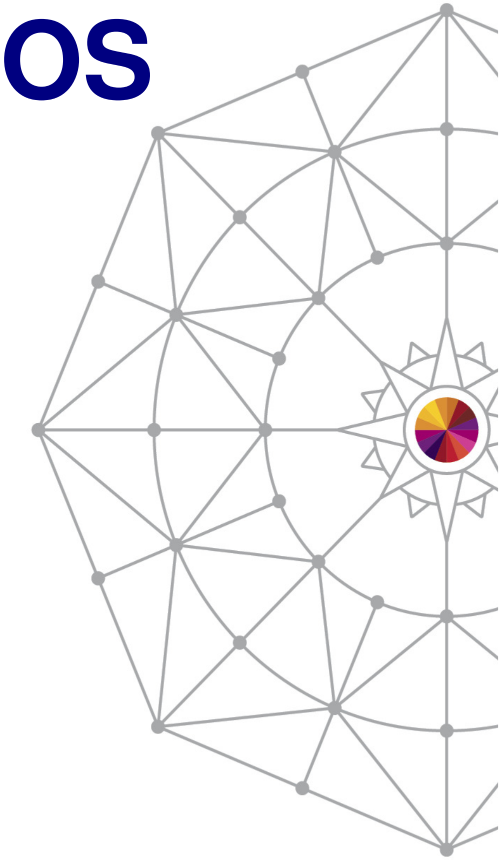
PKI Services: The Best Kept Secret in z/OS



Wai Choi, CISSP®
IBM Corporation

August 7th, 2014
Session: 15773

#SHAREorg

SHARE in Pittsburgh 2014

Trademarks

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.

Agenda

- Introduction to PKI Services
- Savings reported by a PKI Services customer – 66 millions

Introduction to PKI Services

What is a Digital Certificate?

A Digital Certificate is a digital document issued by a trusted third party which binds an end entity to a public key.

- **Digital document:**
  - Contents are organized according to ASN1 rules for X.509 certificates
  - Encoded in binary or base64 format
- **Trusted third party** aka **Certificate Authority** (CA):
  - The consumer of the digital certificate trusts that the CA has validated that the end entity is who they say they are before issuing and signing the certificate.
- **Binds the end entity to a public key:**
  - **End entity** - Any person or device that needs an electronic identity. Encoded in the certificate as the Subjects Distinguished Name (SDN). Can prove possession of the corresponding private key.
  - **Public key** - The shared half of the public / private key pair for asymmetric cryptography
  - **Digitally signed** by the CA

Do you need digital certificates?

- To secure your servers, routers
- To authenticate your business partners, customers, employees

Where/How do you get them?

- Buy them from a well-known Certificate Authority (CA) like VeriSign
- Generate them using program from Windows, free software like openssl
- Generate them using z/OS RACF's RACDCERT command

Have you heard of z/OS PKI Services?

- No
- Yes, but z/OS products are not cheap…
- Yes, but I am happy with what I use now…

Digital Certificate, PKI, z/OS PKI Services

- **Digital Certificate**
  - Provide identity to a person or a server
    - *Person - like an ID card*
    - *Server – like a business license*
  - To establish an identity to be used in secure electronic transactions
  - Issued by a trusted third party called Certificate Authority (CA) that vouches for certificate's identity
- **Public Key Infrastructure (PKI)**
  - System of CAs, software, hardware, policies… that regulate the issuance and validation of digital certificates involved in an electronic transaction
- **z/OS PKI Services**
  - Implementation of PKI on z/OS

z/OS PKI Services Overview

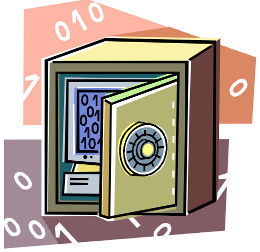
- Enable customers to run their own Certificate Authority to issue certificates for internal or external use
- A component on z/OS since V1R3, V2R1 was available last year
- Closely tied to RACF
  - The CA cert must be installed in RACF's key ring
  - Authority checking goes through RACF's callable service
- Provide more functions than RACDCERT as a Certificate Authority, eg.
  - email notification to notify
    - end user for completed certificate request and expiration warning or a renewed certificate
    - administrator for pending requests
- Generation and administration of certificates via customizable web pages

Benefits of using z/OS PKI Services (1 of 2)

- Supports popular protocols
  - ➢ Support Simple Certificate Enrollment Protocol (SCEP) for routers to request certificates automatically
  - ➢ Support Certificate Management Protocol (CMP) clients to communicate with PKI Services
  - ➢ Provide certificate status through Certificate Revocation List(CRL) and Online Certificate Status Protocol (OCSP)
- Provide customizable features that the other CAs may not have
  - ➢ Provide expiration notification and automatic renewal
  - ➢ Provide options for requestor to generate his own key pair or request the PKI CA to generate it
  - ➢ Support the creation of custom extensions

Benefits of using z/OS PKI Services (2 of 2)

- Not a priced product. Licensed with z/OS
  - A cost efficient alternative for government or companies purchasing certificates
- Leverage existing z/OS skills and resources
- Can run in separate z/OS partitions (integrity of zSeries® LPARs)
- Support multiple instances in one LPAR
- Scalable (Sysplex exploitation)
- The CA's private key can be protected under Crypto hardware



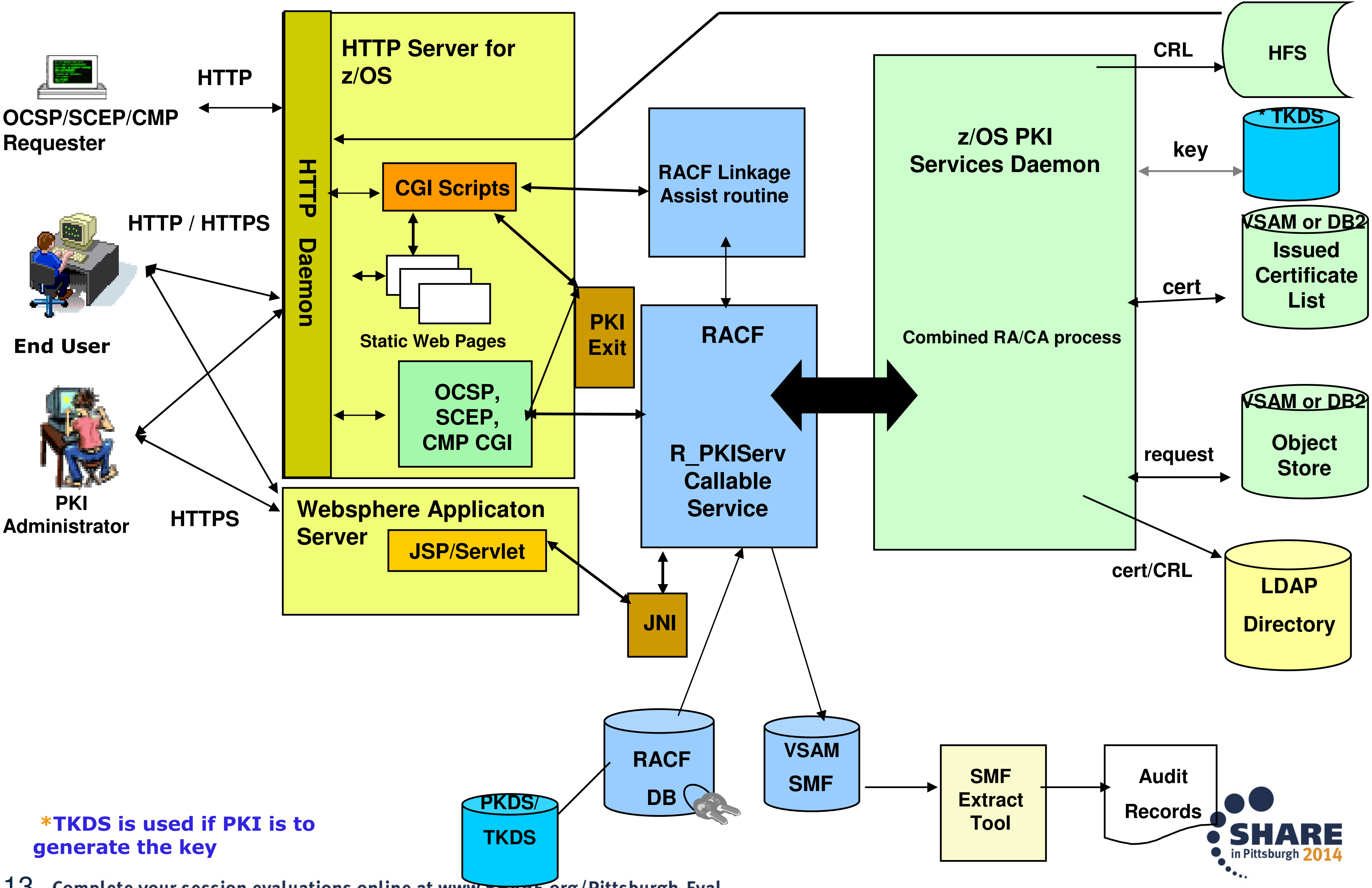
Some usages of certificates issued by z/OS PKI Services

- **For machines**
  - Web servers
  - Email servers
  - Business partners’ servers
  - Point of Sale (POS)
  - Routers
  - Remote desktop
  - Code signing
- **For people**
  - Smart card for employees to logon the system
  - Bank card for the customers

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 for PKI backend VSAM stores

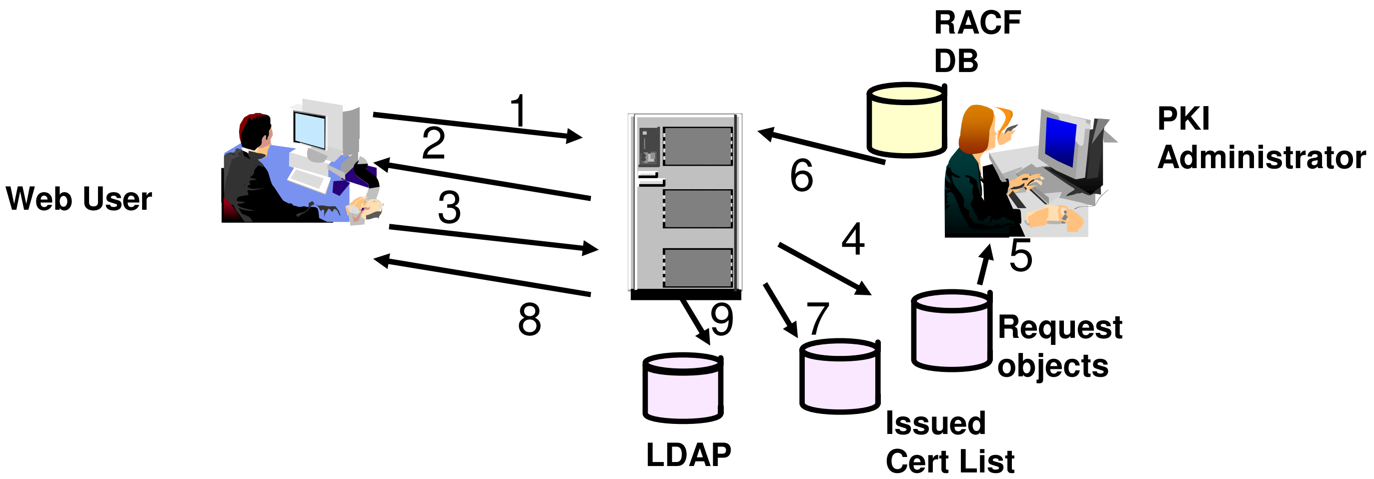
z/OS PKI Services structure



*TKDS is used if PKI is to generate the key

z/OS PKI Services Process Flow – a simplified sample view

1. User contacts PKI Services to request for certificate
2. CGI/JSP constructs a web page for user to input information
3. CGI/JSP packages all the info and send to the callable service
4. Callable service calls the daemon to generate the request object and put it in the Request objects DB
5. Administrator approves the request through the administrator web page
6. CGI/JSP calls callable service which in turn calls the daemon to create the certificate, sign with the CA key in the RACF DB
7. Certificate is placed in the Issued Cert List DB
8. Certificate is sent to the user
9. Certificate is posted to LDAP



Customization

- **Configuaration 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…

Samples shipped to get you started

/usr/lpp/pkiserv/samples

- pkiserv.conf
- pkiserv.tmpl
- pkitmpl.xml
- pkiserv.envars
- More…

SYS1.SAMPLIB

- IKYSETUP (REXX exec to set up RACF authorization profiles for PKI Services)

SYS1.PROCLIB

- PKISERVD (procedure to start PKI Services)

New enhancements

V2R1

- Create secure key in TKDS during certificate creation and return a PKCS#12 package containing the secure key to the requestor
- Create Extended Validation (EV) certificates which can raise the level of trustworthiness on a website since they were issued under stricter requirement
- Provide granular administration authorization control on requests and certificates based on the domain, action and the template. A switch is provided to turn on this granular check
- Allow the creation of certificate with the path length value in the Basic Constraints extension to restrict a subordinate CA from signing another subordinate CA
- Enable PKI Services to optionally issue console message when CRL processing ends, which can act as a trigger for some automation processing

Using RACF or PKI Services as a CA?

Use RACDCERT if	Use PKI Services if
Just need to generate a handful of certificates	Need to generate a large number of certificates
You can manually keep track of the expiration dates of the certs	You want to get notification on the expiration dates of the certs
You want to manually send the certs to the other parties	You want the other parties to retrieve the certs themselves
You don’t care if the certs are revoked	You want the certs to be checked for revocation status
You just need basic extensions in the certs	You want more supported extensions in the certs

Note: PKI Services does not have any function to manage the key ring. Ring management is provided by RACF.

An user experience - saves millions by using z/OS PKI Services

Data is provided by Vicente Ranieri Junior who works with Banco do Brasil in deploying PKI Services

Banco do Brasil

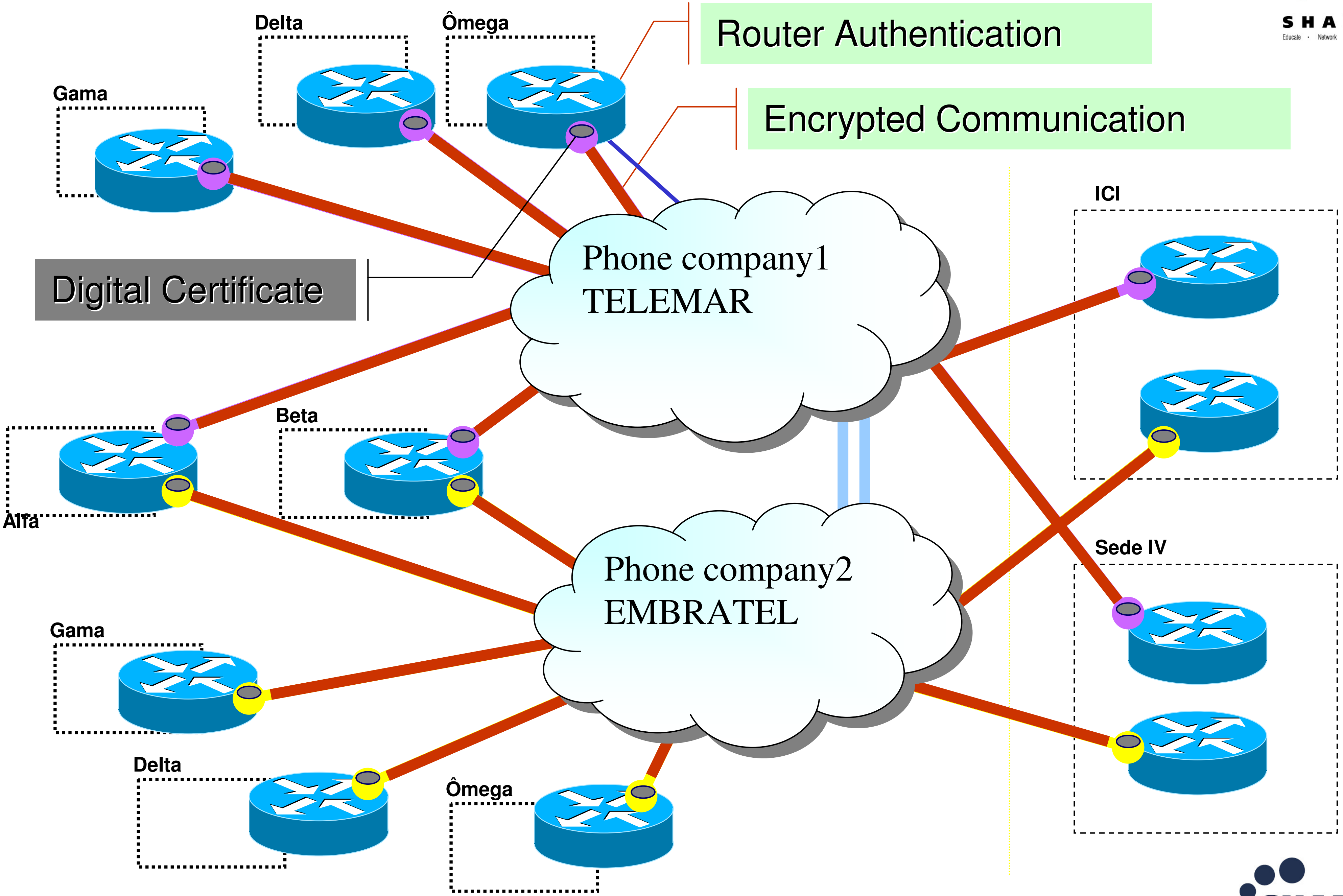
- Owned by the Brazilian government
- The largest bank in Brazil
- Over 200 years old
- It maintains 4,000 banking locations throughout the country and more than a hundred international branches in 23 countries
- It has more than 40,000 ATM machines - the largest number of ATM machines in the financial market
- 87,000 Employees
- More than 30,000,000 customers
- Currently, Banco do Brasil is among the 3 largest IBM zSeries customers worldwide

www.bb.com.br

Banco do Brasil Problem

- In 2003, following a market trend, Banco do Brasil outsourced its network to two telephone companies in Brazil
- Banco do Brasil lost the control over the path security where their critical data are flowing
- In order to enhance the network security, the telephone companies had to establish a VPN tunnel for each router pair in the network providing privacy and authentication

www.bb.com.br



Router Authentication

Encrypted Communication

Digital Certificate

Number of Certificates needed at Banco do Brasil

For Equipments and Applications – routers, internet banking

2007 :	14,000 digital certificates
Near Future:	66,000 digital certificates

For People – employees, bank lawyers

2007 :	2,000 digital certificates
Near Future:	80,000 digital certificates

The increase in projection number for certificates is due the 'extended services network' in which pharmacies, lottery booths need to be authenticated via certificates to perform small banking services.

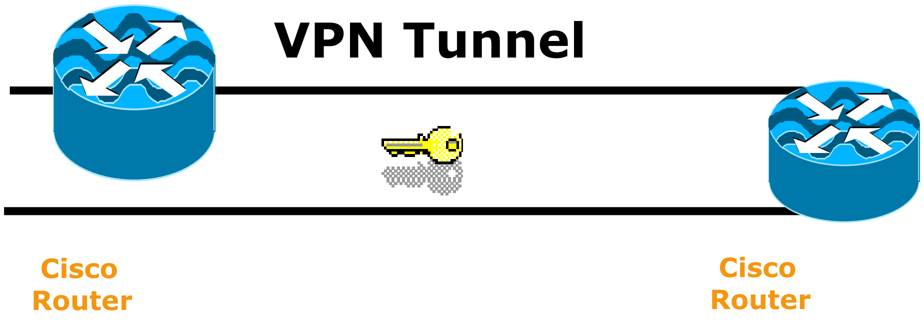
Let’s look at the YEARLY cost

Cost of certs for Equipment and Applications					
First Year			Projected		
Qty	Price per Cert	Total	Qty.	Price per Cert	Total
14,000	995.00	13,930,000.00	66,000	995.00	65,670,000.00

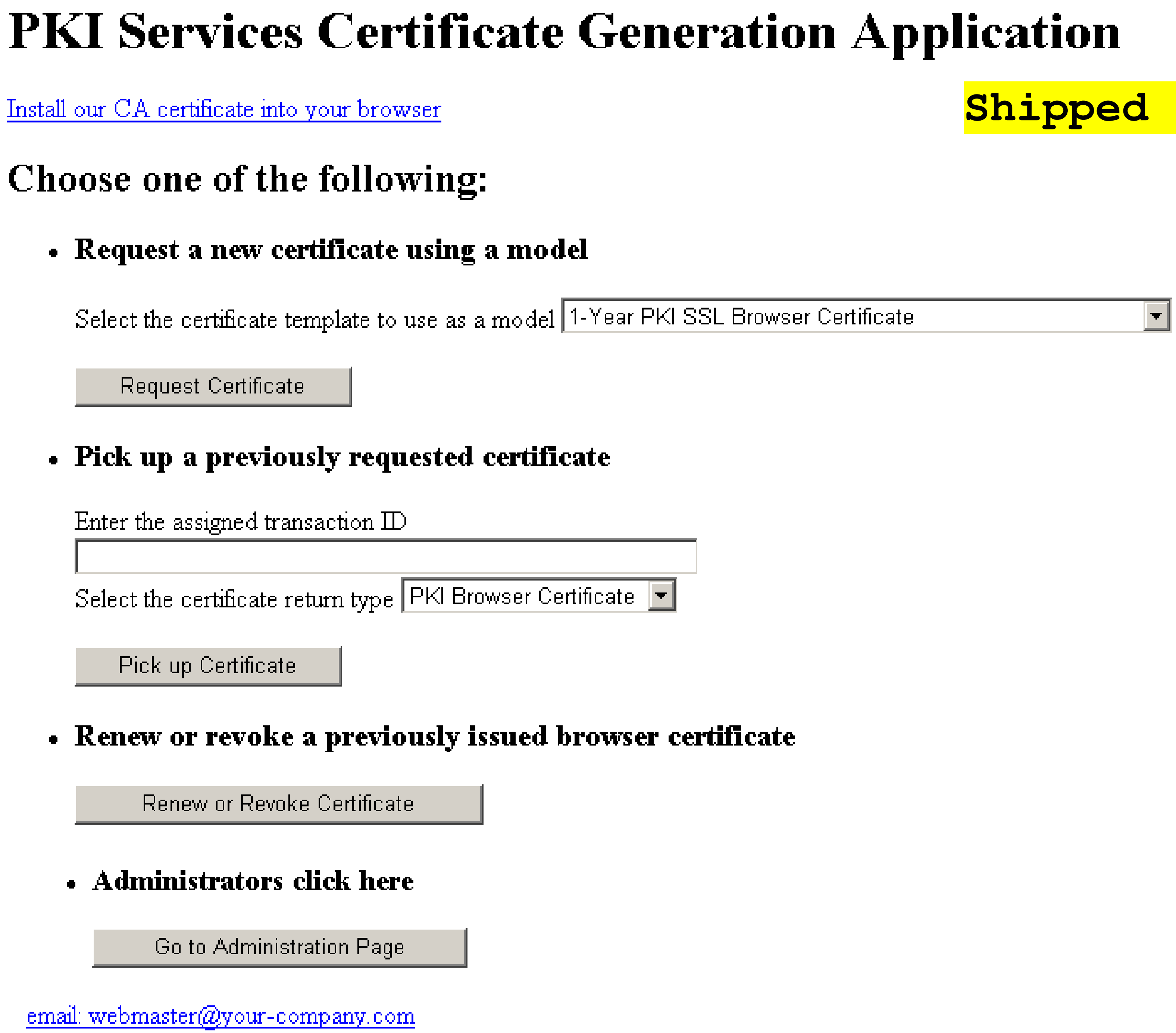
Cost of certs for People					
First Year			Projected		
Qty	Price per Cert	Total	Qty.	Price per Cert	Total
2,000	* 13.00	26,000.00	80,000	* 13.00	1,040,000.00

* Special Price from Brazilian Government Agency CA

Banco do Brasil Solution



- Banco do Brasil network had its security dramatically improved with almost no additional cost (z/OS is their prime operating system and RACF was already deployed)
- In a week’s time, PKI Services was set up and running in the test system
- Low consumption of MIPS to run PKI Services
- There are no extra head counts to run PKI Services
- The customer cost was only related to customize z/OS PKI Services pages to meet their requirements



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

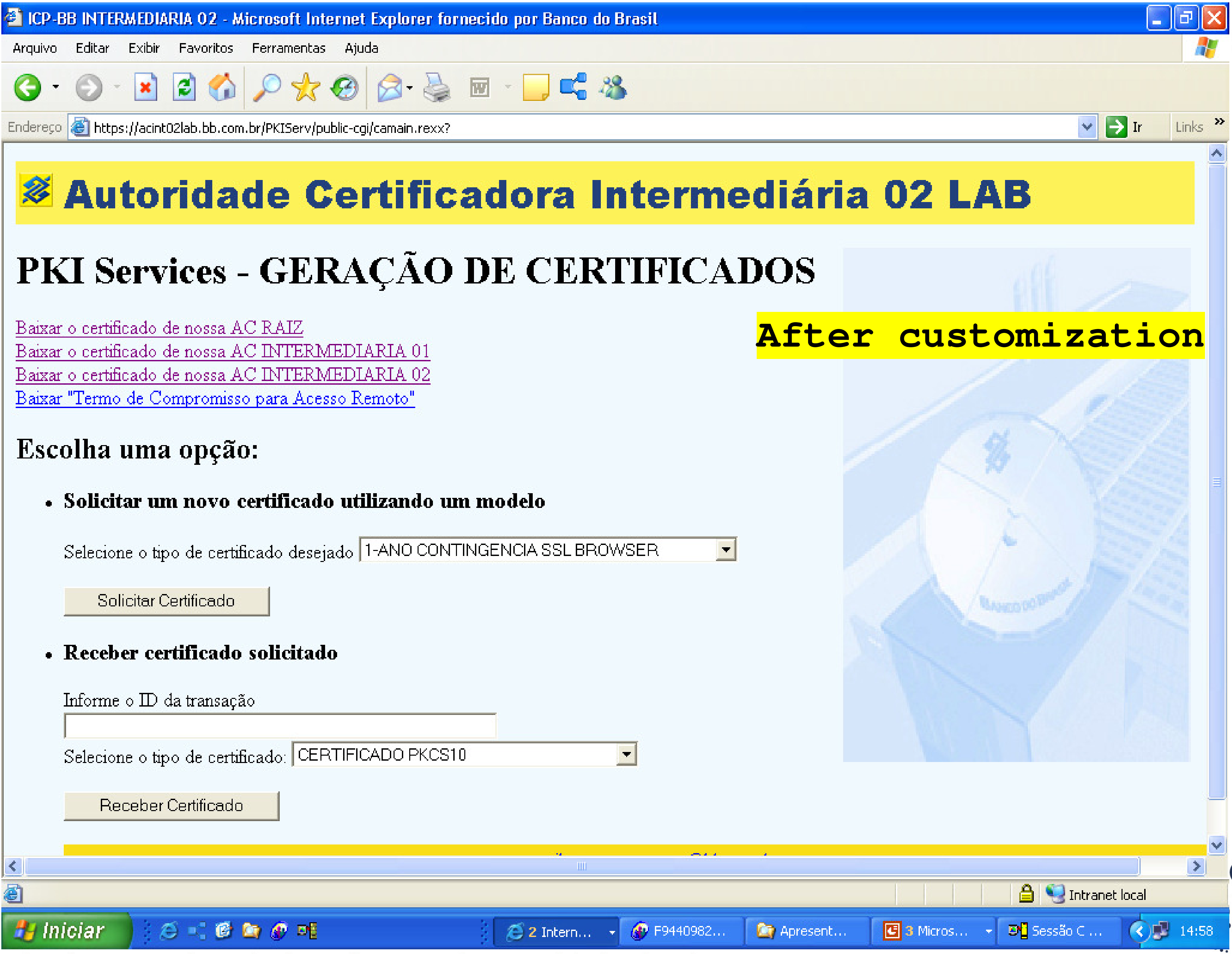
- **Renew or revoke a previously issued browser certificate**

  Renew or Revoke Certificate

- **Administrators click here**

  Go to Administration Page

email: webmaster@your-company.com



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

Autoridade Certificadora Intermediária 02 LAB

PKI Services - GERAÇÃO DE CERTIFICADOS

After customization

[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

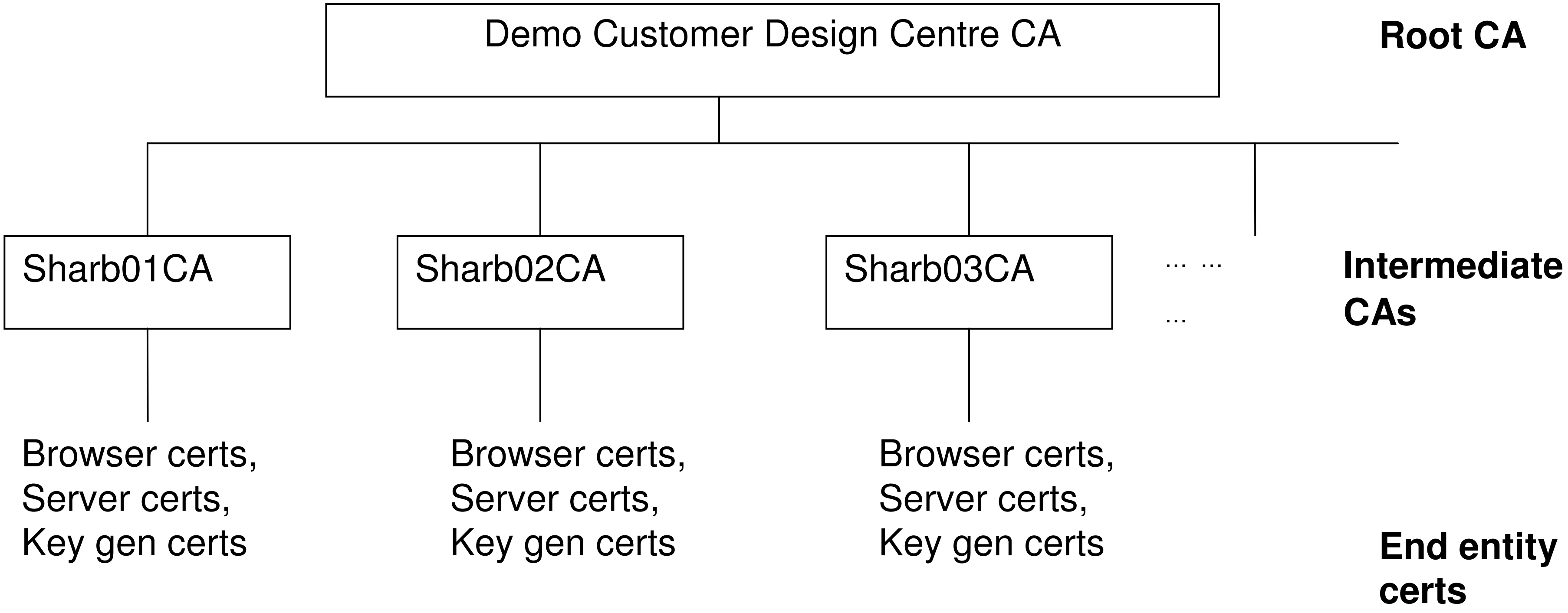
  Selecione o tipo de certificado: CERTIFICADO PKCS10

  Receber Certificado

Summary

- z/OS PKI Services is a complete Certification Authority package running under z/OS.
- It provides full certificate life cycle management
- No cost per issued digital certificate
- It is a very Secure, Scalable and Available PKI solution
- Banco do Brasil is an IBM customer reference

Multiple CAs in one LPAR



Demo Customer Design Centre CA

Root CA

Sharb01CA

Sharb02CA

Sharb03CA

… …

…

Intermediate CAs

Browser certs,
Server certs,
Key gen certs

Browser certs,
Server certs,
Key gen certs

Browser certs,
Server certs,
Key gen certs

End entity certs

What you can try in the PKI Lab

- Submit and approve a certificate request for
  - A certificate with key pair generated by the browser – EX 1
  - A certificate with key pair generated by PKI Services – EX 2
  - A certificate with key pair generated on a z/OS server – EX 3
- View the installed certificate from the broswer – EX 4
- Revoke/Suspend a certificate – EX 5
- Check the certificate status – EX 6
  - Certificate Revocation List (CRL)
  - Online Certificate Status Protocol (OCSP)
- Customize PKI Services – EX 7
  - Configuration file – pkiserv.conf
  - Template file – pkiserv.tmpl

References

- **PKI Services web site:**

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

- **IBM Redbooks**

  System z Cryptographic Services and z/OS PKI Services

  Implementing PKI Services on z/OS

- **Cryptographic Server Manual**

  Cryptographic Services PKI Services Guide and Reference

- **RFCs**

  RFC2459 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile

  RFC5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Questions ?

See you in the PKI Lab!

Session 15773