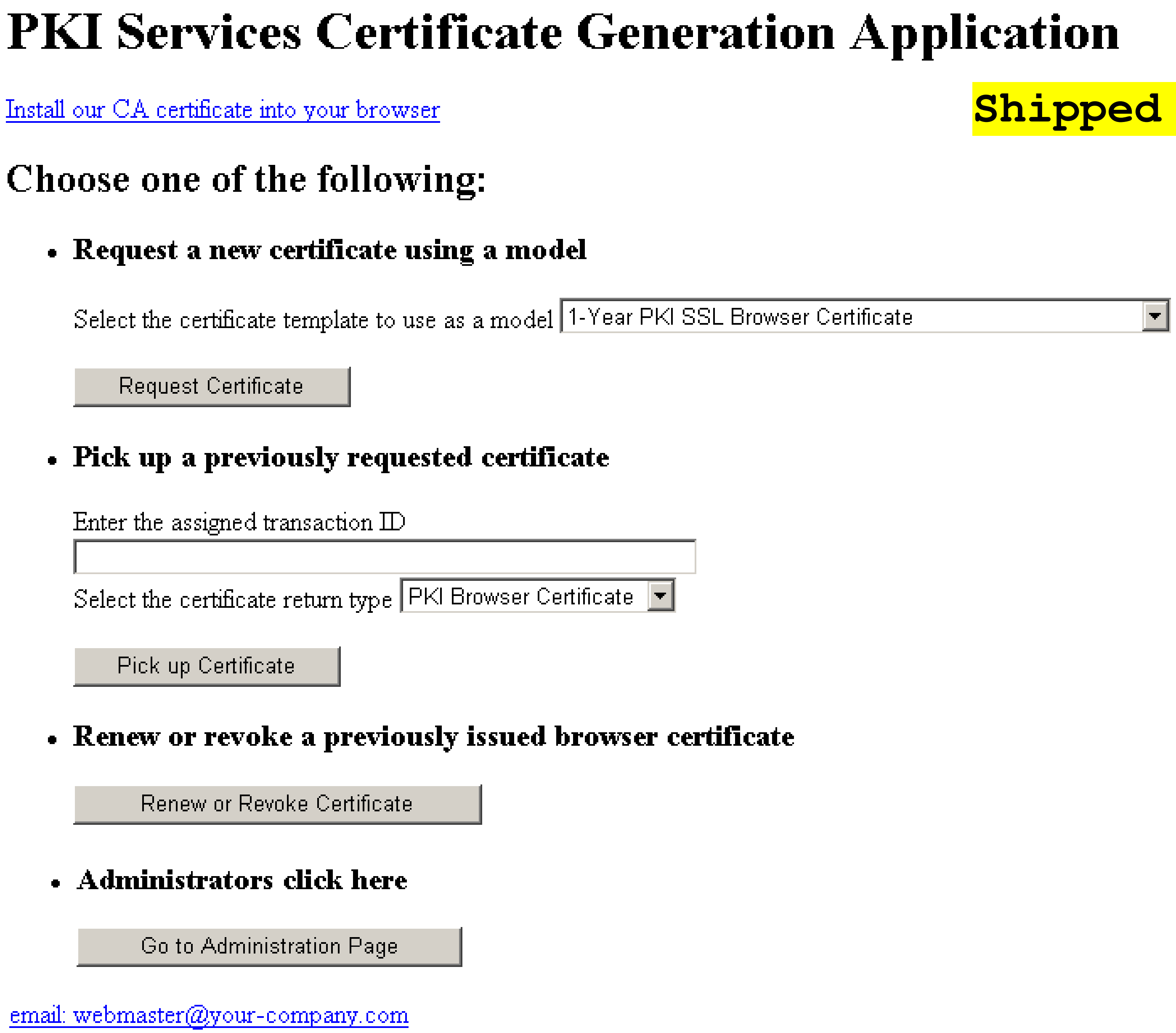
z/OS PKI Services Overview

December 2011

PKI Services - Certificate Authority on z/OS

- PKI Services provides a full functioning Certificate Authority
- Compare with RACDCERT, PKI Services can create certificates with much more fields in the Distinguished Names, and more extensions
- Provides full certificate life cycle management
  - Request, create, renew, revoke certificate
  - Generation and administration of certificates via customizable web pages



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

  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**

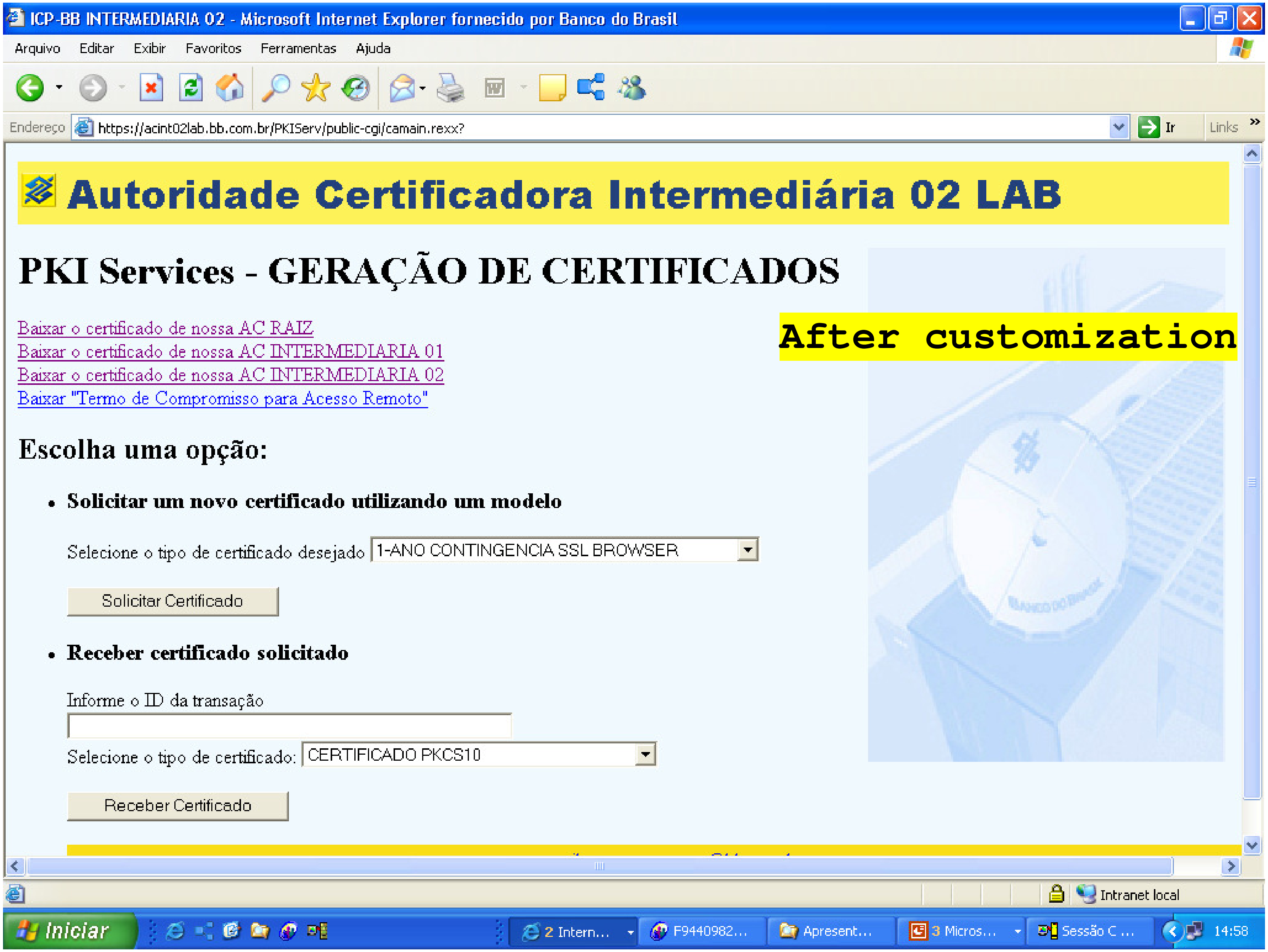
  Renew or Revoke Certificate

- **Administrators click here**

  Go to Administration Page

email: webmaster@your-company.com

Shipped sample


ICP-BB INTERMEDIARIA 02 - Microsoft Internet Explorer fornecido por Banco do Brasil
Arquivo Editar Exibir Favoritos Ferramentas Ajuda
Endereço
Ir
Links
Intranet local
Iniciar
2 Intern...
F9440982...
Apresent...
3 Micros...
Sessão C ...
14:58

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

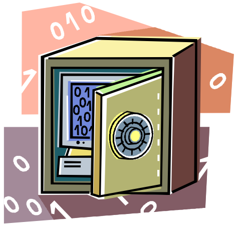
  Receber Certificado

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)

- Relatively low MIPS to drive thousands of certificates
- Leverage existing z/OS skills and resources
- Run in separate z/OS partitions (integrity of zSeries® LPARs)
- Scalable (Sysplex exploitation)
- The CA's private key can be protected under Crypto hardware
- Not a priced product. Licensed with z/OS



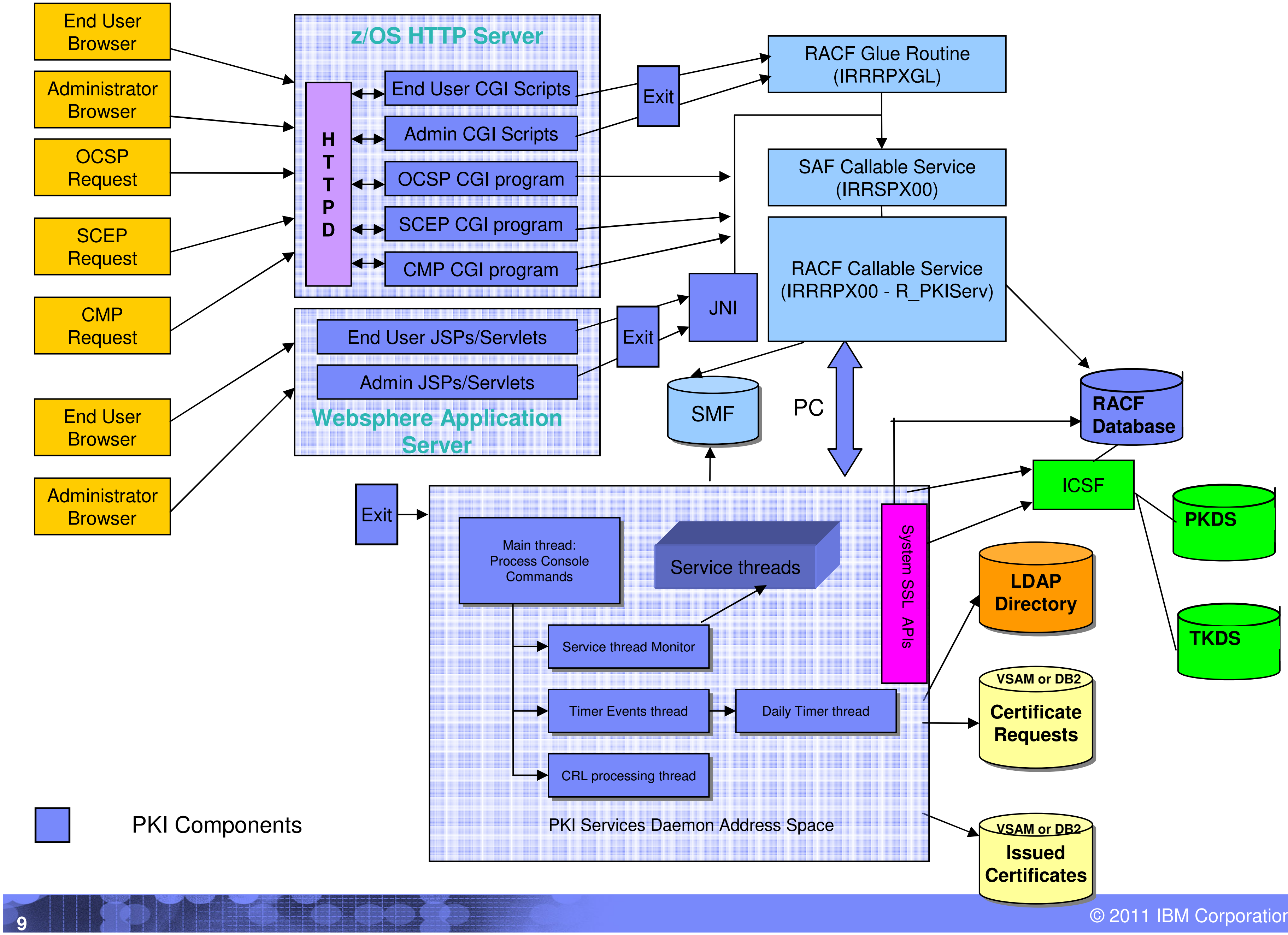
Major Prerequisite Products

- **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

Customization

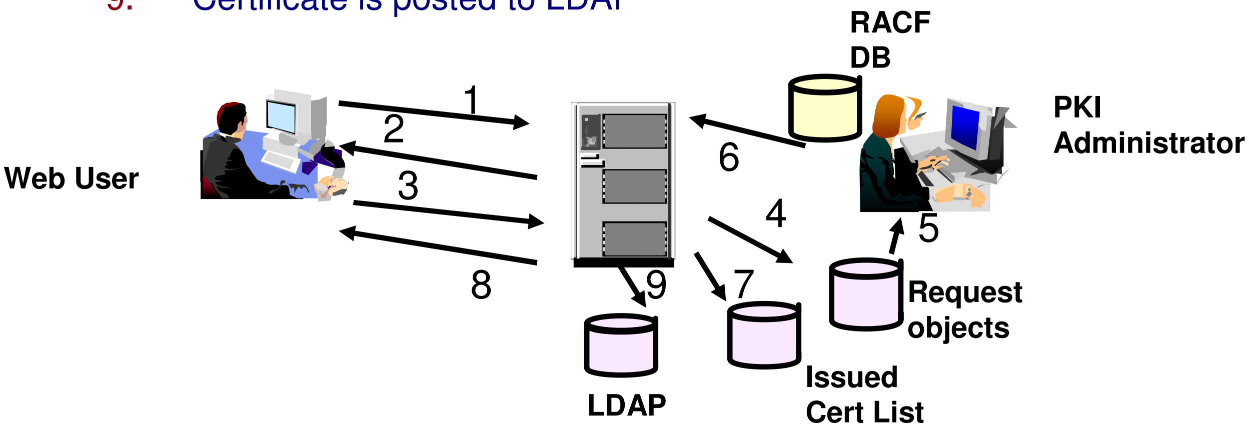
- **Configuaration file** - pkiserv.conf (used by the PKI Services daemon)
  - Contains mainly setup information for PKI Services
  - May contain certificate information applies to all types of certificates that PKI Services creates
- **Template file** - pkiserv.tmpl (used by the PKI Services CGIs)

  - 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…


End User Browser
Administrator Browser
OCSP Request
SCEP Request
CMP Request
End User Browser
Administrator Browser
z/OS HTTP Server
H T T P D
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
Exit
JNI
RACF Glue Routine (IRRRPXGL)
SAF Callable Service (IRRSPX00)
RACF Callable Service (IRRRPX00 - R_PKIServ)
SMF
PC
RACF Database
ICSF
PKDS
TKDS
LDAP Directory
VSAM or DB2
Certificate Requests
VSAM or DB2
Issued Certificates
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
PKI Components

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



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

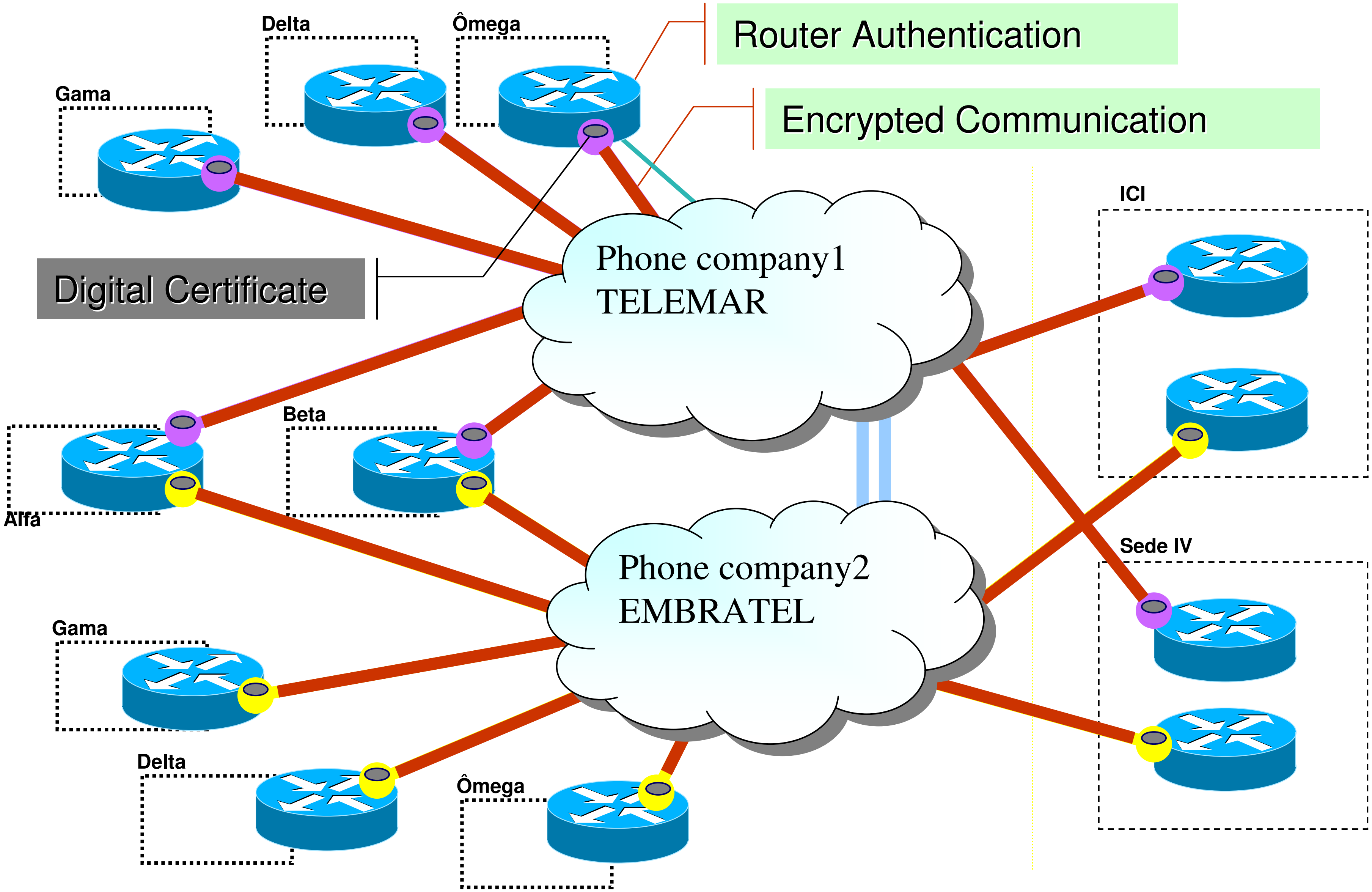
- Owned by the Brazilian government
- The largest bank in Brazil
- Over 200 years old
- It maintains 4,000 banking locations throughout the country and more than a hundred international branches in 23 countries
- It has more than 40,000 ATM machines - the largest number of ATM machines in the financial 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

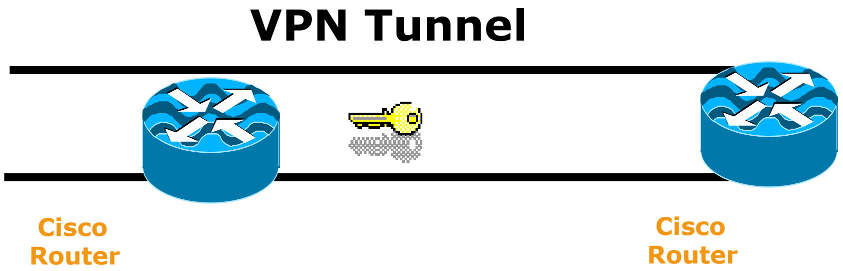
Solutions considered

- **OpenCA**
  - Pros : Free
  - Cons: No support
- **Windows Server Certificate Services**
  - Pros : Support available
  - Cons: Scalabity issue
- **z/OS PKI Services**
  - Pros : Free, scalable, support available
  - Cons: Some required certificate fields and protocol not supported yet

Banco do Brasil Solution

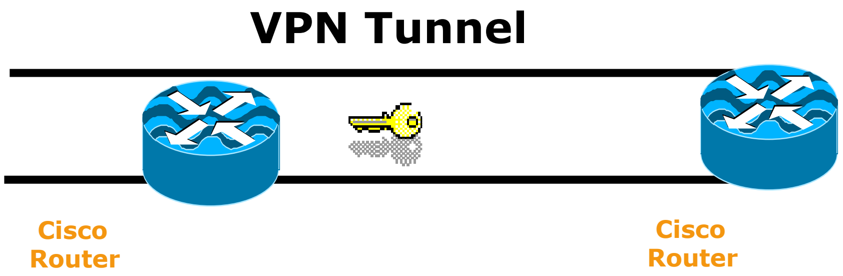
- Banco do Brasil submitted requirements to IBM to enhance PKI Services
- After knowing that the requirements were in plan, Banco do Brasil decided to start exploiting z/OS PKI Services to issue its VPN digital certificates

Banco do Brasil Solution



- In Brazil, there are 2 ways to be a certified CA
  - get a certification from the PKI Brazil government department which requires the PKI application runs alone on a separate machine (the bank is working on getting the acceptance that LPAR isolation is as good as a stand alone machine)
  - the issuer and the requester sign an agreement
- Banco do Brasil signed an agreement with the telephone companies

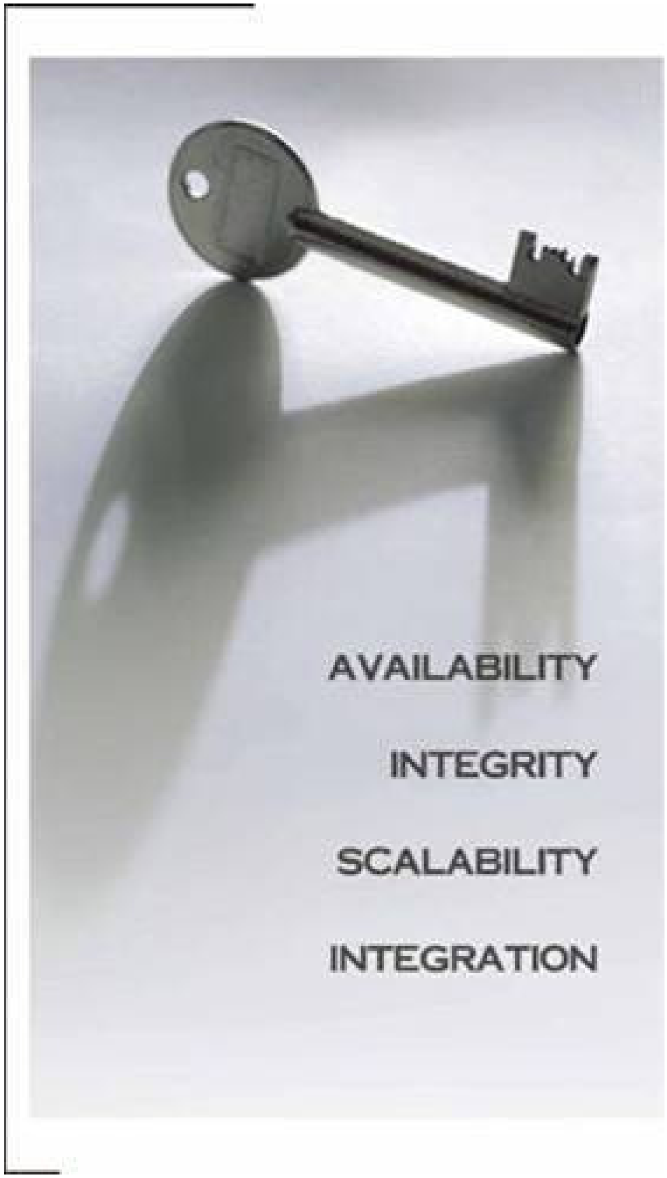
Banco do Brasil Solution



- 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

Banco do Brasil Solution

- Both telephone companies that outsourced Banco do Brasil network request and receive the VPN digital certificates through PKI Services web interface
- The phone companies send the serial numbers of the routers that need certificates to a manager
- They then use the RACF IDs in the Bank's system to request certificates for the routers
- The administrator checks if there's an email from the manager on the routers before the requests are approved
- The certificates are issued with 1 to 2 years' validity period



Performance

- Measured in a z900 model 2064-104 with hardware encryption and VSAM buffering
- 19.2 certificates created per second
- 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 an average 3 minutes.

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

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