24TH ANNUAL
VANGUARD SECURITY 2010
the ONE event you need to attend
Flamingo Las Vegas
April 19-22, 2010

RTT10 - PKI Services: The Best Kept Secret in z/OS

Wai Choi
IBM Corporation

21-Apr-10

Session Abstract:

Most people know about RACDCERT to manage digital certificates. But there is a newer component of PKI Services providing digital certificate services. It is a complete digital certificate authority included in the base of z/OS at no additional charge. We will introduce the full cycle certificate management provided by PKI Services, compare it with RACDCERT and discuss its newest unique key generation feature introduced in V1R11.

Instructor's Bio:

Ms. Wai Choi works in RACF/PKI development, design and test at IBM. Her expertise has made her classes popular at the Vanguard conferences. She also actively participates in the RACF-L forum answering certificate related questions.

Note: These Materials present the views and opinions of the Author. Vanguard does not necessarily endorse the materials and Vanguard is not responsible for the accuracy of the materials. These materials may not be redistributed or reproduced without the express permission of Vanguard or the Author.

PKI Services: The Best Kept Secret in z/OS

Vanguard Las Vegas, NV
Session RTT10
April 21st 2010

Wai Choi, CISSP
IBM Corporation
RACF/PKI Development & Design
Poughkeepsie, NY

e-mail: wchoi@us.ibm.com

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

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…

z/OS PKI Services

- Not a priced product. Licensed with z/OS
  - not getting enough marketing focus
  - not sure if IBM will continue the investment in this ‘free’ component
- A component on z/OS since V1R3, V1R11 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

z/OS PKI Services

– **Provide more functions than RACDCERT**

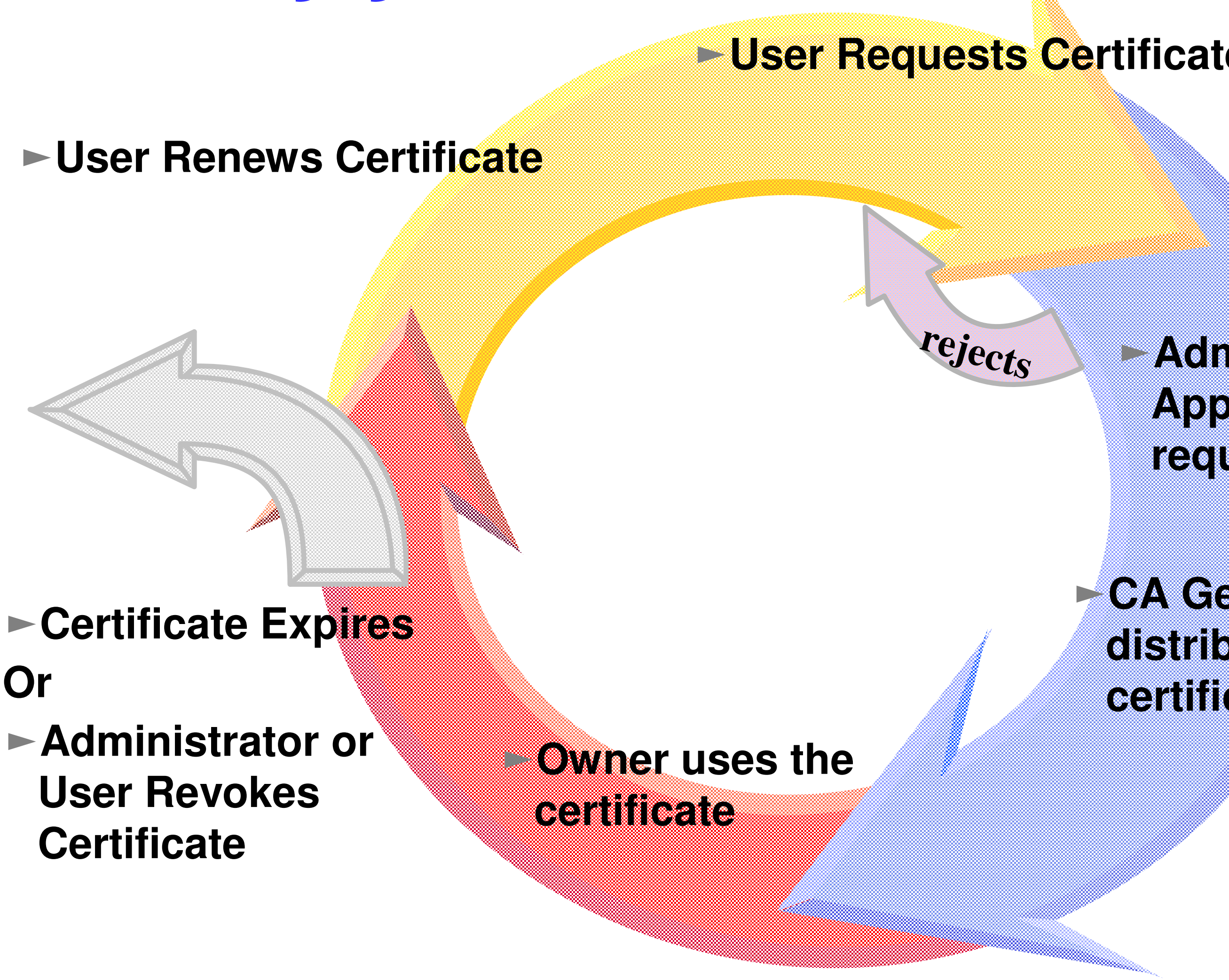
- Full certificate life cycle management: request, create, renew, revoke
- Generation and administration of certificates via customizable web pages
- Support automatic or administrator approval process
- Certificates can be picked up from the requestor's machine
- Support multiple revocation checking mechanisms
  - Certificate Revocation List (CRL)
  - Online Certificate Status Protocol (OCSP)
- Certificates and CRLs can be posted to LDAP and/or stored in an HFS file
- Support Simple Certificate Enrollment Protocol (SCEP) to enable routers to request/renew certificates automatically

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

– Provides Trust Policy Plug-in for certificate validation

Certificate Life Cycle – This is why you need PKI Services



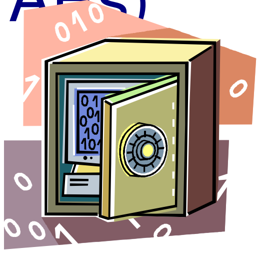
- User Requests Certificate
- Administrator Approves the request
- CA Generates and distributes certificate
- Owner uses the certificate
- Certificate Expires

Or

- Administrator or User Revokes Certificate
- User Renews Certificate

Other benefits of using PKI Services

- An alternative to purchasing third party certificates
  - Cost efficient for banks, government agencies to host Digital Certificate management
- Provide options for requestor to generate his own key pair or request the PKI CA to generate it
- 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
- Run in separate z/OS partitions (integrity of zSeries® LPARs)
- Scalable (Sysplex exploitation)
- Secure the CA private key with zSeries cryptography



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

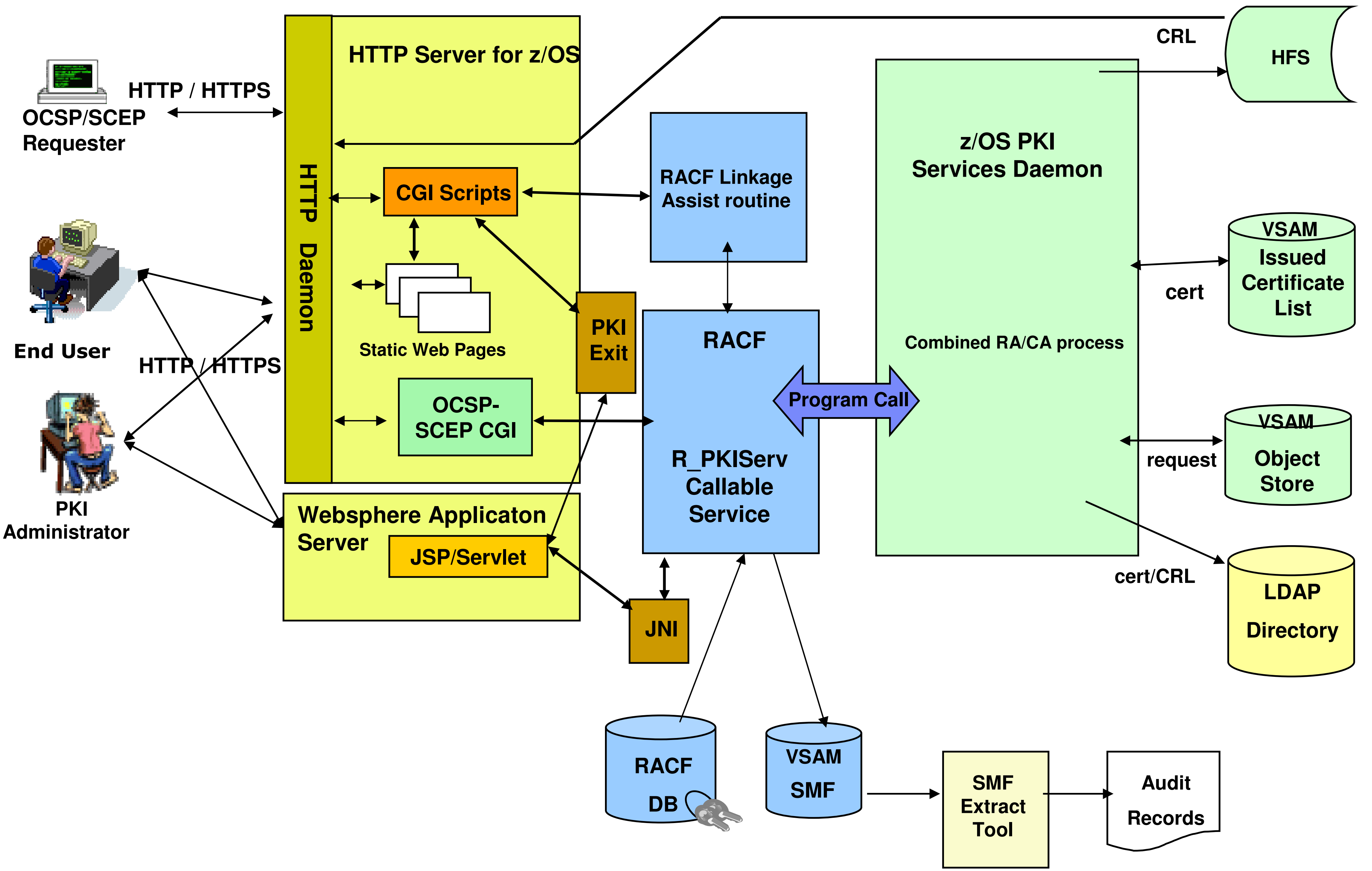
–ICSF (optional)

- For more secure CA private key
- For PKI CA to generate key pair

–z/OS Communications Server (optional)

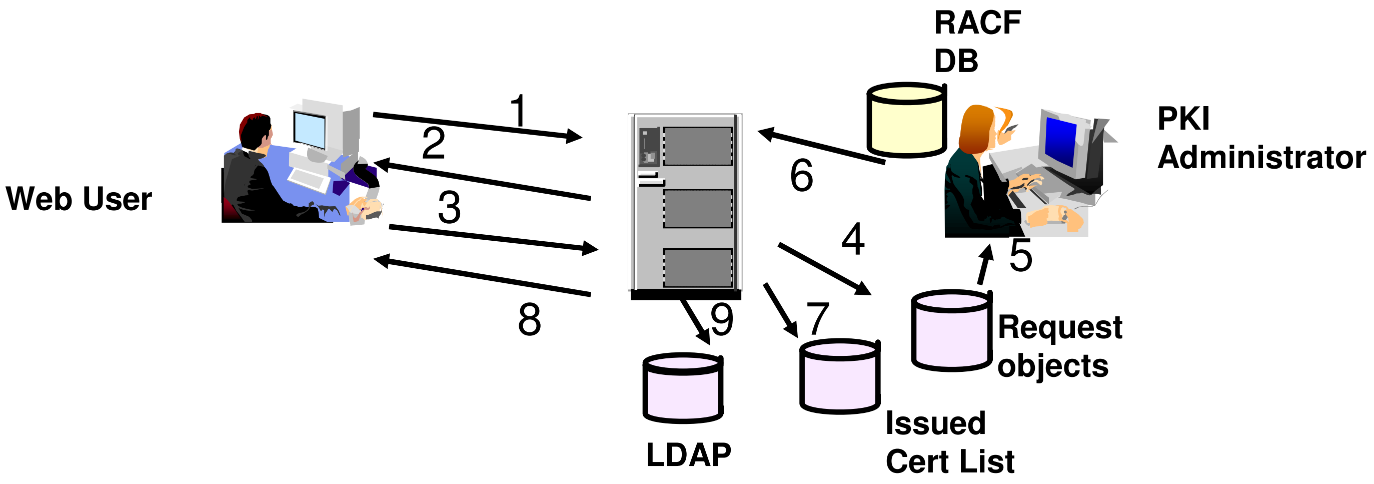
- For email notification

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/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…

Continuous enhancements

V1R8:

- Support 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
- Creation of Windows Smart Card Logon certificate with extended key usage 'Microsoft Smart Card Logon'

V1R9:

- Automatic certificate renewal, email to user
- Email notification to administrator on pending requests
- Support SDBM credential for LDAP
- Query on expiring certificates

Continuous enhancements (contd)

V1R10:

- Support Alternate Name extension with IPv6 format
- Support Subject Distinguished Name with non-English character set
- Support long Subject Distinguished Name up to 1024 characters (PTF UA52091)
- Add three additional distinguished name attribute types
  - Distinguished Name Qualifier
  - Domain Component
  - User ID
- Remove dependency on the Open Cryptographic Services Facility (OCSF) component

Continuous enhancements (contd)

V1R11:

- Support long Subject Distinguished Name up to 1024 characters (PTF UA52092)
- Provide option for the user to request PKI CA to generate the key pair
- Provide support for key recovery for those generated by the PKI CA
- Support SHA256 in the signing algorithm
- Implement the web pages with XML and JSPs to facilitate the integration with PKI Services from other applications

Continuous enhancements (contd)

V1R12 (Preview)

- Support Elliptic Cryptographic Curve (ECC) keys, in addition to RSA and DSA keys
- Support Certificate Management Protocol (CMP) clients to communicate with PKI Services
- Provide automatic detection and correction on the potential problem causing by the used serial number
- Provide utilities to post certificates and Certificate Revocation List (CRL) on demand.
- Provide configurable time switches for the housekeeping tasks
- Support the creation of custom extensions to certificate
- Support the creation of Subject Alternate Name that contains multiple instances of each of the General Name forms
- Support the creation of certificates with expiration dates in the far future

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

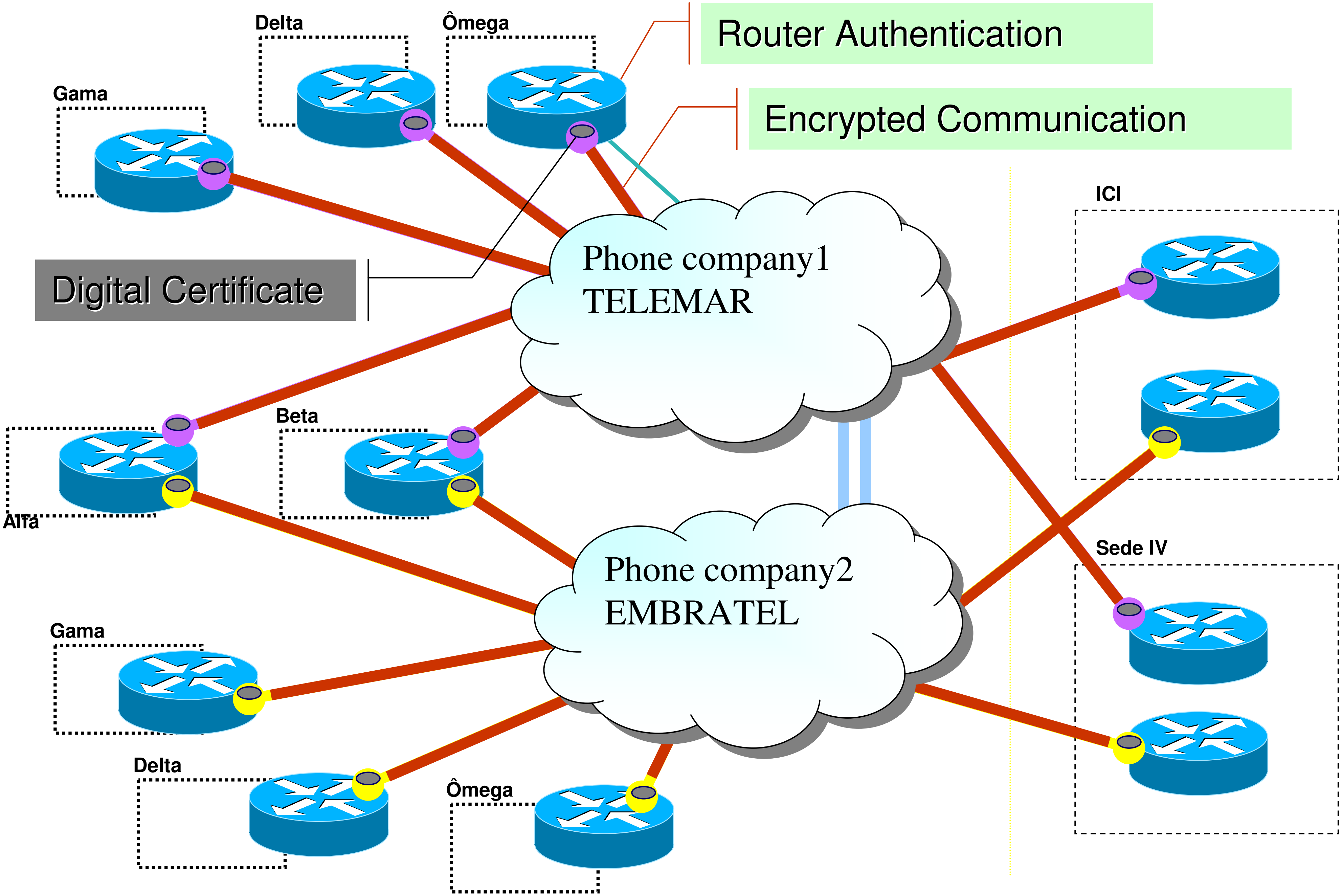
- Owned by the Brazilian government
- The largest bank in Brazil
- Over 200 years old
- It maintains 4,000 banking locations throughout the country and more than a hundred international branches in 23 countries
- It has more than 40,000 ATM machines - the largest number of ATM machines in the financial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

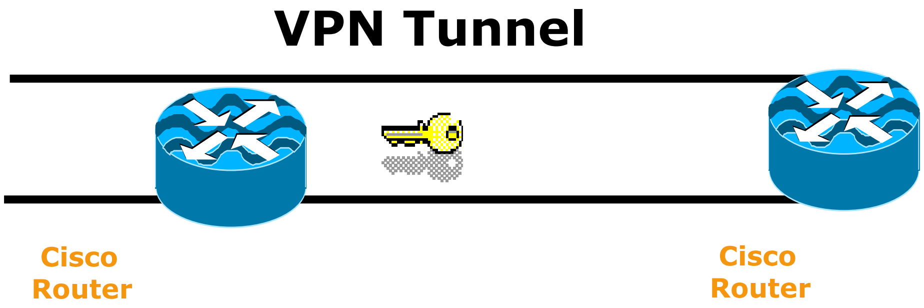
Solutions considered

- **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

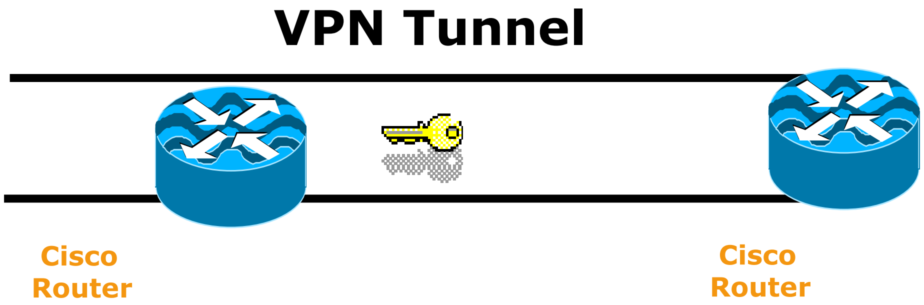
- Banco do Brasil submitted requirements to IBM to enhance PKI Services
- After knowing that the requirements were in plan, Banco do Brasil decided to start exploiting z/OS PKI Services to issue its VPN digital certificates

Banco do Brasil Solution

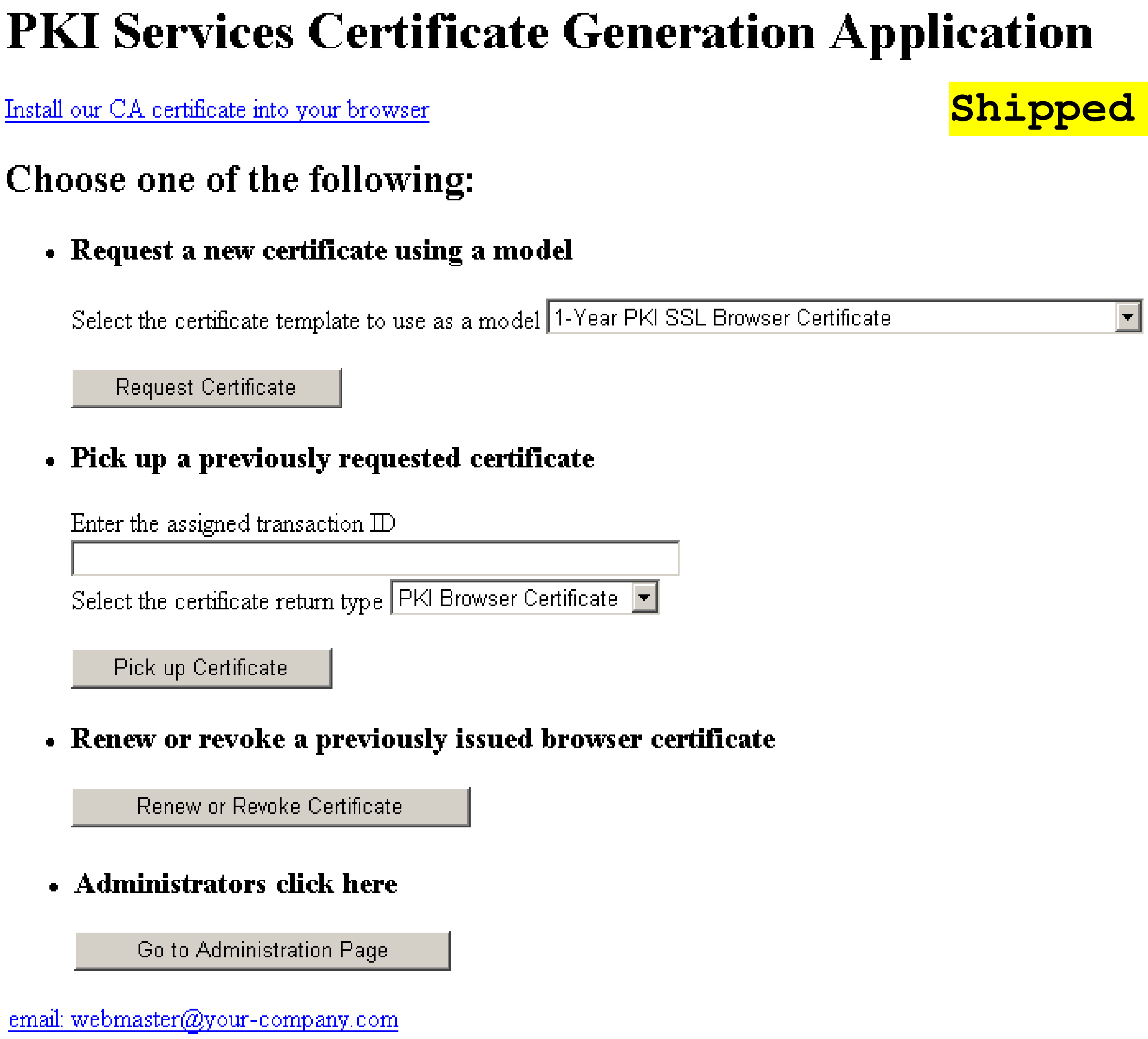


- In Brazil, there are 2 ways to be a certified CA
  - get a certification from the PKI Brazil government department which requires the PKI application runs alone on a separate machine (the bank is working on getting the acceptance that LPAR isolation is as good as a stand alone machine)
  - the issuer 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]

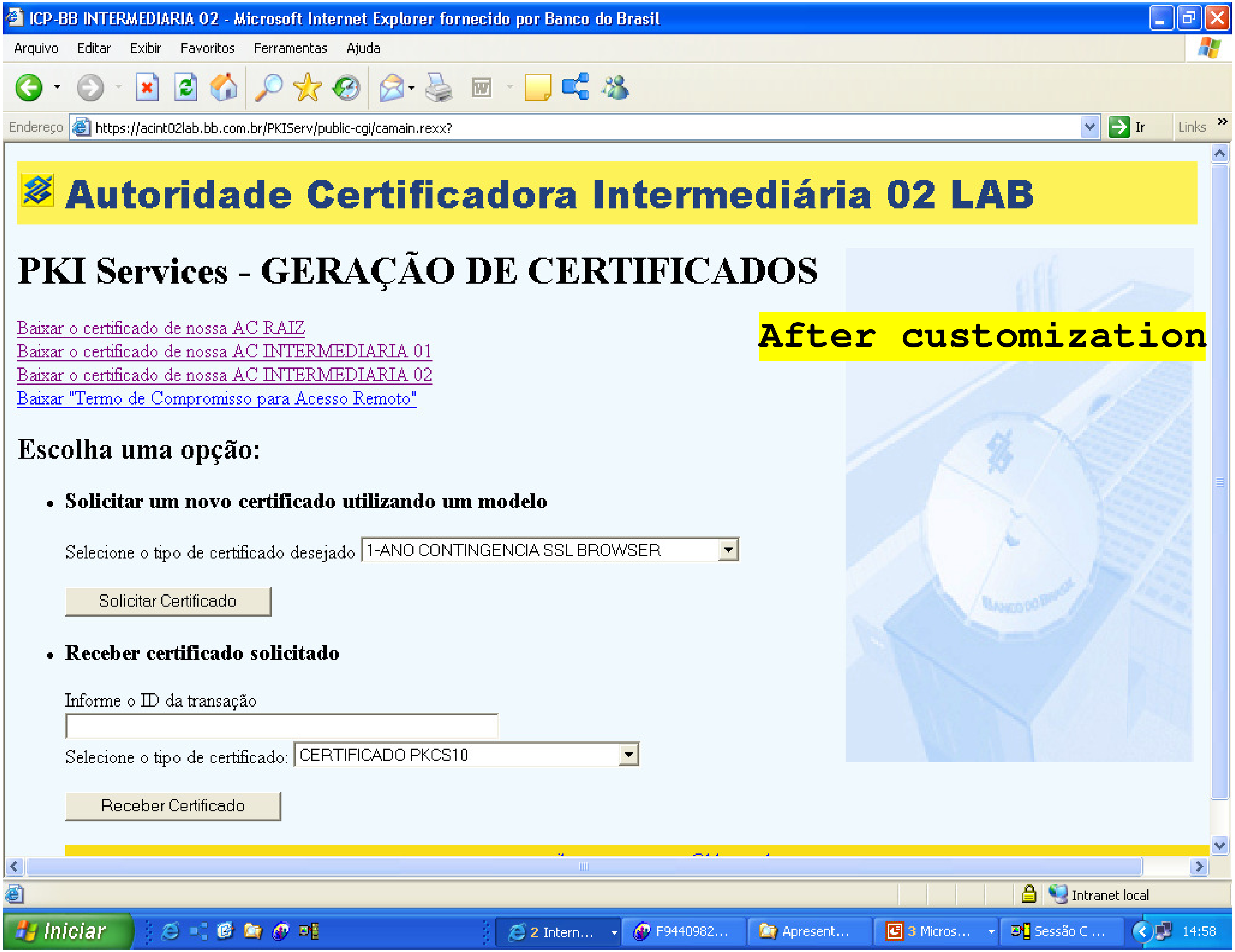
- **Renew or revoke a previously issued browser certificate**

  [Renew or Revoke Certificate]

- **Administrators click here**

  [Go to Administration Page]

email: webmaster@your-company.com



Endereço: 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"

After customization

Escolha uma opção:

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

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

  Solicitar Certificado

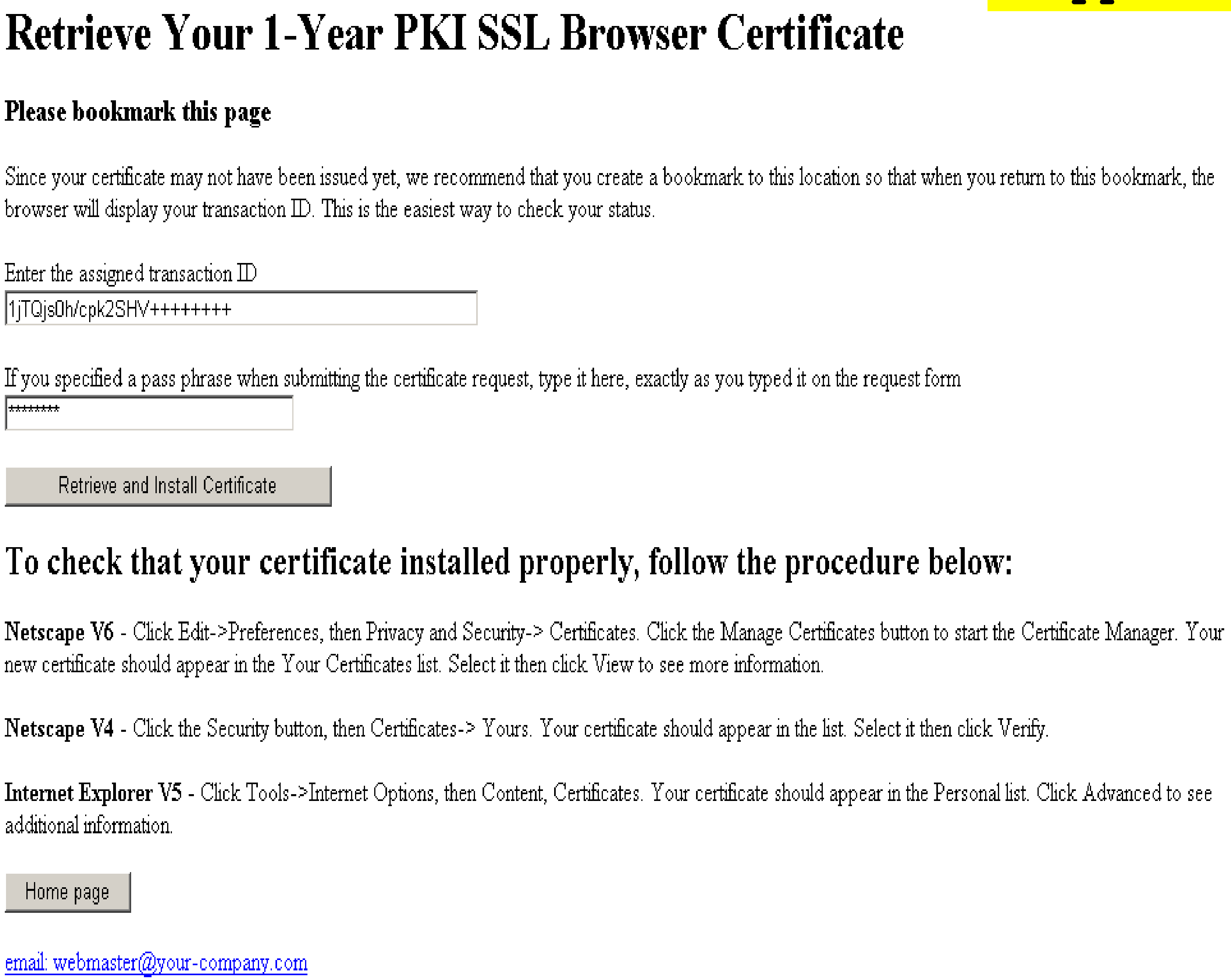
- **Receber certificado solicitado**

  Informe o ID da transação

  Selecione o tipo de certificado: CERTIFICADO PKCS10

  Receber Certificado

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:

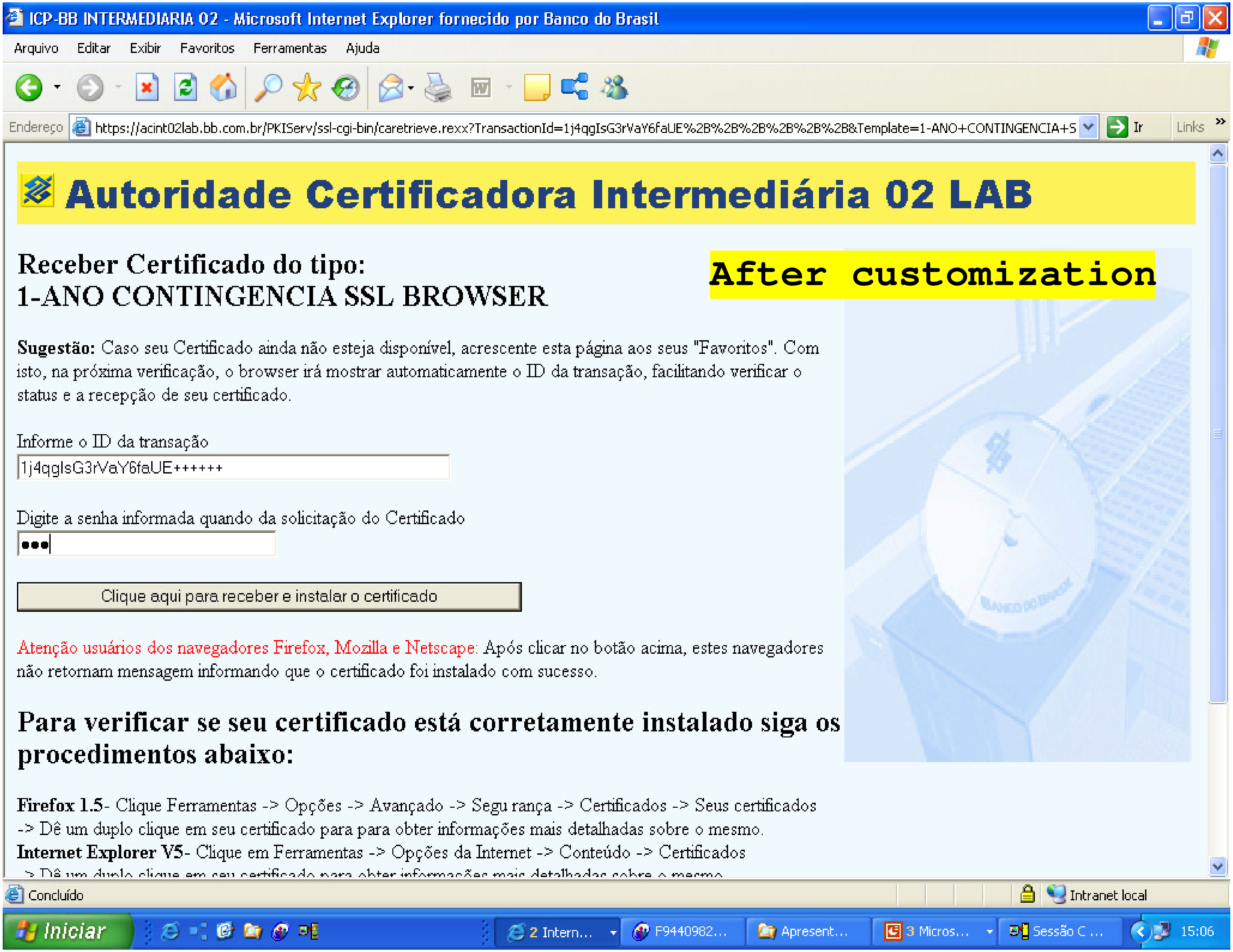
Netscape V6 - Click Edit->Preferences, then Privacy and Security-> Certificates. Click the Manage Certificates button to start the Certificate Manager. Your new certificate should appear in the Your Certificates list. Select it then click View to see more information.

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



https://acint02lab.bb.com.br/PKIServ/ssl-cgi-bin/caretrieve.rexx?TransactionId=1j4qgIsG3rVaY6faUE%2B%2B%2B%2B%2B%2B&Template=1-ANO+CONTINGENCIA+S

Autoridade Certificadora Intermediária 02 LAB

After customization

Receber Certificado do tipo:
1-ANO CONTINGENCIA SSL BROWSER

Sugestão: Caso seu Certificado ainda não esteja disponível, acrescente esta página aos seus "Favoritos". Com isto, na próxima verificação, o browser irá mostrar automaticamente o ID da transação, facilitando verificar o status e a recepção de seu certificado.

Informe o ID da transação
1j4qgIsG3rVaY6faUE++++++

Digite a senha informada quando da solicitação do Certificado
•••

Clique aqui para receber e instalar o certificado

Atenção usuários dos navegadores Firefox, Mozilla e Netscape: Após clicar no botão acima, estes navegadores não retornam mensagem informando que o certificado foi instalado com sucesso.

Para verificar se seu certificado está corretamente instalado siga os procedimentos abaixo:

Firefox 1.5- Clique Ferramentas -> Opções -> Avançado -> Segu rança -> Certificados -> Seus certificados -> Dê um duplo clique em seu certificado para para obter informações mais detalhadas sobre o mesmo.
Internet Explorer V5- Clique em Ferramentas -> Opções da Internet -> Conteúdo -> Certificados -> Dê um duplo clique em seu certificado para obter informações mais detalhadas sobre o mesmo.

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 on 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

- **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.**