z/OS PKI Services
A User Experience

SHARE Baltimore, MD
Session 1736
August 17th 2006

Wai Choi
IBM Corporation
Poughkeepsie, NY

Phone: (845) 435-7623
e-mail: wchoi@us.ibm.com

Acknowledgement

- This presentation is based on the one that my colleague Vicente Ranieri Junior made in another conference
- Vicente is the IT specialist who works with Banco do Brasil in deploying PKI Services

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*
- zSeries*

* 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

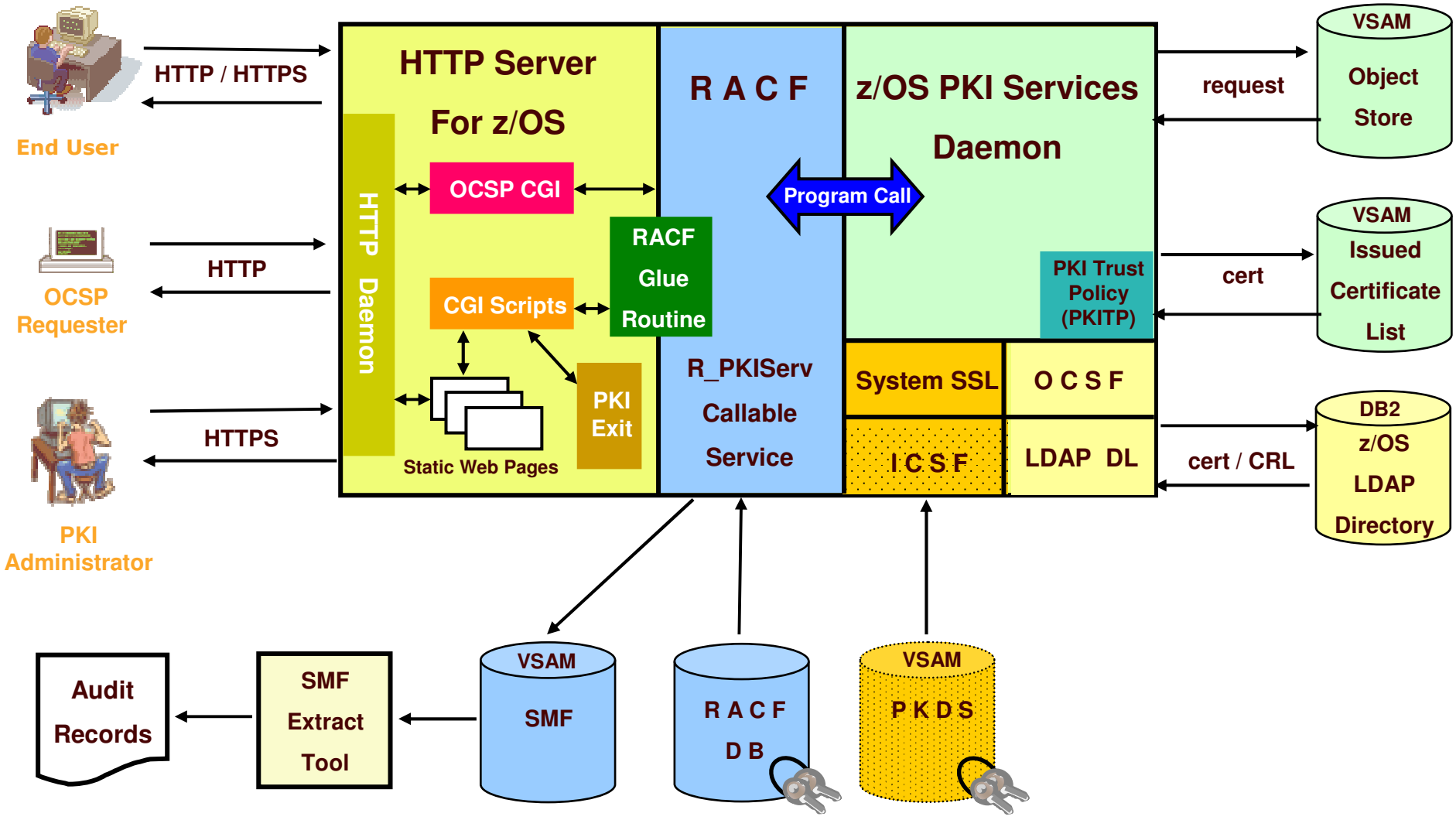
- Overview on z/OS PKI Services
- z/OS PKI Services at Banco do Brasil
- Enhancements on PKI Services that Banco do Brasil can take advantage of
- Session Summary

Overview on z/OS PKI Services

Introduction to PKI Services

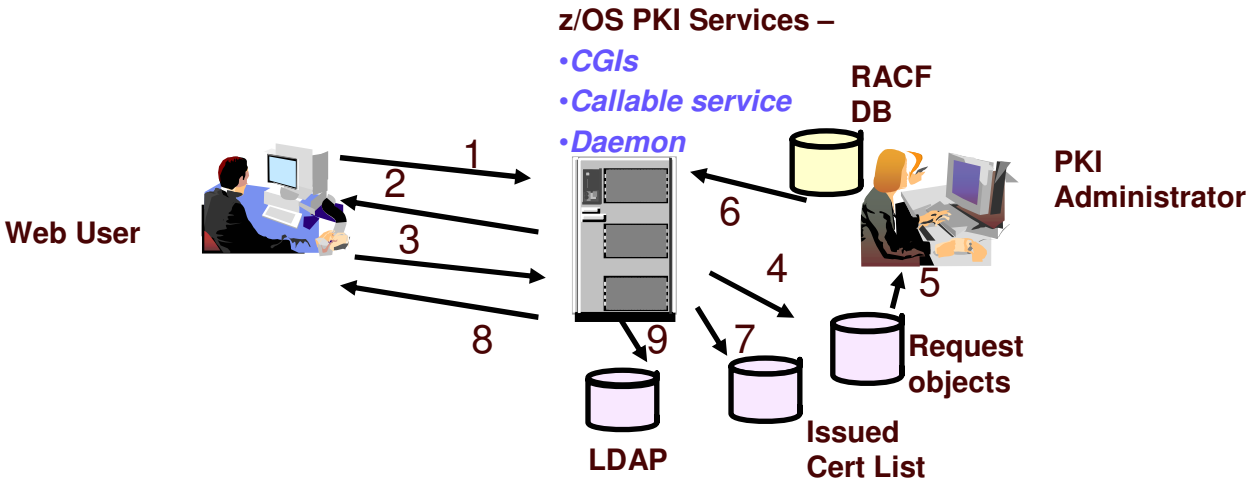
- A component on z/OS since V1R3
- Closely tied to RACF
  - The CA cert must be installed in RACF's key ring
  - Authority checking goes through RACF's callable service
- Supports more functions than RACDCERT
  - Full certificate life cycle management: request, create, renew, revoke
  - Generation and administration of certificates via customizable web pages
  - Support automatic or administrator approval process
  - Support multiple revocation checking mechanisms
  - Certificates and Certificate Revocation Lists (CRLs) can be posted to LDAP
  - Provides email notification for completed certificate request and expiration warnings

z/OS PKI Services Structure



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

1. User contacts PKI Services to request for certificate
2. CGI constructs a web page for user to input information
3. CGI 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 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. User retrieves the certificate
9. Certificate is posted to LDAP



z/OS PKI Services at Banco do Brasil

Banco do Brasil

- Owned by the Brazilian government
- The largest bank in Brazil
- 197 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 – 120,000 MIPs

www.bb.com.br

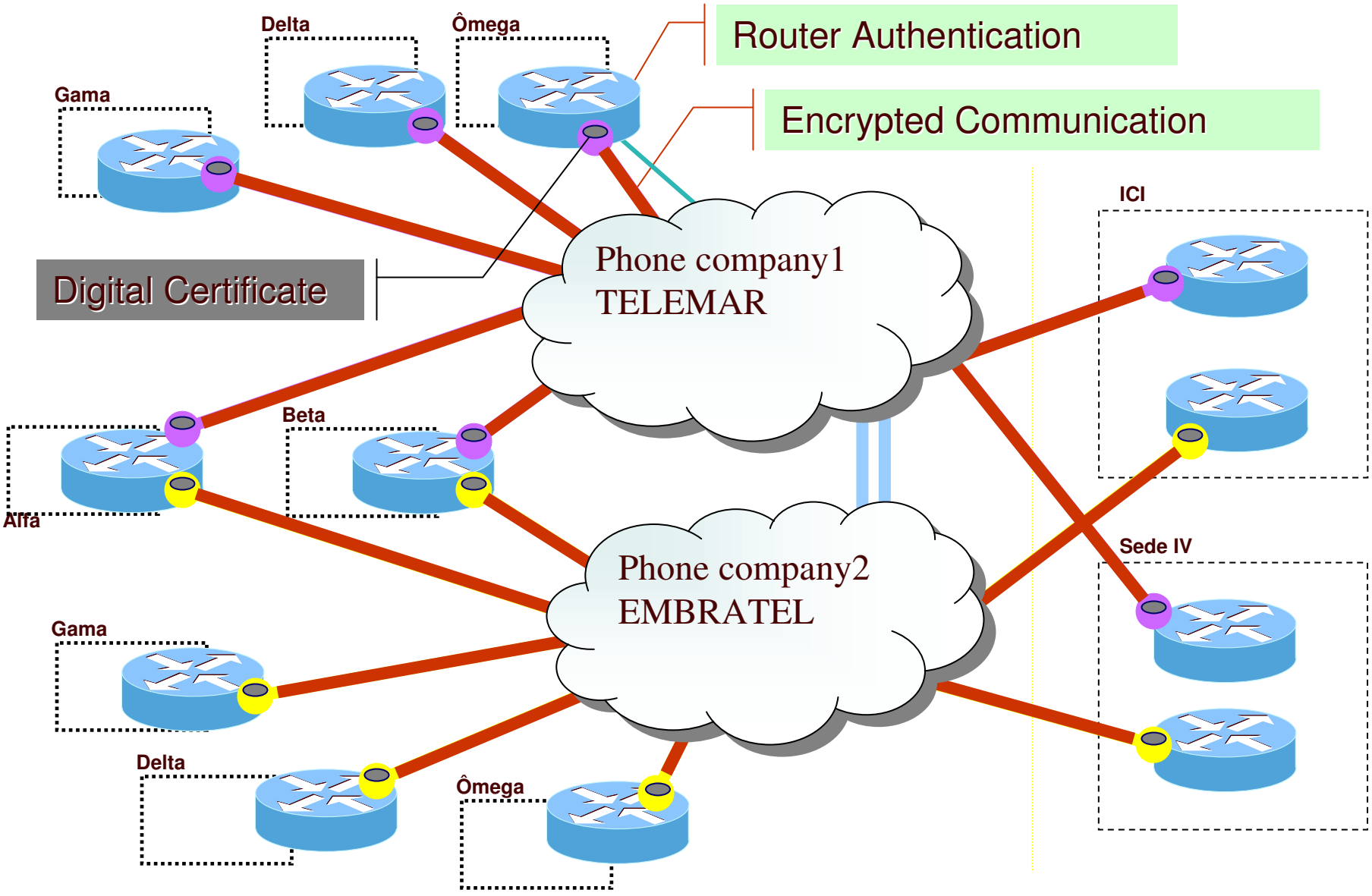
Banco do Brasil IT Evolution

	1995	2006
Online Branches	83%	100%
Online Transactions	93.6 millions	620 millions
Availability	75%	99.80%
Self Service Rooms	2	3,700
Self Service Terminals	11,600	40,000

Banco do Brasil Problem

- About 3 years ago, 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



Number of Certificates needed at Banco do Brasil

- **For Equipments and Applications – routers, internet banking**
  - Today : 7,500 digital certificates
  - Near Future: 13,000 digital certificates
- **For People – employees, bank lawyers**
  - Today : 1,300 digital certificates
  - Near Future: 80,000 digital certificates

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
7,500	995.00	7,462,500.00	13,000	995.00	12,935,000.00

Cost of certs for People					
First Year			Projected		
Qty	Price per Cert	Total	Qty.	Price per Cert	Total
1,300	* 13.00	16,900.00	80,000	* 13.00	1,040,000.00

* Special Price from Brazilian Government Agency CA

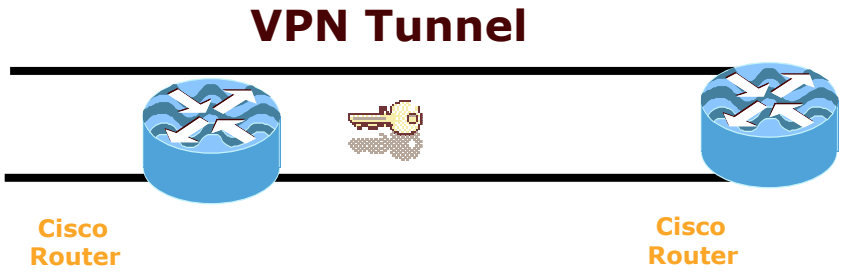
Solutions considered

- **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

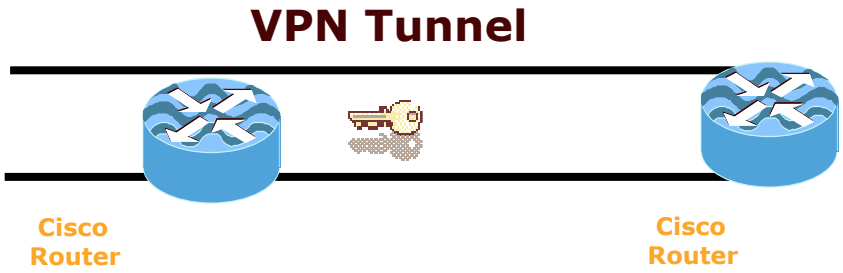
- **Banco do Brasil submitted requirements to IBM to enhance PKI Services**
- **After knowing that the requirements were in plan, Banco do Brasil decided to start exploiting z/OS PKI Services to issue its VPN digital certificates**

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

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

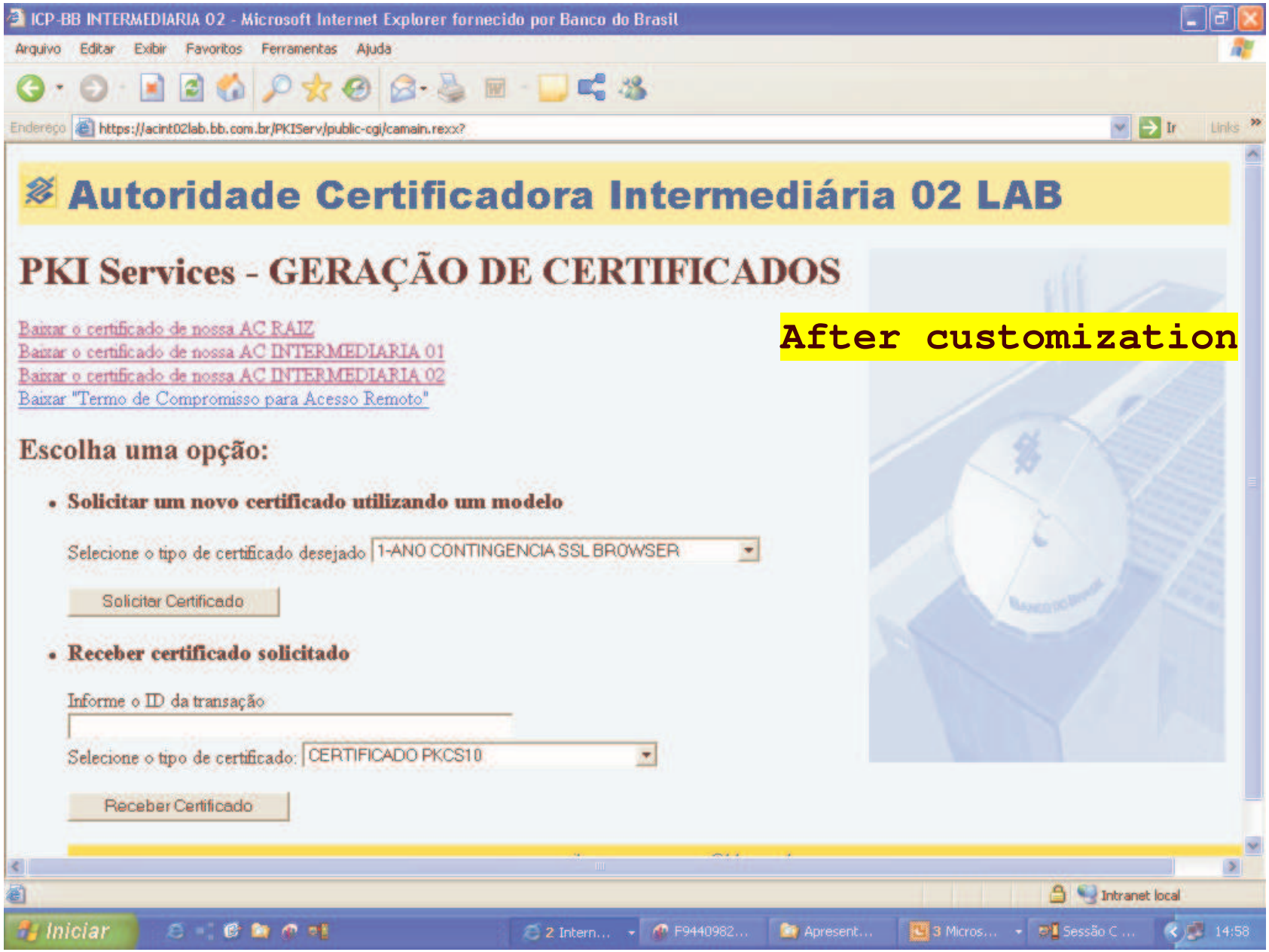
- **Renew or revoke a previously issued browser certificate**

  Renew or Revoke Certificate

- **Administrators click here**

  Go to Administration Page

email: webmaster@your-company.com



Shipped sample

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

1jTQjs0h/cpk2SHV++++++++

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:

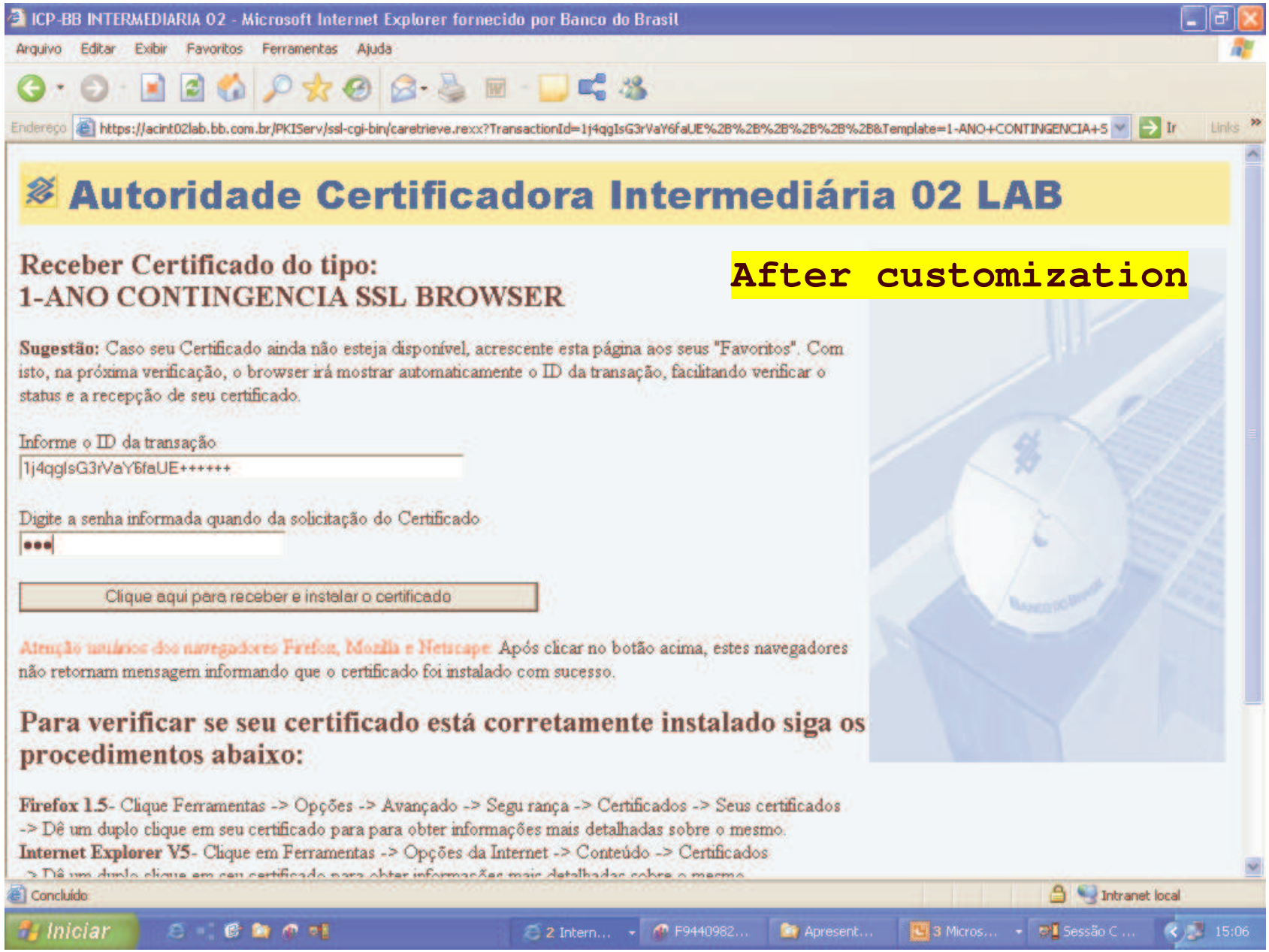
Netscape V6 - Click Edit->Preferences, then Privacy and Security-> Certificates. Click the Manage Certificates button to start the Certificate Manager. Your new certificate should appear in the Your Certificates list. Select it then click View to see more information.

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

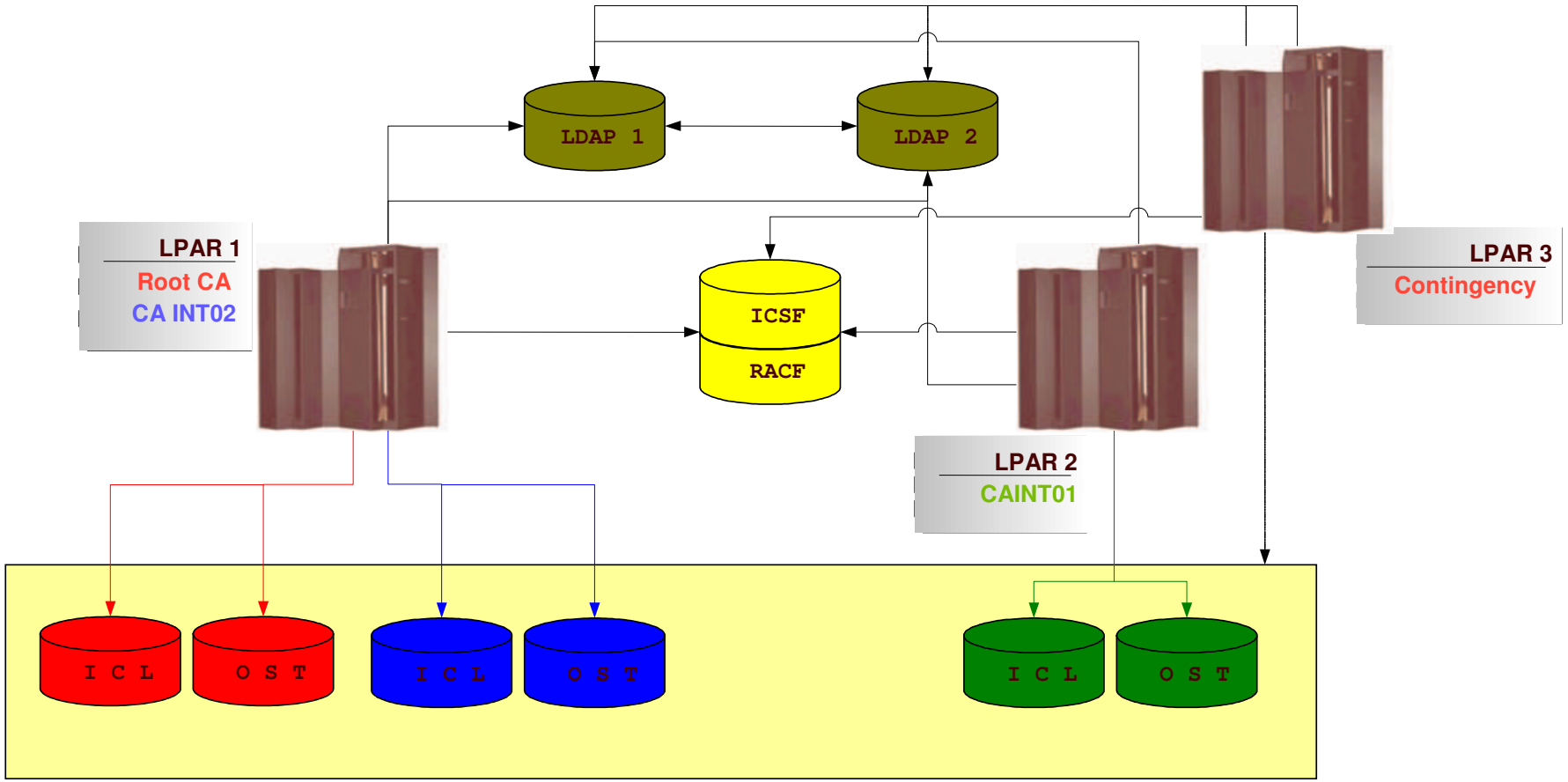
Internet Explorer V5 - Click Tools->Internet Options, then Content, Certificates. Your certificate should appear in the Personal list. Click Advanced to see additional information.

Home page

email: webmaster@your-company.com



PKI Implementation at Banco do Brasil



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

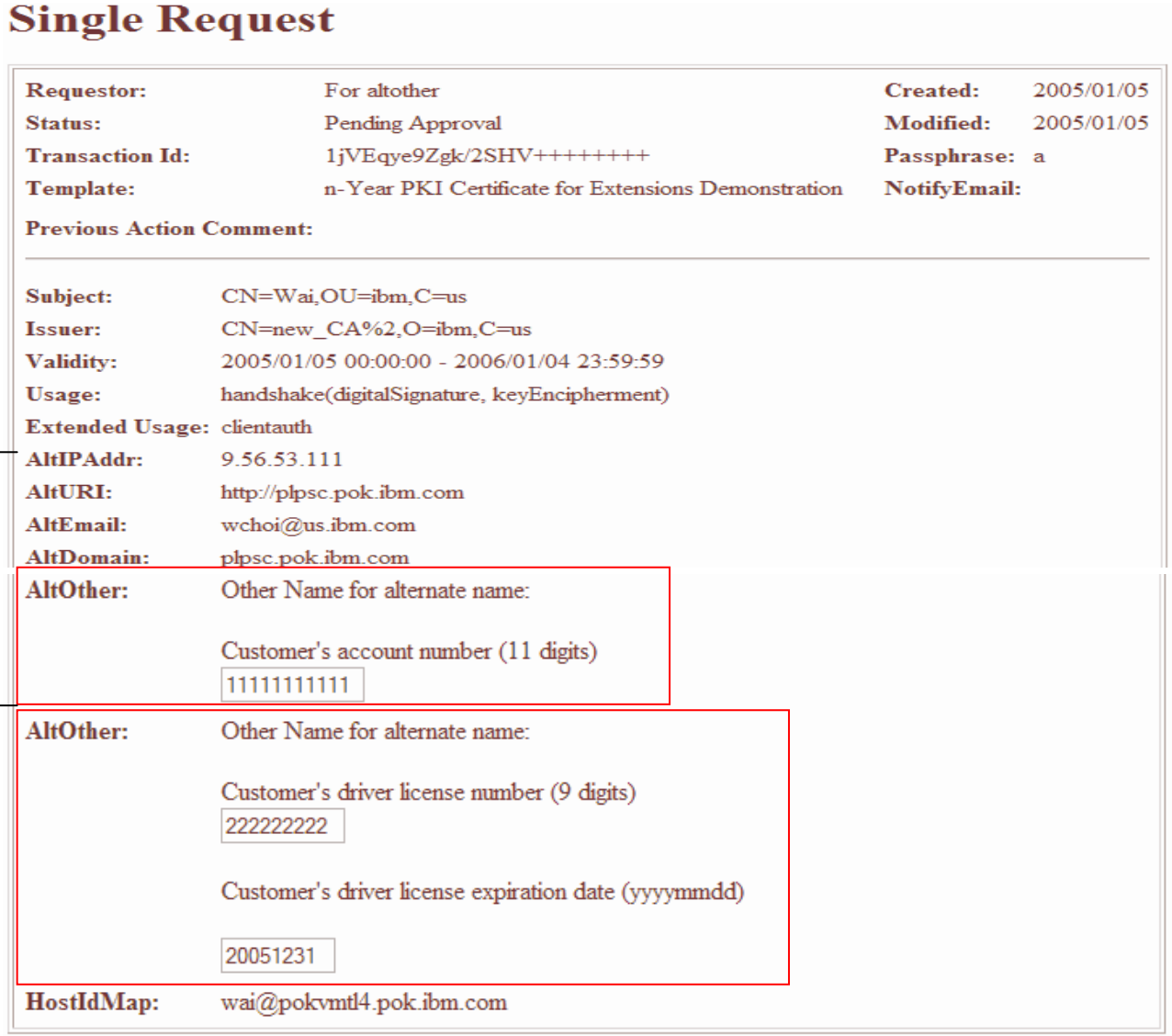
Enhancements on PKI Services that Banco do Brasil can take the advantage of

Enhancements on z/OS V1R7

- **Creation of Authority Revocation List (ARL)**
- **The PKI-Brazil CA certificate was added to the list of default CERTAUTH certificates in RACF**
- **Creation of the otherName format in Subject Alternate Name Extension**
  - This allows any kinds of information about the subject, eg. Birth date, social security number, driver's license number, voting ID, voting zone, user principal name (for Windows logon application)...

Digital Certificate Enhanced Extension

All these are different forms in the Subject Alternate Name extension



Single Request

Requestor:	For altother	**Created:**	2005/01/05
Status:	Pending Approval	**Modified:**	2005/01/05
Transaction Id:	1jVEqye9Zgk/2SHV++++++++	**Passphrase:**	a
Template:	n-Year PKI Certificate for Extensions Demonstration	**NotifyEmail:**	
Previous Action Comment:			

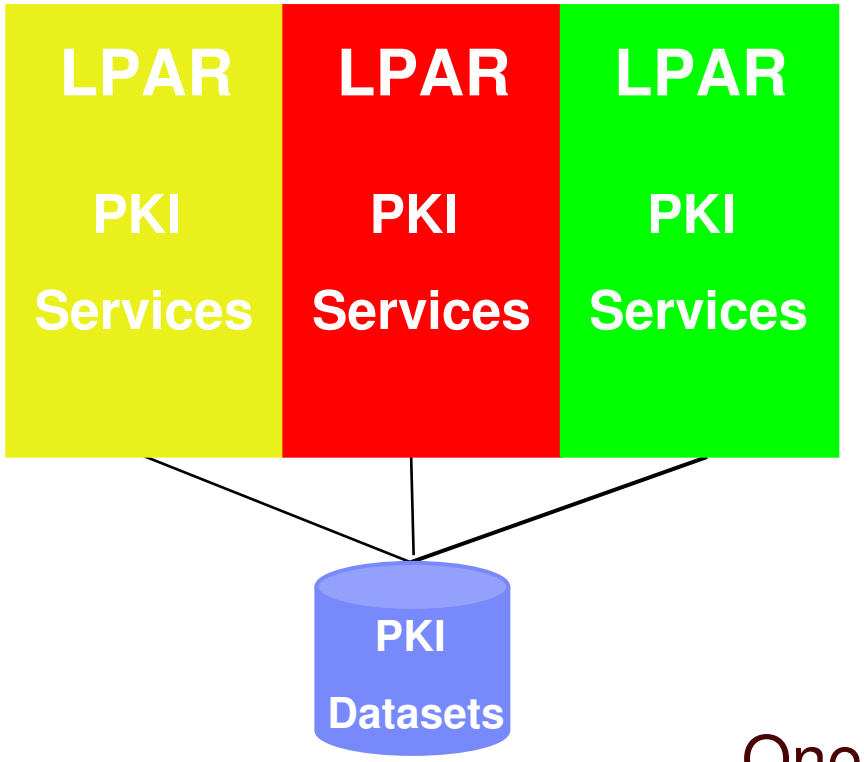
Subject:	CN=Wai,OU=ibm,C=us
Issuer:	CN=new_CA%2,O=ibm,C=us
Validity:	2005/01/05 00:00:00 - 2006/01/04 23:59:59
Usage:	handshake(digitalSignature, keyEncipherment)
Extended Usage:	clientauth
AltIPAddr:	9.56.53.111
AltURI:	http://plpsc.pok.ibm.com
AltEmail:	wchoi@us.ibm.com
AltDomain:	plpsc.pok.ibm.com
AltOther:	Other Name for alternate name: Customer's account number (11 digits) 11111111111
AltOther:	Other Name for alternate name: Customer's driver license number (9 digits) 222222222 Customer's driver license expiration date (yyyymmdd) 20051231
HostIdMap:	wai@pokvmtl4.pok.ibm.com

Enhancements on z/OS V1R8

- **z/OS PKI Services is deploying Simple Certificate Enrollment Protocol (SCEP) permitting the router to talk directly to the Certification Authority in a secure fashion.**
- **Allow multiple instances of PKI Services to be run in one LPAR**
- **Provide additional distinguished name qualifiers in the subject name for the routers and firewall machines**
- **Creation of Windows Smart Card Logon certificate with extended key usage 'Microsoft Smart Card Logon'**
  - The Bank is planning to issue certificates on smart cards for the employees to access the office buildings, logon to the machines, access network from home through the dialer…

Other benefits of using PKI Services

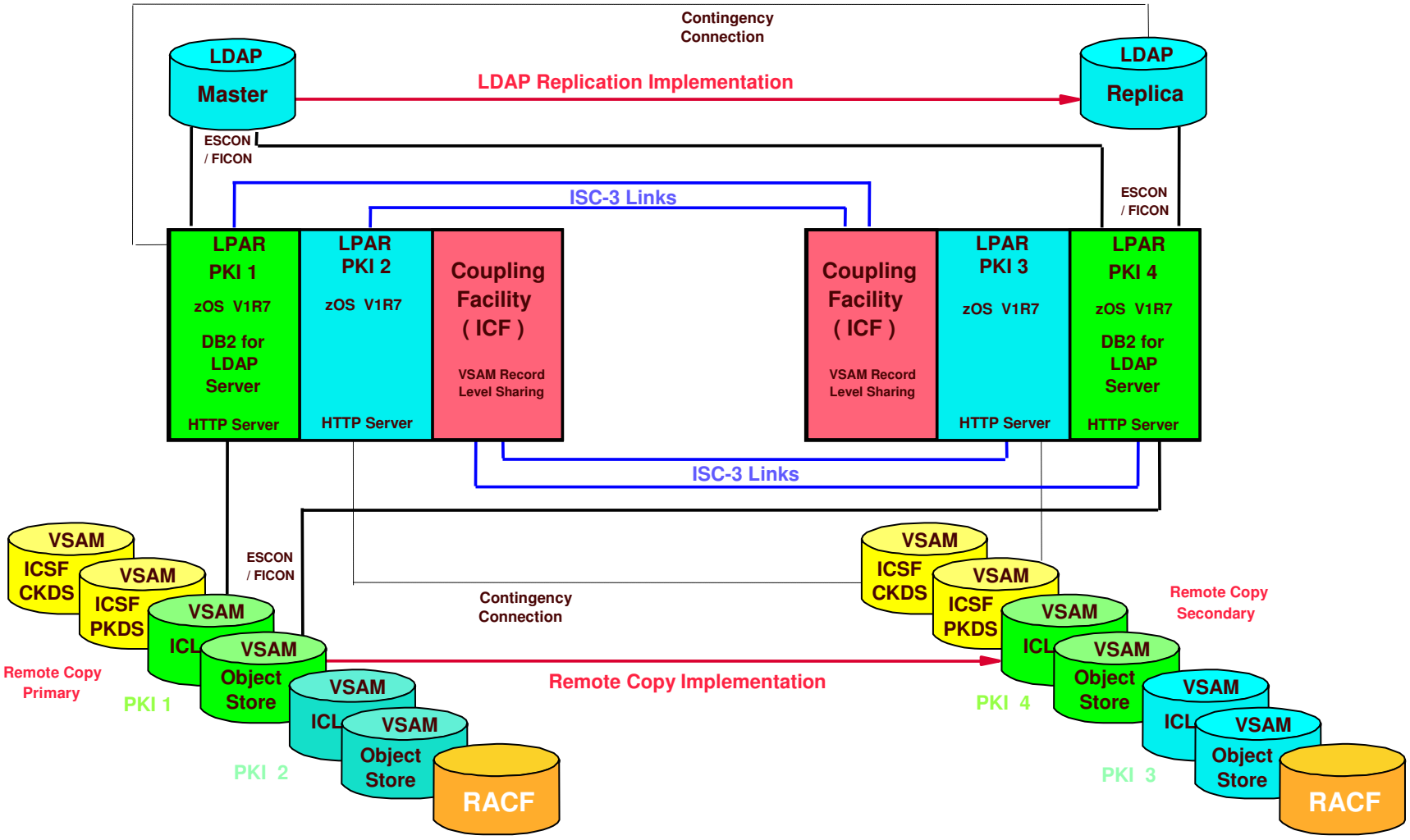
Very Scalable Solution

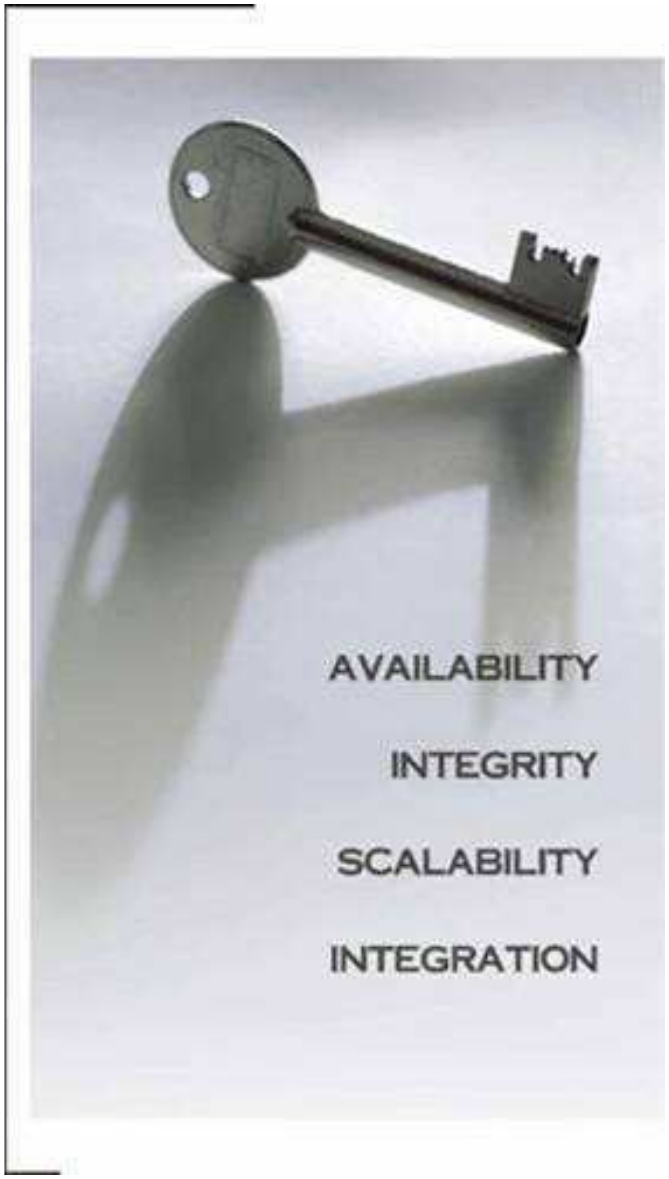


One PKI Server per LPAR

LPAR Isolation (EAL5 Certification)

High Available Infrastruture – the next step Banco do Brasil will take



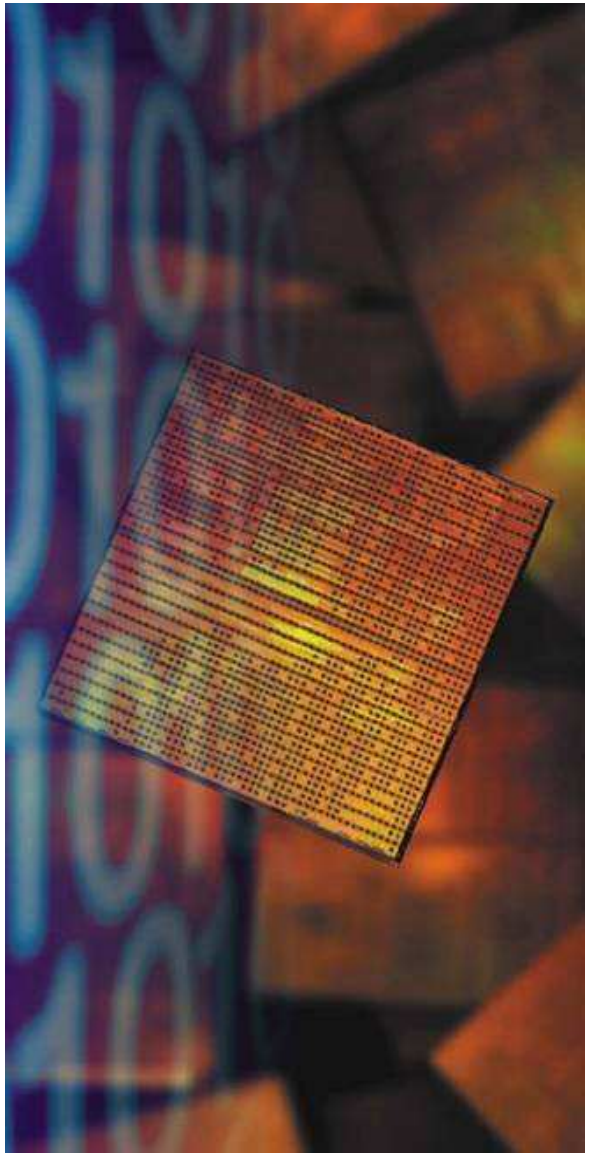


Performance

- 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 on average 3 minutes.

Very Secure Solution

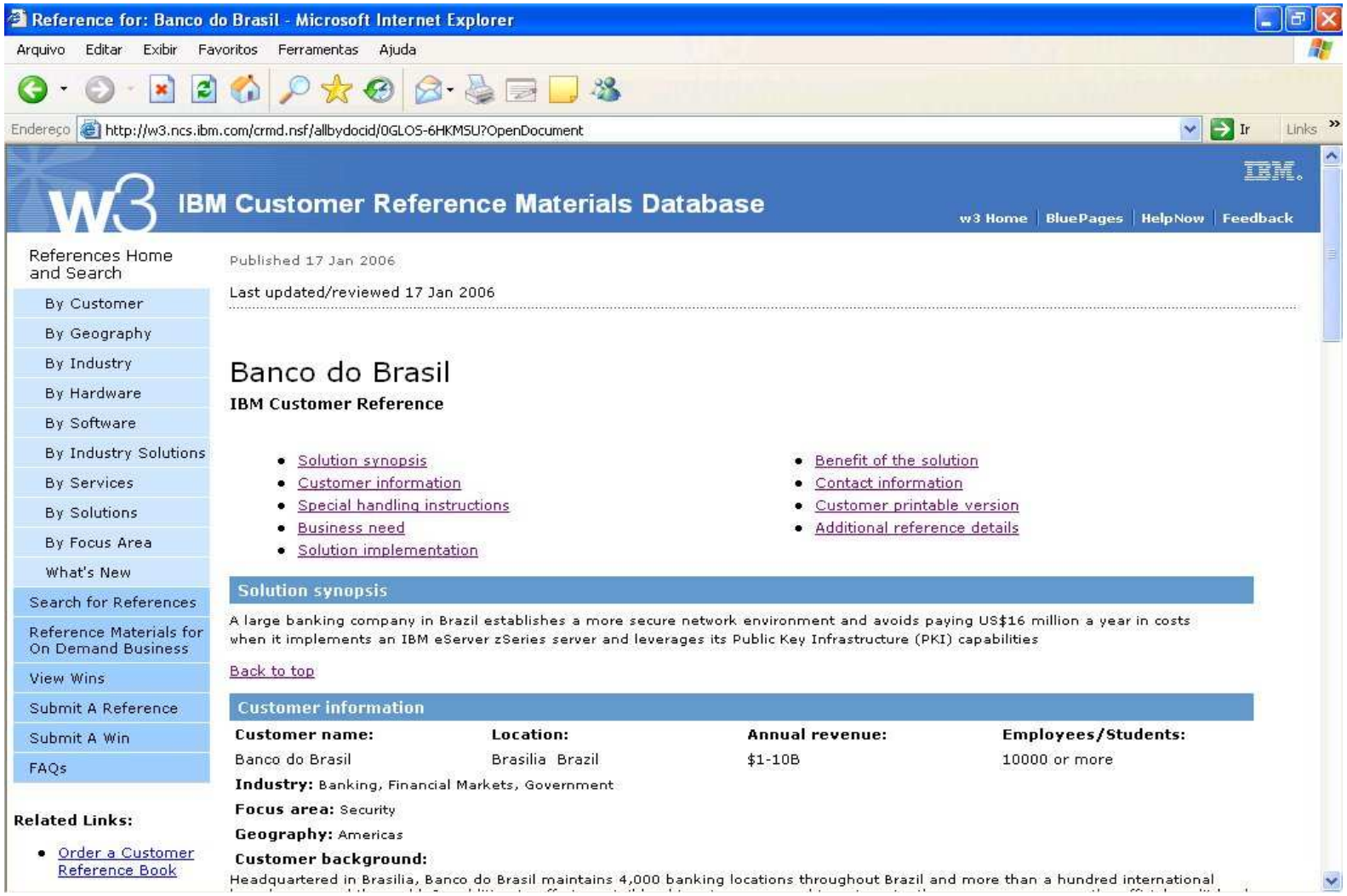
- **Cryptographic coprocessor available on zSeries**
  - Designed to meet FIPS 140-2 Level 4 specification
- **Keep the Certification Authority Private Key in a very secure boundary**
- **Cryptographic hardware access controlled by RACF**



Session 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

IBM Customer Reference Materials Database

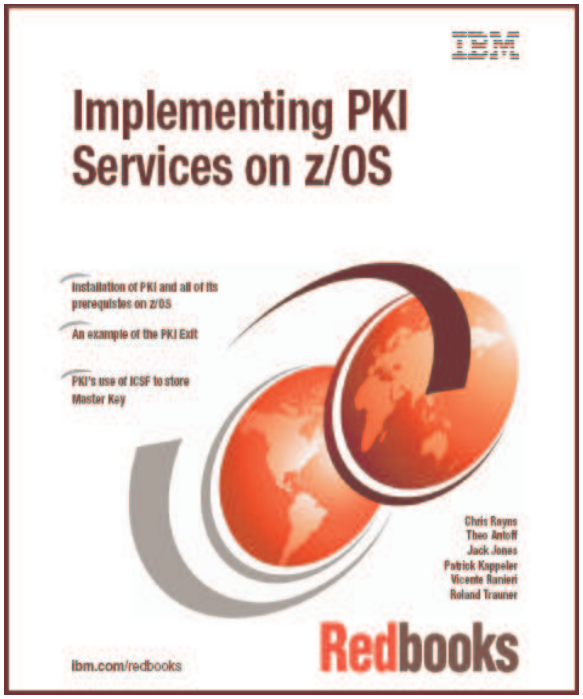


http://w3.ncs.ibm.com/crmd.nsf/allbydocid/0GLOS-6HKMSU?OpenDocument

PKI Services Bibliography

Publications

- **Implementing PKI Services on z/OS (SG24-6968)**



- *z/OS Cryptographic Services PKI Services Guide and Reference* (*SA22-7693*)
- *z/OS Security Server RACF Command Language Reference* (*SA22-7687*)
- *z/OS Security Server RACF Security Administrator's Guide* (*SA22-7683*)
- *z/OS Security Server RACF Callable Services* (*SA22-7691*)
- *z/OS Integrated Security Services LDAP Server Administration and Use* (*SC24-5923*)
- *z/OS Security Server Open Cryptographic Enhanced Plug-ins Application Programming* (*SC24-5925*)
- *z/OS OCSF Service Provider Module Developer's Guide and Reference* (*SC24-5900*)
- *z/OS Cryptographic Services System Secure Sockets Layer Programming* (*SC24-5901*)
- *z/OS Cryptographic Services ICSF Administrator's Guide* (*SA22-7521*)
- *z/OS HTTP Server Planning, Installing, and Using* (*SC34-4826*)

Websites

- PKI Services http://www-1.ibm.com/servers/eserver/zseries/zos/pki
- PKIX http://www.ietf.org/html.charters/pkix-charter.html
- Identrus http://www.identrus.com