



# **IBM HTTP Server (IHS) with the OS/390 Digital Certificate in Release 10**

Paul de Graaff  
Field Technical Sales Specialist  
E-Mail : [graaff@us.ibm.com](mailto:graaff@us.ibm.com)

February 27 2001 - Session Number 1721  
The Westin Hotel

# Agenda



## IBM HTTP Server (IHS) 5.3 Support for RACF Keyrings

- Use of System SSL - Change in Key Management

## RACF SPE - Digital Certificate Enhancements

- Replacement of CA Servlet (GO CA)

# RACF Keyring support

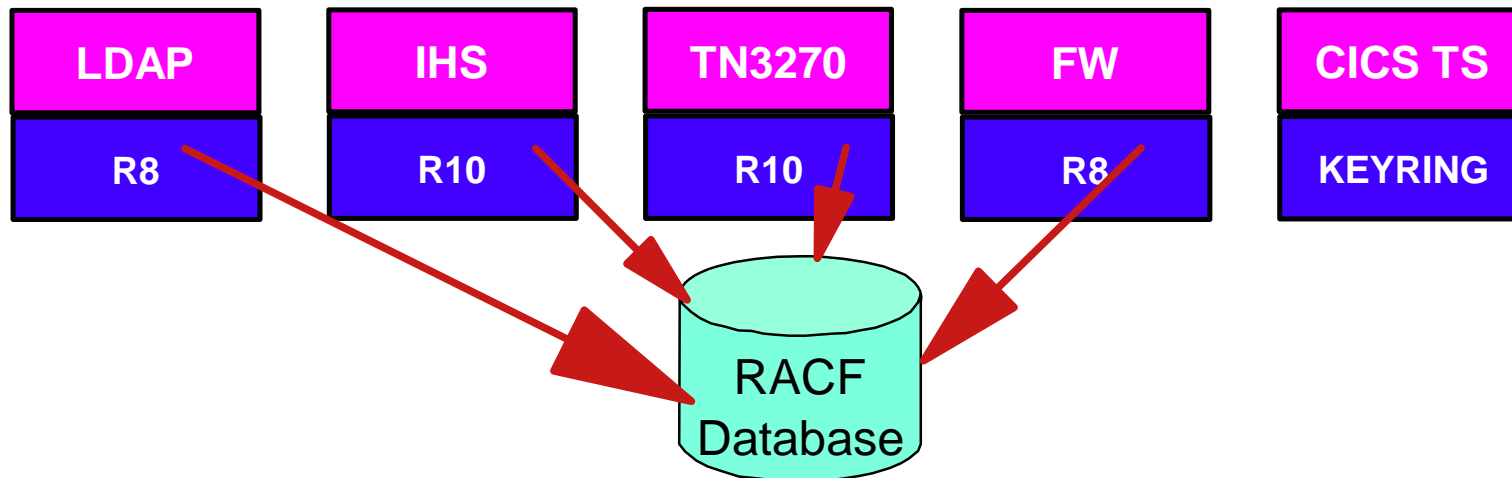


Every product had/has his own keyring !



Managed by MKKF, IKEYMAN or GSKKYMAN !

**Release 8 added keyring support to RACF**



# RACF Keyring Support in V2R8



## RACDCERT GENCERT

- create public/private key pair and digital certificates

## RACDCERT ADDRING or CONNECT

- create keyring and add certificates

# IBM HTTP Server (IHS) 5.3



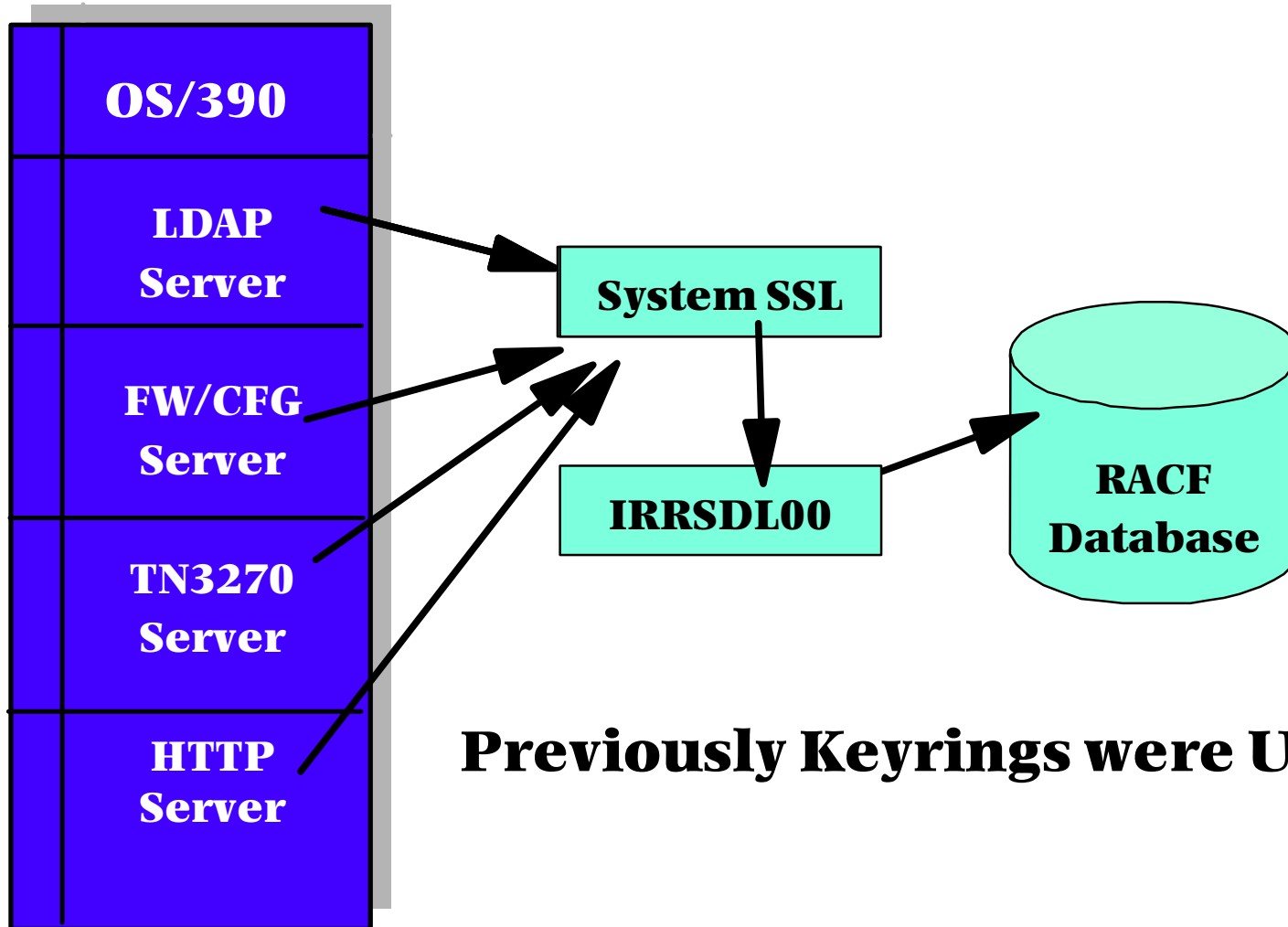
## Exploits System SSL

- Changes in key Management

- uses GSKKYPAN instead of IKEYMAN to manage your digital certificate and keyring (USS File)
- support for RACF keyrings - generated using RACDCERT ADDRING
- server certificate generated using RACDCERT GENCERT or imported using RADCERT ADD

Note: The ICSF is not (yet) supported for digital certificates in RACF Keyrings

# RACF Key Rings



**Previously Keyrings were USS Files**

# RACF Keyring Set-up



## Generate digital certificate for the Server

- `RACDCERT GENCERT ID(WEBSRV) SUBJECTSDN(CN('WTSC57.ITSO.IBM.COM')  
OU('ITSO')O('IBM')L('POUGHKEEPSIE')SP('NEW YORK')C('US'))  
SIZE(1024) WITHLABEL('SC57W') SIGNWITH(CERTAUTH LABEL('ITSO CA'))  
KEYUSAGE(HANDSHAKE)`

## Create RACF Keyring

- `RACDCERT ID(WEBSRV) ADDRING(SC57WEB)`

## Associate the digital certificate of server and any CA's with the RACF keyring

- `RACDCERT ID(WEBSRV) CONNECT(ID(WEBSRV)LABEL('SC57W') RING(SC57WEB)  
DEFAULT USAGE(PERSONAL))`

# RACF Key Ring Example



```
racdcert id(websrv) listring(sc57web)
```

Digital ring information for user WEBSRV:

Ring:

```
>sc57web<
```

Certificate Label Name	Cert Owner	USAGE	DEFAULT
-----	-----	-----	-----
sc57w	ID(WEBSRV)	PERSONAL	YES

```
racdcert id(tcpipu) listring(*)
```

Digital ring information for user TCPIPU:

Ring:

```
>telnetserver<
```

Certificate Label Name	Cert Owner	USAGE	DEFAULT
-----	-----	-----	-----
ITSO CA	CERTAUTH	CERTAUTH	NO
telnetserver	ID(TCPIPU)	PERSONAL	YES
peggy's test cert	ID(TCPIPU)	PERSONAL	NO



# RACF Certificate Example



RACDCERT ID(WEBSRV) LIST(LABEL(SC57W))

Label: sc57w

Certificate ID: 2QbmxcLi2eWig/X3pkBA

Status: TRUST

Start Date: 2000/10/02 23:00:00      End Date: 2001/10/03 22:59:59

Serial Number:

>00<

Issuer's Name:

>CN=wtsc57.itso.ibm.com.OU=ITSO.O=IBM.C=US<

Subject's Name:

>CN=wtsc57.itso.ibm.com.OU=ITSO.O=IBM.C=US<

Key Usage: HANDSHAKE

Private Key Type: Non-ICSF

Private Key Size: 1024

Ring Associations:

Ring Owner: WEBSRV

Ring: >sc57web<

# HTTPD.CONF changes



The **KEYFILE** directive now points to the **LABEL** of the RACF keyring;

The owner of the keyring and the (default) digital certificate has to be the User ID associated with the HTTP Server's Started Task (webserv in our case !)

The changes to the **KEYFILE** directive is as follows:

- **keyfile label SAF**

The Started Task User ID needs READ access to :

- IRR.DIGTCERT.LIST in the FACILITY class
- IRR.DIGTCERT.LISTRING in the FACILITY class



# PKISERV - Release 10

## Digital Certificate Enhancement

Technology ▪ Connections ▪ Results

# A little History First



The GO CA function was introduced in DGW 5.0 and was later renamed to the CA Servlet in the IBM HTTP Server rename timeframe.

It provided PKI capabilities to the OS/390 platform

It was able to generate digital certificates for :

- Personal Digital Certificates (Browser)
- Server Digital Certificates

Certificate Authority - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Guide Print Security Stop

Bookmarks Location: http://wtsc58oe.iso.ibm.com/ServletExpress/resources/CAServlet/Welcome.html

Instant Message Internet Lookup New&Cool

# CERTIFICATE AUTHORITY

## Browser Certificates

1. [Download](#) CA certificate from the Webserver.
2. [Request](#) a browser certificate.
3. [Receive](#) the approved certificate.

## Server Certificates

1. [Download](#) CA certificate from the Webserver.
2. [Request](#) a server certificate.
3. [Receive](#) the approved certificate.

[Administration](#)

Simplify administering your private network by using the Certificate Authority to request, process, and receive browser and server certificates.

To use the Certificate Authority:

- Complete the steps in [Preparing to use Certificate Authority](#).
- Use Netscape Navigator Version 3.0 or higher to open the Certificate Authority (this page).
- On the menu, select the task you want to perform.

Document Done

# CERTIFICATE AUTHORITY

## Browser Certificates

1. [Download](#) CA certificate from the Webserver.
2. [Request](#) a browser certificate.
3. [Receive](#) the approved certificate.

## Server Certificates

1. [Download](#) CA certificate from the Webserver.
2. [Request](#) a server certificate.
3. [Receive](#) the approved certificate.

## [Administration](#)

## Browser Certificate Request

Key Size:  (required)

Common Name:  (required)

Organization:  (required)

Organization Unit:

Locality/City:

State:

Zip Code:

Country:  (required)

Email address:

Challenge Phrase:  (required)

# PKISERV Introduction



Release 10 Introduces a Web based application to generate:

- Personal (Browser) Digital Certificates
- Sign Digital Certificates for non-390 based Server

The following APARs are required:

- RACF APAR OW45211
- SAF APAR OW45212

It is a replacement for the CA Servlet shipped previously with IBM HTTP Server for OS/390 Release 5.2 and prior.

# PKISERV Introduction ...



Documentation is available from the RACF Homepage

Soon redbook SG24-5675 will have the documentation as well, plus examples.



# PKISERV Introduction ...



PKISERV is basically a web based interface to some of the RADCERT capabilities available in Release 10:

Release 8 supported generation of digital certificates

- no export function of the certificate in PKCS#12
- was targeted at OS/390 Servers

Release 10 will no longer support the CA Servlet function

- RACF will now allow export of certificates in PKCS#12 format

# PKISERV Introduction ...



You can also generate Digital Certificates using

- RACDCERT GENCERT

To export the certificate you will need to take the following steps:

- RACDCERT EXPORT
- Download to your PC
- Import it to your Browser (IE, Netscape)

The Web based interface eliminates these cumbersome steps !!

# RACDCERT GENCERT Syntax



## RACDCERT

[ ID(userid) | CERTAUTH | SITE ]

GENCERT[('request-data-set-name')]

[SUBJECTSDN([C('country')]

[SP('state-or-province')]

[L('locality')]

[O('organization-name')]

[OU('organization-unit-name1'

[,'organization-unit-name2',...]

)]

[T('title')]

[CN('common-name')] )]

# RACDCERT GENCERT Syntax ...



**[SIZE(key-size)]**  
**[NOTBEFORE([DATE(yyyy-mm-dd)]**  
**[TIME(hh:mm:ss)])]**  
**[NOTAFTER([DATE(yyyy-mm-dd)]**  
**[TIME(hh:mm:ss)])]**  
**[WITHLABEL('label-name')]**  
**[SIGNWITH([CERTAUTH|SITE]**  
**LABEL('label-name'))]**  
**[ICSF]**

# RACDCERT GENCERT Syntax ...



**[KEYUSAGE(HANDSHAKE DATAENCRYPT  
DOCSIGN CERTSIGN)]**

**[ALTNAME(**

**IP(numeric-ip-address)**

**DOMAIN('internet-domain-name')**

**EMAIL('email-address')**

**URI('universal-resource-identifier'))]**

**]**

# RACDCERT EXPORT Syntax



**RACDCERT**

**[**

**| EXPORT ( LABEL('Label Name') )**

**DSN('Output Dataset Name')**

**[ FORMAT(CERTDER | CERTB64 |**

**PKCS12DER | PKCS12B64) ]**

**[ PASSWORD('PKCS12 Password') ]**

# PKISERV - Configuration



Configuration File (**PKI.CONF**) allows for flexible configuration

Differences with the CA Servlet:

- Provides no administration approval process (auto-approved)
- Digital Certificate requests are based on RACF permissions to FACILITY class profiles !

# PKISERV - Configuration ...



The structure of the configuration File (**PKI.CONF**) is:

- Templates define the type of certificates you want to generate and/or approve
  - SAF Browser Certificate 1 Year (provided)
  - SAF Server Certificate 1 Year (provided)
- **CONTENT** Section - What HTML to display
- **APPL** Section - identifies certificate fields the application should provide (User ID)
- **CONSTANT** Section - certificate fields that have a hardcoded value



# PKISERV - Configuration ...



The structure of the configuration File (**PKI.CONF**) is:

- **SUCCESSCONTENT** Section - display HTML when cert request is successful
- **FAILURECONTENT** Section - display HTML when cert request fails
- **RETRIEVECONTENT** Section - display HTML to enable cert retrieval
- **RETURNCERT** Section - display HTML when cert retrieval successful

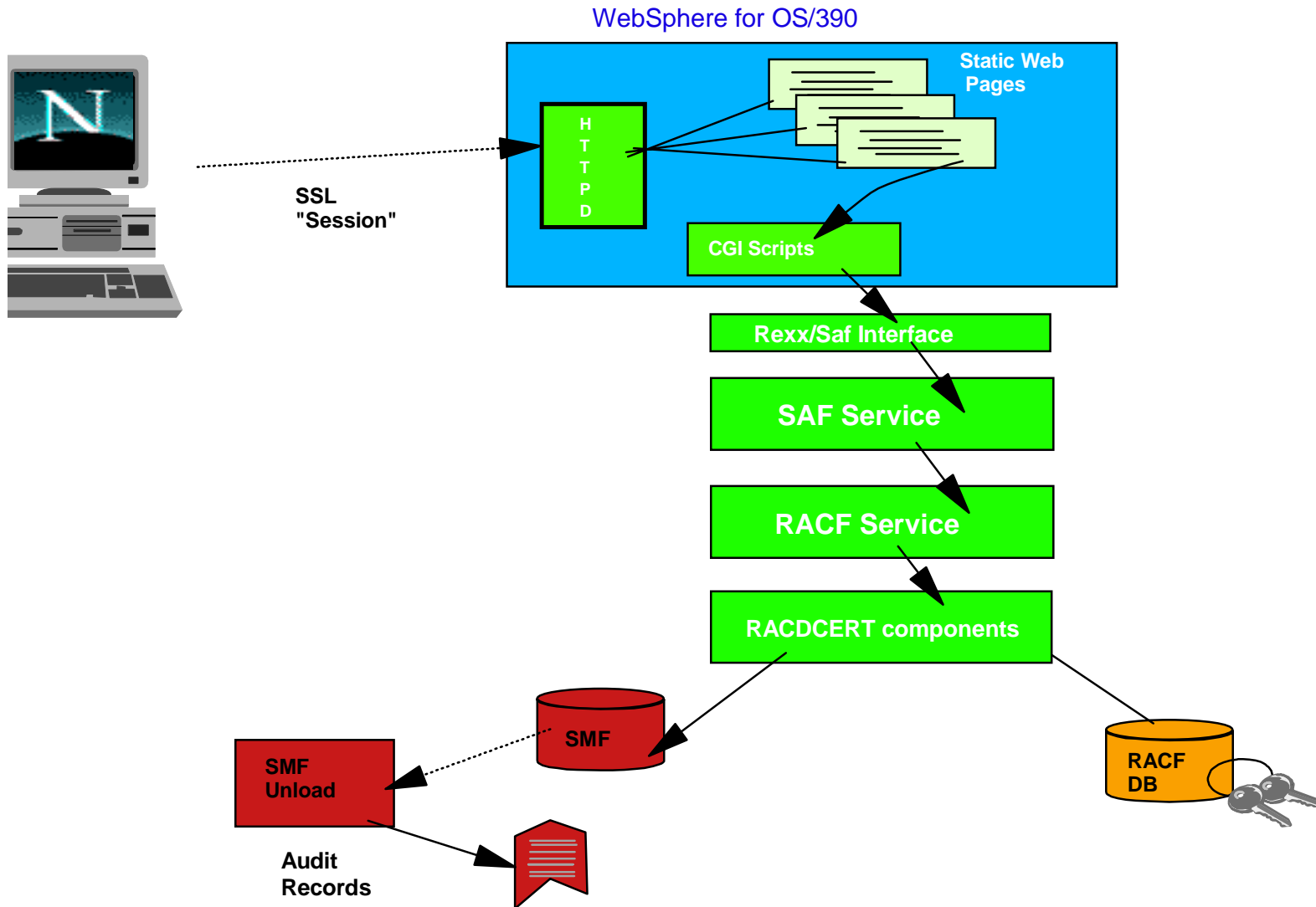
# PKISERV - Configuration ...



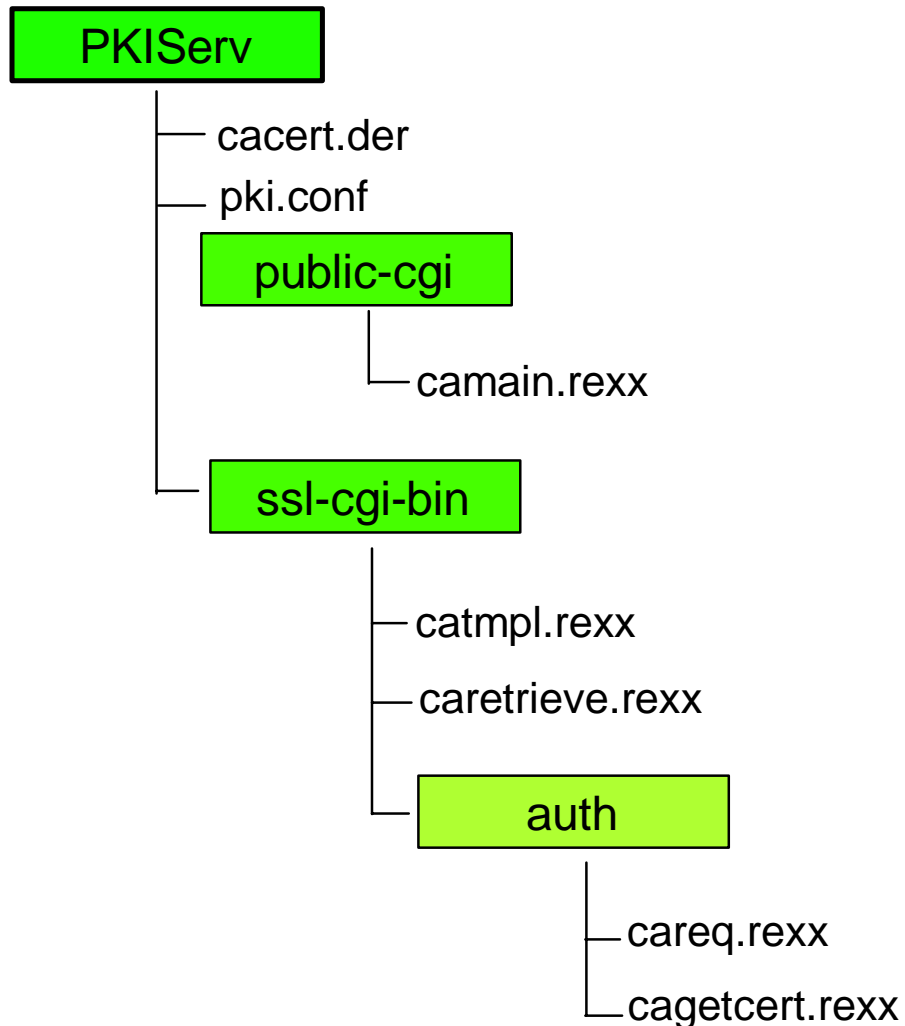
The configuration File (**PKI.CONF**) requires at least changes to the CONTENT section, for example

<APPL>	
%%UserId%%	==> User ID of the User requesting cert
</APPL>	
<CONSTANT>	
%%Org=IBM%%	==> Hardcoded Value for Organization
%%OrgUnit=ITSO%%	==> Hardcoded Value for Organizational Unit
%%KeyUsage=handshake%%	==> Hardcoded Value = Indicates SSL Usage
%%NotAfter=365%%	==> Hardcoded Value = Validity Period 365 Days
%%Country=US%%	==> Hardcoded Value for Country
%%SignWith=SAF:CERTAUTH/ITSO CA%%	==> Hardcoded Value for signing CA cert
</CONSTANT>	
%%CommonName=%%	==> CommonName provided by End User

# RACF SPE - Flow Chart



# RACF SPE - Directory Structure provided



# RACF SPE - Web based Interface



Web Based Certificate Generation Application - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print

Address <http://wtsc57.itso.ibm.com/PKIServ/public-cgi/camain.rexx> Go Links

Y! Ticker: Quotes Charts News Rsrch Add To My Portfolios Markets Y! Bookmarks Sign Out

## PKISERV Certificate Generation Application

[Install our CA certificate into your browser](#)

Select the certificate template to use

email: [graaff@us.ibm.com](mailto:graaff@us.ibm.com)

Technology ▪ Connections ▪ Results

# RACF SPE - Web based Interface



Web Based SAF Certificate Generation Application Pg 2 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print

Address <https://wtsc57.lso.ibm.com/PKIServ/ssl-cgi-bin/catmpl.rexx?Template=1+Year+SAF+Browser+Certificate> Go Links

Y! Ticker: Quotes Charts News Rsrch Add To My Portfolios Markets Y! Bookmarks Sign Out

## SAF Browser Certificate 1 Year (Auto Approved)

Choose one of the following:

- Request a New Certificate

Enter values for the following field(s)

Label assigned to certificate being requested

Organization

Organizational Unit

Select the following key information

Cryptographic Service Provider

Use Smart Card for private key protection?

- Pick Up a Previously Issued Certificate

Done Internet

# RACF SPE - Web based Interface

A screenshot of a Windows-style dialog box titled "Enter Network Password". It contains a key icon and the text "Please type your user name and password." Below this, it shows "Site: wtsc57.itso.ibm.com" and "Realm: PKISPE2". There are two input fields: "User Name" and "Password". At the bottom, there is a checkbox labeled "Save this password in your password list" which is unchecked, and two buttons: "OK" and "Cancel".

**You need to be authorized to generate a digital certificate !**

# RACF SPE - Web based Interface



A screenshot of a Microsoft Internet Explorer browser window. The title bar reads "Web Based Certificate Generation Success - Microsoft Internet Explorer". The address bar shows the URL "https://wts57.tso.ibm.com/PKIServ/ssl-cgi-bin/auth/careq.rexx". The browser's menu bar includes "File", "Edit", "View", "Favorites", "Tools", and "Help". The toolbar contains "Back", "Forward", "Home", "Search", "Favorites", "History", "Print", and "Stop". The main content area displays the heading "Request Submitted Successfully" in a large, bold, black font. Below the heading, a paragraph of text reads: "Here's your transaction ID. You will need it to retrieve your certificate. Press 'Continue' to retrieve the certificate." A text input field contains the transaction ID: "2QbH2cHBxsbXgaSTQMnFQMOFmaOJhomDgaOF". Below the input field is a "Continue" button. At the bottom of the page, the email address "email: graaff@us.ibm.com" is displayed. The browser's status bar at the bottom shows "Done" and "Internet".



# RACF SPE - Web based Interface



Web Based SAF Certificate Generation Application Pg 3 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print

Address <http://wts57.itso.ibm.com/PKIServ/ssl-cgi-bin/caretrieve.rexx?Template=1+Year+SAF+Browser+Certificate&TransactionId=2QbH2cHBxsbXgaSTQMnFQMOFmaOJhomDgaOF> Go Links

Y! Ticker: Quotes Charts News Rsrch Add To My Portfolios Markets Y! Bookmarks Sign Out

## Retrieve Your 1 Year SAF Browser Certificate

Enter the assigned transaction ID

Retrieve and Install Certificate

**To check that your certificate installed properly, follow the, procedure below:**

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

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

Home page

email: [graaff@us.ibm.com](mailto:graaff@us.ibm.com)

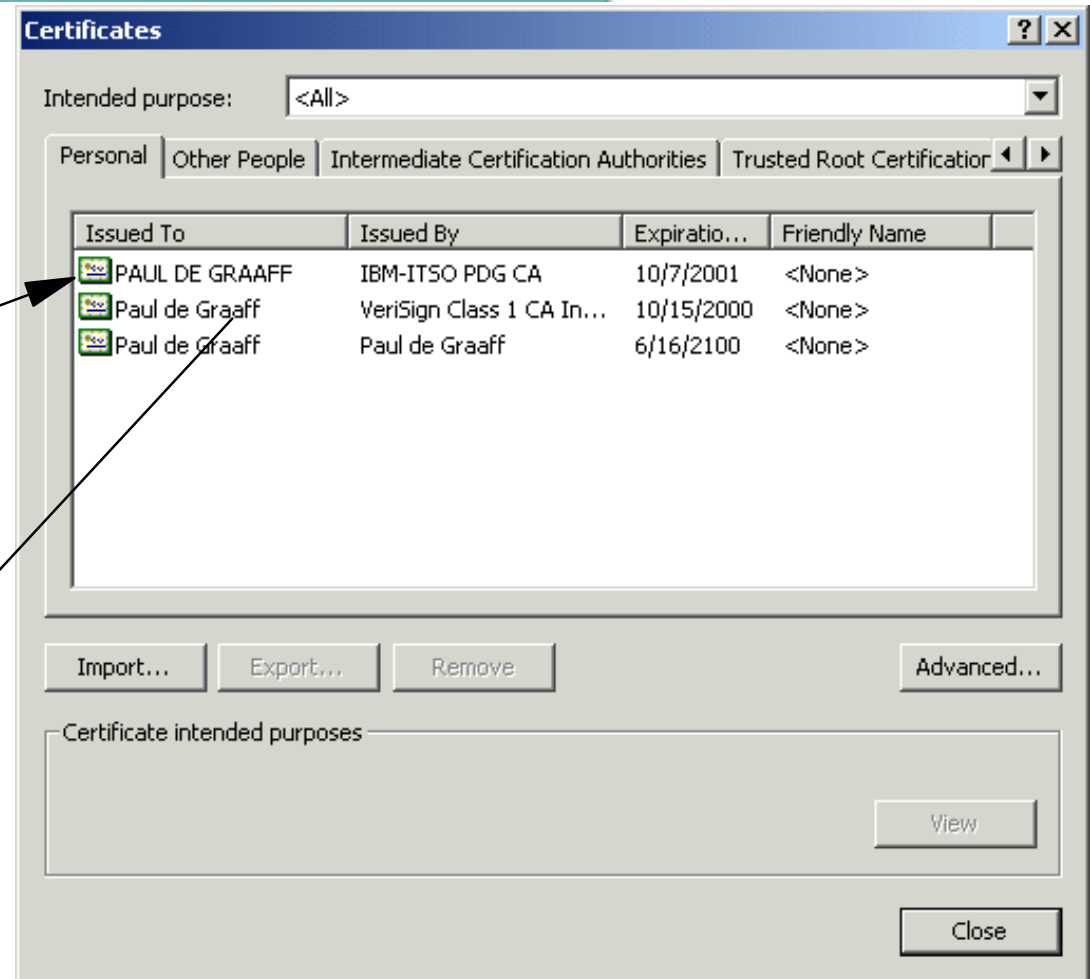
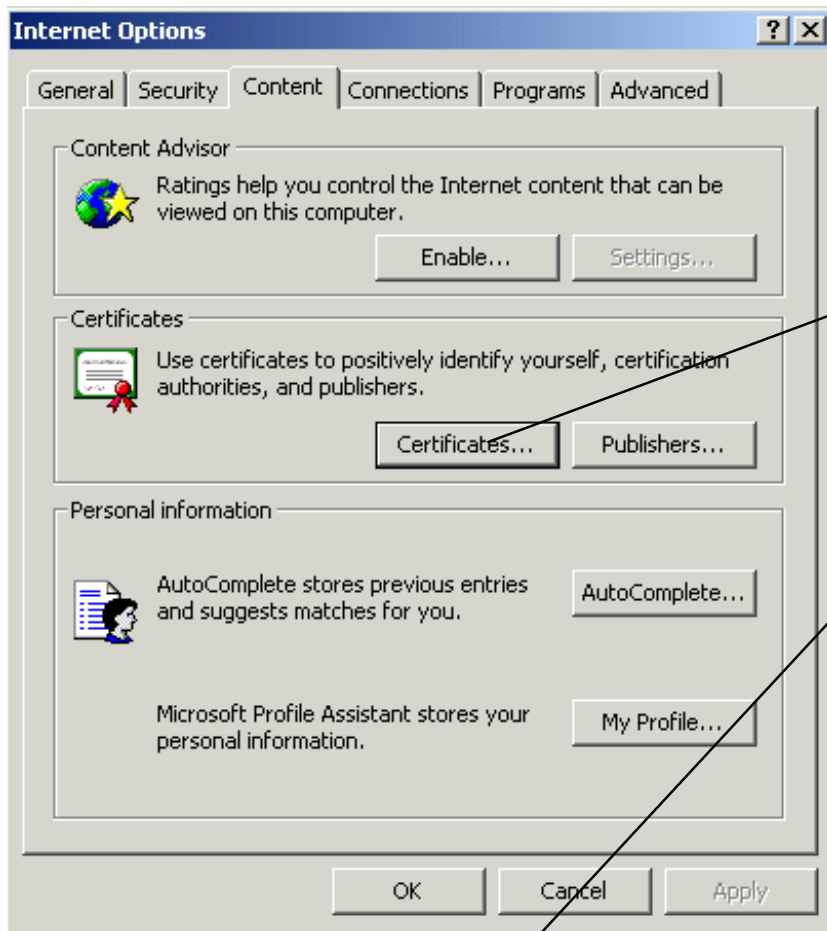
Done Internet

# RACF SPE - Web based Interface



A screenshot of a Microsoft Internet Explorer browser window. The title bar reads "MSIE Certificate Install - Microsoft Internet Explorer". The address bar shows a URL: "rexx?Template=1+Year+SAF+Browser+Certificate&amp;TransactionId=2QbH2cHBxsbXga5TQMnFQMOfmaNA44Wio0BA". The main content area displays the heading "Internet Explorer Certificate Install" and the instruction "Click 'Install Certificate' to store your new, certificate into your browser". Below this are two buttons: "Install Certificate" and "Home page". A black arrow points from the "Install Certificate" button to a small dialog box titled "VBScript: Certificate Installation". The dialog box contains an information icon and the text "Your new certificate installed successfully." with an "OK" button. The status bar at the bottom shows "Done" and "Internet".

# RACF SPE - Web based Interface



Common Name retrieved from RACF Name Field

# RACF - RACDCERT LIST Output



Label: **Paul IE Certificate**

Certificate ID: 2QbH2cHBxsbXgaSTQMnFQMOfmaOJhomDgaOF

Status: TRUST

Start Date: 2000/10/07 00:00:00

End Date: 2001/10/07 23:59:59

Serial Number:

>10<

Issuer's Name:

>CN=IBM-ITSO PDG CA.OU=ITSO.O=IBM.C=US<

Subject's Name:

>**CN=PAUL DE GRAAFF**.OU=ITSO.O=IBM.C=US<

Key Usage: HANDSHAKE

Private Key Type: None

Ring Associations:

\*\*\* No rings associated \*\*\*

# PKISERV - R\_PKIServ Authorizations



To be able to generate a digital certificate, a User ID will need to be RACF SPECIAL or have access to:

**IRR.RPKISERV.<function>** in the **FACILITY** class

**READ** - access to subsequent RACDCERT functions is based on the client's User ID

**UPDATE** - access to subsequent RACDCERT functions is based on the daemon User ID (not used by Websphere)

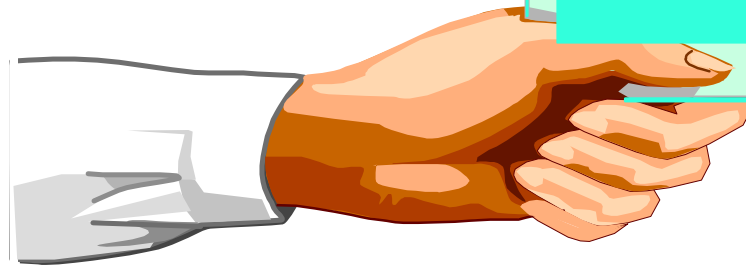
**CONTROL** - no subsequent checks are being made to RACDCERT functions

Functions are GENCERT and EXPORT !

# Questions ???



Questions  
or Time for  
Coffee ?



Technology ▪ Connections ▪ Results