


Customizing z/OS® PKI services Certificates templates file



@business on demand software

© 2008 IBM Corporation

z/OS PKI Services allows the use of z/OS to establish a public key infrastructure and serve as a certificate authority. Allowing for the issuing and administering of digital certificates in accordance with your organization's policies for both internal and external users. end-users can use PKI Services to request and obtain certificates through their own Web browsers, while authorized PKI administrators approve, modify, or reject these requests through their own Web browsers. The plan is to provide additional z/OS PKI customization education modules that will give an in depth look into customizing the Web applications provided with z/OS PKI Services.

Objectives

- Customizing end-user z/OS PKI Services Web pages
- Overview of the certificate templates file, pkiserv.tpl
- Identifying template sections and subsections
- Examples of simple modifications

The objective of this presentation is to demonstrate the customization of z/OS PKI Services Web pages. This module will begin with an overview of the certificate templates file and then focus on those parts of the template file that are customizable.

At the end of this presentation, you will have the ability to make updates to the template file customizing the end-user Web pages by building on the examples shown in this presentation.

Customizing PKI Web pages

- External look and behavior is dictated by the contents of the template file (pkiserv.tmpl)
- User display is the result of the CGI modules and content in the template file.

Once z/OS PKI Services has been installed properly, you may be interested in customizing the end-user Web pages and the PKI administrator Web pages. As it is shipped, the Web pages only exploit the services provided by z/OS PKI Services and are very basic in design. Not only can an organization personalize the Web pages they can also limit or expand functionality of z/OS PKI Services based on their policies for both internal and external users.

The external look and behavior of the z/OS PKI Services is dictated by the contents of the certificate templates file, pkiserv.tmpl, for the Web end-user and the PKI administrator.

The user interface display is the result of the CGI modules interacting with the certificate templates file.

The rest of presentation will examine in detail the certificate templates file and show how changes to the file can alter the Web pages.

Understanding pkiserv.tpl

- Default location of template file
 - ▶ /etc/pkiserv/pkiserv.tpl
- Contains certificate templates
 - ▶ Defines fields for a certificate request
- Contains real HTML tags and z/OS PKI tags
- Template file is broken into three sections
 - ▶ APPLICATION
 - ▶ TEMPLATE
 - ▶ INSERT
- pkiserv.tpl begins with a prolog.
- Any line with a # in column 1 is a comment
- Changes in the certificate templates file will be picked up dynamically

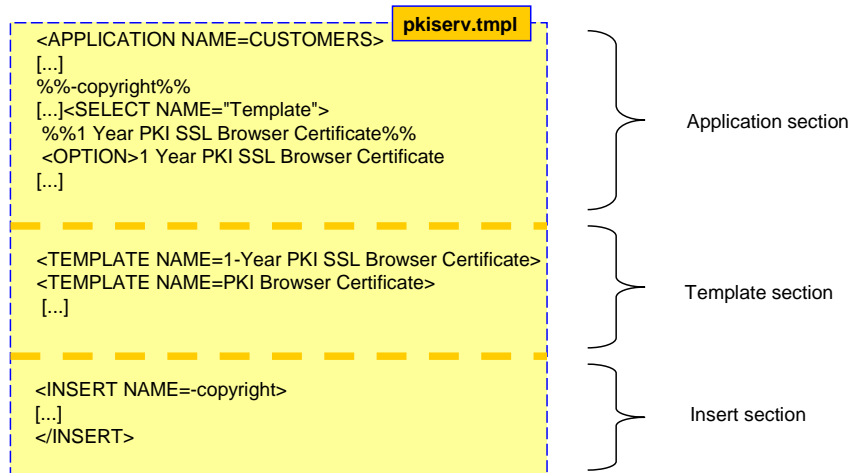
Before beginning to customize the Web pages, a understanding of the `pkiserv.tpl` certificate templates file is required. This file contains certificate templates, which define the fields that comprise a specific certificate request.

The certificate templates file is a combination of real HTML tags and z/OS PKI tags which are interpreted by the CGI modules. The HTML can also contain JavaScript for verifying user input fields. The certificate templates file is broken into: APPLICATION, TEMPLATE, and INSERT sections.

The `pkiserv.tpl` certificate templates file begins with a prolog. This is a section of comments that explains the main sections and subsections of the file. Any line with a # in column 1 is considered a comment and will be ignored when being parsed.

Any changes made to the certificate templates file will be dynamically picked up.

Certificate template file – Basic layout



This illustration demonstrates the basic layout of the certificate templates file. The templates file typically has two Application Sections, one for the end-user and one for the administrator. This slide shows the application section for the end-user. In a typical installation there will be multiple template sections and insert sections. Not included in this illustration is the prolog section which would be in the beginning of the file.

You will see more on the Application section, template section, and the Insert section.

APPLICATION section

- Identify the application domain supported by PKI Services
- Default pkiserv.tmpl ships with
 - ▶ PKISERV – for PKI administrator
 - ▶ CUSTOMERS – for users

The APPLICATION section identifies the application domain supported by the PKI Services. The default certificate templates file ships with two application sections, PKISERV for the PKI Administrator and CUSTOMERS for end-users. The application section is used to construct the main page for the end-user or administrator. It provides options for the end-user to pick a template to use for the certificate request or it provides options for the administrator to pick a CA domain to administer.

TEMPLATE section

- Contains the HTML to produce requests forms and retrieve the signed certificates
- Defines permissible fields in the certificate
- Example:

```
<TEMPLATE NAME=1-Year PKI SSL Browser Certificate>
<TEMPLATE NAME=PKI Browser Certificate>
<NICKNAME=1YBSSL>
[ ... ]
</TEMPLATE>
```

- Can have more than one alias use additional <TEMPLATE NAME=*alias*> per line
- NICKNAME max is 8 characters
- SAF Certificates do not contain nicknames

The TEMPLATE sections are the certificate templates that contain the HTML to produce certificate request forms and to retrieve the signed certificates. It defines fields for the user input and fields that are pre-determined values.

TEMPLATE sections define the fields that comprise a specific certificate request. They define the certificate templates referenced in the APPLICATION section.

Each template section begins with one or more template names. See the example to understand the basic format of how the template section begins.

The true name of the certificate template is the actual complete name. In the above example, 1-Year PKI SSL Browser Certificate is the true name of the certificate. However, you can refer to a single template by more than one name by using an alias. The template name in the third line, PKI Browser Certificate, is an alias. An alias is used to differentiate browser from server certificates. The NICKNAME is used to prepare for the renewal of the certificate later. If it is absent at the time of your request the certificate cannot be renewed.

Remember that a NICKNAME can have a maximum of eight characters. And that SAF templates do not contain nicknames.

TEMPLATE section

Names, aliases, and nicknames of certificate templates		
True name	Alias	Nickname
1-Year PKI SSL Browser Certificate	PKI Browser Certificate	1YBSSL
1-Year PKI S/MIME Browser Certificate	PKI Browser Certificate	1YBSM
2-Year PKI Browser Certificate For Authenticating To z/OS	PKI Browser Certificate	2YBZOS
2-Year PKI Authenticode - Code Signing Certificate	PKI Server Certificate	2YIACS
2-Year PKI Windows Logon Certificate	PKI Browser Certificate	2YBWL
5-Year PKI SSL Server Certificate	PKI Server Certificate	5YSSSL
5-Year PKI IPSEC Server (Firewall) Certificate	PKI Server Certificate	5YSIPS
5-Year PKI Intermediate CA Certificate	PKI Server Certificate	5YSCA
5-Year SCEP Certificate - Preregistration	--	5YSCEPP
<i>n</i> -Year PKI Certificate for Extensions Demonstration	PKI Browser Certificate	SAMPLB
1-Year SAF Browser Certificate	SAF Browser Certificate	--
1-Year SAF Server Certificate	SAF Server Certificate	--

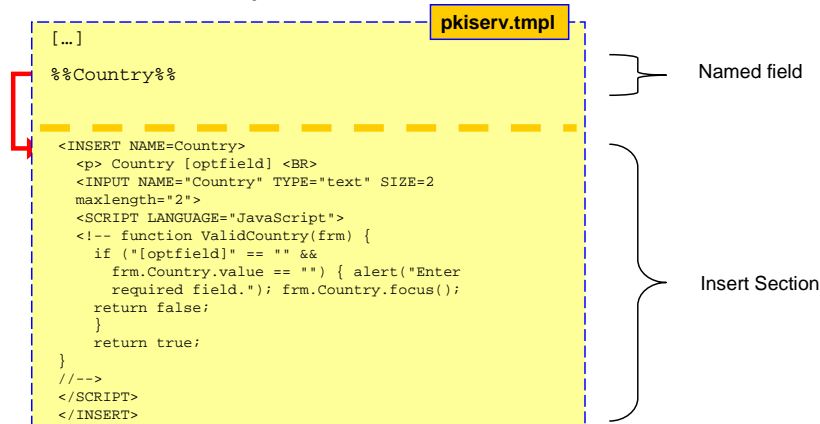
This table shows the true name, alias, and nickname for each certificate template.

It should be noted that SAF certificates are generated by RACF®, and not by PKI Services. They cannot be managed by PKI Services, that means you cannot query, renew, revoke, and other PKI Services' functions.

The SCEP template is not to request a certificate, but to register a client so that it can request a certificate later.

INSERT section

- Any named field must correspond to an INSERT section
- Contains no subsections
- Here is an example that defines a certificate field:



The insert section contains the HTML code to display user input fields as a text box, a drop down box, and other HTML forms. It can be customized to validate the user input field through embedded JavaScript.

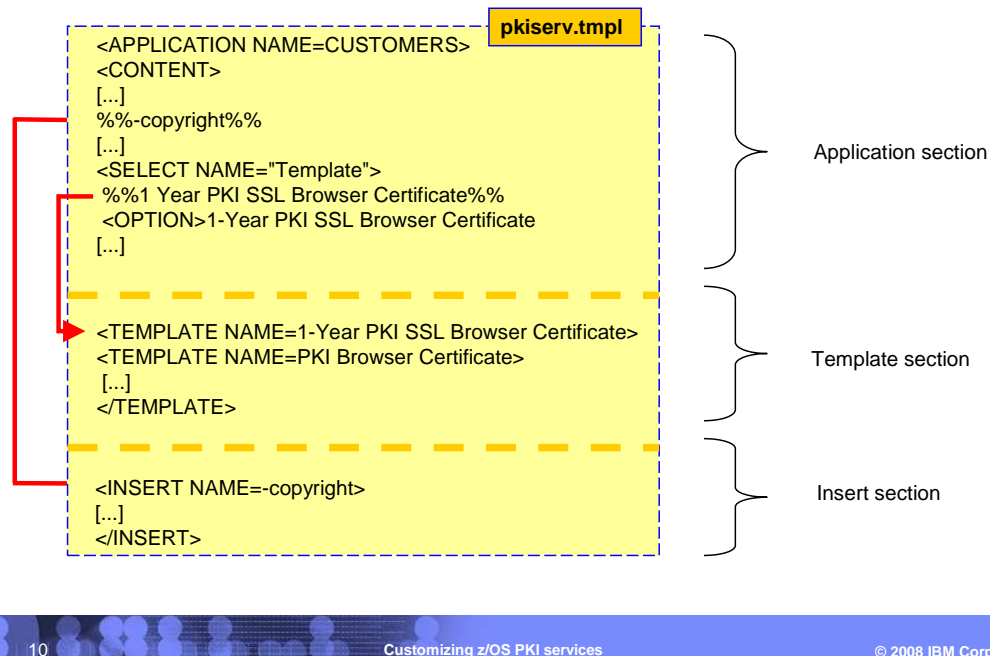
A named field inserts common HTML code on a Web page, each named field corresponds to an INSERT section or TEMPLATE section. An INSERT section is a method of specifying common HTML code, such as a common input field, a page header or footer, that must be inserted into a Web page.

The named field format is percent sign, percent sign, field name, percent sign, percent sign. For example, a named field such as `%%Country%%` is a reference to the Country section. It will insert the country user input field on the page.

A named field such as `%%1-Year PKI SSL Browser Certificate%%` is a reference to the 1-year PKI SSL Browser certificate template.

Note: the named fields are case-sensitive.

Certificate template file – Basic function



In this example, the application section CUSTOMERS will display the initial first page of the users' Web page. The `-copyright` named field will branch down to the insert named `-copyright` and insert the HTML code found in that section in your Web page. The options in the HTML select statement "Template" will link to a dynamically generated Web page based off the code found in the template section. In the example above option "1-Year PKI SSL Browser Certificate" will link to a dynamic page generated by the template section "1-Year PKI SSL Browser Certificate."

Both the application section and the template sections consists of subsections. This presentation will focus on the content subsection since it is most customizable.

User APPLICATION section subsections

- CUSTOMERS
 - ▶ CONTENT
 - ▶ RECONTENT
 - ▶ RESUCCESSCONTENT
 - ▶ REFAILURECONTENT

```

<APPLICATION NAME=CUSTOMERS>
<APPLICATION NAME=CUSTOMERS>
<CONTENT>
<HTML><HEAD>
<TITLE> Customers Certificate Generation
Application </TITLE>
%%-copyright%%
</HEAD>
<BODY>
<H1>PKI Services Certificate Generation
Application</H1>
[...]
</CONTENT>
<APPLICATION NAME=CUSTOMERS>
[...]
</CONTENT>
<RECONTENT>
[...]
</RECONTENT>
<RESUCCESSCONTENT>
%%-renewrevokeok%%
</RESUCCESSCONTENT>
<REFAILURECONTENT>
%%-renewrevokebad%%
</REFAILURECONTENT>

```

The CUSTOMERS APPLICATION section can contain these subsections:

The CONTENT subsection contains the HTML to display the PKI Services home page to the user who is requesting and retrieving certificates. This subsection should contain one or more named fields identifying certificate templates to use for requesting or managing certificates through this application.

The RECONTENT subsection, the RE in RECONTENT stands for RENEW/REVOKE. This subsection contains the HTML to display information about the certificate so you can confirm that this is the correct certificate to renew or revoke.

The RESUCCESSCONTENT and REFAILURECONTENT subsections contain the HTML to display a Web page to the user when the renewal or revocation request is successful or unsuccessful.

Administrator APPLICATION section subsections

- PKISERV (Administrator)
 - ▶ CONTENT
 - ▶ ADMINHEADER
 - ▶ ADMINFOOTER
 - ▶ *ADMINSCOPE - optional*

```
<APPLICATION_NAME=PKISERV>
</CONTENT>
<ADMINHEADER>
<HTML><HEAD>
  </CONTENT>
  [...]
  <ADMINSCOPE>
  %%SelectCADomain%%
  </ADMINSCOPE>
</APPLICATION>
<ADMINFOOTER>
<p> %%-pagefooter%%
</BODY>
</HTML>
</ADMINFOOTER>
```

In addition to the CONTENT section, the PKISERV application section also contains, the ADMINHEADER and ADMINFOOTER subsections contain the general installation-specific HTML content for the header and footer of all administration Web pages.

And the ADMINSCOPE is an optional subsection allowing the administrator to choose a different CA domain.

Example of updating the application content subsection

Application - Content

```
<APPLICATION NAME=CUSTOMERS>
<CONTENT>
<HTML><HEAD>
<TITLE> Customers Certificate Generation Application </TITLE>
%%-copyright%%
</HEAD>
<BODY>
<H1>PKI Services Certificate Generation Application</H1>
<p>
<A HREF="/PKIServ/cacerts/cacert.der">
Install the CA certificate to enable SSL sessions for PKI Services
</A>
[...]
</APPLICATION>
```

This is a sample of the Customer's application section. Notice the HTML tags within the content section? These tags will dictate the layout of the Customers page.

Example of customers' Web page

The screenshot shows a web browser window with the URL <http://wbs1051.psk.ibm.com/Customers/public-eg/owaam.exe?>. The page title is "PKI Services Certificate Generation Application". Below the title is a link: [Install the CA certificate to enable SSL sessions for PKI Services](#). The main heading is "Choose one of the following:" followed by three bullet points:

- **Request a new certificate using a model**
Select the certificate template to use as a model: 1-Year PKI SSL Browser Certificate [v]
- **Pick up a previously requested certificate**
Enter the assigned transaction ID: [text box]
Select the certificate return type: PKI Browser Certificate [v]
- **Renew or revoke a previously issued browser certificate**

Below these options is a link: [Go to Administration Page](#). At the bottom of the page is an email address: [email: webmaster@voss-company.com](mailto:webmaster@voss-company.com).

The application section Customers just discussed previously will generate this Web page.

Changing background color

Application - Content

```
<APPLICATION NAME=CUSTOMERS>
<CONTENT>
<HTML><HEAD>
<TITLE> Customers Certificate Generation Application
  </TITLE>
%%-copyright%%
</HEAD>
→<BODY bgcolor="orange">
<H1>PKI Services Certificate Generation Application</H1>
<p>
<A HREF="/PKIServ/cacerts/cacert.der">
Install the CA certificate to enable SSL sessions for PKI
  Services </A>
[... ]
</APPLICATION>
```

This example shows a simple html code update. The red arrow points to the the change, the background color has been changed from default to orange.

Removing content

Application - Content

```
[...]  
#<li><h3>Administrators click here</h3>  
# The following action will force userid/pw authentication for  
# administrators  
#<FORM name=admform METHOD=GET  
#ACTION="/ application /ssl-cgi/auth/admmain.rexx">  
# The following action will force client certificate authentication  
# for  
# administrators  
#<FORM name=admform METHOD=GET  
# ACTION="/ application /clientauth-cgi/auth/admmain.rexx">  
#<p>  
#INPUT TYPE="submit" VALUE="Go to Administration Page">  
#</FORM>  
[...]
```

You can effectively remove lines without actually deleting them. Recall that comments are ignored. This comes in handy if you are debugging and do not want to actually delete code. If you noticed in the default customer Web page that there was a button for administrators at the bottom. Since this is the customer page, the “Administrator Click Here” bullet and the button are commented out.

The updated customers' Web page

PKI Services Certificate Generation Application

[Install the CA certificate to enable SSL sessions for PKI Services](#)

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
 -
- Pick up a previously requested certificate
 - Enter the assigned transaction ID:
 - Select the certificate return type: PKI Browser Certificate
 -
- Renew or revoke a previously issued browser certificate
 -

[email webmaster@your-company.com](mailto:webmaster@your-company.com)

With the updates this customer page no longer shows the administrator option and the background color is now orange. Similarly, you can customize the page to fit your company Website design by manipulating the HTML and PKI Tags to add a company logo, company colors, and other graphics.

TEMPLATE section

- Contains these subsections
 - ▶ CONTENT
 - ▶ APPL
 - ▶ CONSTANT
 - ▶ ADMINAPPROVE
 - ▶ SUCCESSCONTENT
 - ▶ FAILURECONTENT
 - ▶ RETRIEVECONTENT
 - ▶ RETURNCERT
 - ▶ PREREGISTER

```

<CONTENT>
<HTML><HEAD>
<TITLE> Web Based PKIX Certificate
Generation Application Pg 2
</TITLE> %%-copyright%%
%%-AdditionalHead[browsertype]%%

<APPL>
%%UserId%%
%%HostIdMap=@host-name%%
</APPL>
CertificateGeneration Application

<PREREGISTER>
AuthenticatedClient=AutoApprove
SemiauthenticatedClient=AdminApprove
UnauthenticatedClient=Reject
SubsequentRequest=AutoApprove
RenewalRequest=AutoApprove
</PREREGISTER>

```

The TEMPLATE section can have these subsections: CONTENT, CONSTANT, ADMINAPPROVE, SUCCESSCONTENT, FAILURECONTENT, RETRIEVECONTENT, RETURNCERT, and APPL.

The CONTENT subsection contains the HTML to display a Web page to the user requesting a certificate of a specific type. This subsection will be examined further.

The APPL subsection identifies certificate fields for which the application itself should provide values. This subsection should contain only named fields, one per line. The only supported named fields allowed in this section are **Userld** and **HostldMap**

The CONSTANT subsection identifies certificate fields that have a constant or hard coded value for everyone.

The ADMINAPPROVE subsection is an optional subsection that contains the named fields that the administrator can modify when approving certificate requests

The SUCCESSCONTENT subsection contains the HTML to display to the user a Web page saying that the certificate request was submitted successfully.

The FAILURECONTENT subsection contains the HTML to display to the user a Web page saying that the certificate request was not submitted successfully.

The RETRIEVECONTENT subsection contains the HTML to display to the user a Web page to enable certificate retrieval.

The RETURNCERT subsection contains the HTML to display to the user a Web page upon successful certificate retrieval.

The PREGISTRATION subsection is an optional subsection that indicates the creation of a preregistration record and contains the Simple Certificate Enrollment Protocol (SCEP) rules for approval of a SCEP request. Here's an example of a preregistration subsection.

```

<PREREGISTER> AuthenticatedClient=AutoApprove SemiauthenticatedClient=AdminApprove
UnauthenticatedClient=Reject SubsequentRequest=AutoApprove RenewalRequest=AutoApprove
</PREREGISTER>

```

CONTENT subsection

- Contains HTML for displaying certificate request

The CONTENT subsection contains the HTML to display a Web page to the user who requests a certificate of a specific type. Field names on the certificate request, such as a text box where you enter a value for Common Name, match the names of INSERT sections.

CONTENT subsection

Template - Content

```

<TEMPLATE NAME=1 Year PKI SSL Browser Certificate>
<TEMPLATE NAME=PKI Browser Certificate>
<NICKNAME=1YBSSL>
<CONTENT>
<HTML><HEAD>
<TITLE> Web Based PKIX Certificate Generation Application Pg 2</TITLE>
%%-copyright%%
%%-AdditionalHead[browsertype]%%
</HEAD> <BODY>
<H1>1 Year SSL Browser Certificate</H1> <p>
<H2>Choose one of the following:</H2> <p> <ul><h3><i>Request a New Certificate</i></h3> <FORM NAME="CertReq"
METHOD=POST ACTION="/PKIServ/ssl-cgi-bin/careq.rexx" onSubmit="if(ValidateEntry()) return false; else return true;"> <INPUT
NAME="Template" TYPE="hidden" VALUE="[tmplname]"> <p> Enter values for the following field(s)
<SCRIPT LANGUAGE="JavaScript">
<!--
function ValidateEntry(){
[.]
</SCRIPT>
%%Requestor (optional)%%
%%Email (optional)%%
%%CommonName%%
%%NotifyEmail (optional)%%
%%PassPhrase%%
%%PublicKey[browsertype]%%
[.]
<p>%%-pagefooter%%
</BODY>
</HTML>
</CONTENT>

```

This is an example of a certificate template CONTENT subsection. Note that in this example a runtime logic is introduced in the template using JavaScript. Note also the named fields referring to the contents of the certificate fields.

1-Year PKI SSL browser certificate Web page

1-Year PKI SSL Browser Certificate

Choose one of the following:

- **Request a New Certificate**
Enter values for the following field(s)
Your name for tracking this request (optional)

Email address for notification purposes (optional)

Pass phrase for securing this request. You will need to supply this value when retrieving your certificate

Reenter your pass phrase to confirm

Email address for distinguished name MAIL= attribute (optional)

Common Name

Select a key size: 2048 (High Grade) ▾
- **Pick Up a Previously Issued Certificate**

[email: webmaster@your-company.com](mailto:webmaster@your-company.com)

This is the Web page that is dynamically generated based of the template section code in the previous slide.

CONSTANT subsection

- Certificate fields that have hard-coded values
- Only contains one named field per line
- Example:

```
[...]
</CONTENT>
<CONSTANT>
%%NotBefore=0%%
%%NotAfter=365%%
%%KeyUsage=handshake%%
%%OrgUnit=Class 1 Internet Certificate CA%%
%%Org=The Firm%%
%%SignWith=PKI:%%
</CONSTANT>
[...]
```

Template - Constant

The CONSTANT subsection identifies certificate fields that have a constant, hard-coded, value for everyone. This subsection should contain only named fields, one per line. This is shown in the example.

CONSTANT subsection

- Critical
 - ▶ Mark critical certificate extensions in the issued certificates
 - ▶ List of acceptable values for Critical
 - BasicConstraints
 - KeyUsage
 - ExtKeyUsage
 - SubjectAltName, AltEmail, AltIPAddr, AltDomain, AltURI
 - HostIdMappings, HostIDMap
 - CertificatePolicies, CertPolicies
 - ▶ Example: %%Critical=ExtKeyUsage%%

In the CONSTANT subsection, certain certificate extensions can be defined as Critical. Critical identifies a certificate extension that is to be marked critical in the issued certificates. This name-value pair may be repeated for each extension to be marked critical. Here is the list of acceptable values for **Critical**:

BasicConstraints, which is always marked critical,
KeyUsage, which is always marked critical,
ExtKeyUsage, **SubjectAltName**, **AltEmail**, **AltIPAddr**, **AltDomain**, **AltURI**,
HostIdMappings, **HostIdMap**, **CertificatePolicies**, and **CertPolicies**

Making the validity dates a user input field

Template - Content

```
[...]
%%Requestor (optional)%%
%%NotifyEmail (optional)%%
%%PassPhrase%%
%%Mail (optional)%%
%%CommonName%%
%%PublicKey browsertype %%
%%NotBefore%%
%%NotAfter%%
[...]
</CONTENT>
<CONSTANT>
%%NotBefore=0%%
%%NotAfter=365%%
%%KeyUsage=handshake%%
%%OrgUnit=Class 1 Internet Certificate CA%%
%%Org=The Firm%%
%%SignWith=PKI:%%
</CONSTANT>
[...]
```

This example shows how to make the validity dates a user input field. First, the not before and not after named fields has to be deleted from the constant section. And then move them to your input area in the content section.

To make a user input field optional just add “(optional)” to named field.

Making the validity dates a user input field

Validity Date

1-Year PKI SSL Browser Certificate

Choose one of the following:

- Request a New Certificate**
Enter values for the following field(s)
Your name for tracking this request (optional)
Email address for notification purposes (optional)
Pass phrase for securing this request. You will need to supply this value when retrieving your certificate.
Reenter your pass phrase to confirm
Email address for distinguished name MAIL= attribute (optional)
Common Name
Select a key size: 2048 (High Grade)
Number of days after today before the certificate becomes current (optional)
Length of time that the certificate is current (optional)
1 Year
- Pick Up a Previously Issued Certificate**
Retrieve your certificate

[email: webmaster@your-company.com](mailto:webmaster@your-company.com)

Now the customer Web page displays the validity dates as user input fields. This procedure can be done for any of the certificate information named fields.

ADMINAPPROVE subsection

- Optional subsection containing named fields the administrator can modify when approving a certificate request.
- Administrator can modify:
 - ▶ Fields visible to the user in the request form
 - ▶ Fields not visible to the user but are hard-coded
 - ▶ Fields not visible to the user and administrator can add, for example, HostIdMappings extensions or an empty Org Unit field

This optional subsection contains the named fields that the administrator can modify when approving certificate requests. When an user requests a certificate, the certificate request may contain fields that the user cannot see. When approving a request, the administrator can modify:

Fields that are present and visible to the user in the certificate request, for example, the Common Name.

Fields that are not visible to the user but are hard coded in the CONSTANT subsection in the template such as Organizational unit.

And fields that are not visible to the user and that the administrator can add, such as HostIdMappings extension or an empty Organizational Unit field.

ADMINAPPROVE subsection

- Presence of ADMINAPPROVE section (even if empty) indicated that a request must be approved by the administrator
- Absence of this field indicated request will be auto-approved
- Example:

Template - AdminApprove

```
</CONSTANT>
<ADMINAPPROVE>
%%CommonName (Optional)%%
%%OrgUnit (Optional)%%
%%OrgUnit (Optional)%%
%%Org (Optional)%%
%%NotBefore (optional)%%
%%NotAfter (Optional)%%
%%KeyUsage (Optional)%%
%%HostIdMap (Optional)%%
%%HostIdMap (Optional)%%
%%HostIdMap (Optional)%%
%%HostIdMap (Optional)%%
</ADMINAPPROVE>
```

The presence of the ADMINAPPROVE subsection, even if empty, indicates that an administrator must approve this request. The absence of this section indicates that this certificate type will be auto-approved.

It should be noted that the Label, PublicKey, Requestor, SignWith, and UserId fields are not modifiable and are ignored in the ADMINAPPROVE section.

Making the certificates auto-approved

- Original

Template - AdminApprove

```

<TEMPLATE NAME=1 Year PKI SSL Browser Certificate>
<TEMPLATE NAME=PKI Browser Certificate>
<NICKNAME=1YBSSL>
<CONTENT>
[ ... ]
<CONSTANT>
%%NotBefore=0%%
%%NotAfter=365%%
%%KeyUsage=handshake%%
%%OrgUnit=Class 1 Internet Certificate CA%%
%%Org=The Firm%%
%%SignWith=PKI:%%
</CONSTANT>
<ADMINAPPROVE>
%%CommonName (Optional)%%
%%OrgUnit (Optional)%%
%%OrgUnit (Optional)%%
%%Org (Optional)%
[ ... ]
%%HostIdMap (Optional)%%
</ADMINAPPROVE>
<SUCCESSCONTENT>
[ ... ]

```

You may like the ability to have a certificate request auto-approved, eliminating the administrator's manual work of approving a request thus issuing the certificate as soon as possible. But you would probably only want to do this if you had some automated way of authenticating the end-user up front.

In order to make a certificate type auto-approved, you would remove the ADMINAPPROVE subsection from the certificate template as shown in the next slide.

Making the certificates auto-approved

- Modified

Template - AdminApprove

```
<TEMPLATE NAME=1 Year PKI SSL Browser Certificate>
<TEMPLATE NAME=PKI Browser Certificate> <NICKNAME=1YBSSL>
<CONTENT>
[... ]
</CONSTANT>
#<ADMINAPPROVE>
# %%CommonName (Optional)%%
# %%OrgUnit (Optional)%%
# %%OrgUnit (Optional)%%
# %%Org (Optional)%%
[... ]
# %%HostIdMap (Optional)%%
#</ADMINAPPROVE>
<SUCCESSCONTENT>
```

The highlighted section shows the ADMINAPPROVE subsection is commented out. This will make certificate request for a 1-year PKI SSL Browser Certificate automatically approved.

How to require RACF user authentication

- Authenticate with a RACF User ID and Password before allowing user to request “1 Year PKI SSL Browser Certificate”

- ▶ Original

```
<TEMPLATE NAME=1 Year PKI SSL Browser Certificate>
<TEMPLATE NAME=PKI Browser Certificate>
<NICKNAME=1YBSSL>
<CONTENT>

[...]

<h3><li>Request a New Certificate</h3>
# This ACTION forces userid/pw authentication and
runs the task under
# the client's ID
#<FORM NAME="CertReq" METHOD=POST ACTION=
#"/ application /ssl-cgi-bin/auth/careq.rexx"
onSubmit=
[...]
```

Template - Content

In this example you want to require a person to authenticate himself using his RACF User ID and Password before making a certificate request for a 1 Year PKI SSL Browser Certificate.

How to require RACF user authentication

- Authenticate with a RACF User ID and Password before allowing user to request “1 Year PKI SSL Browser Certificate”

▶ Modified

Template - Content

```
<TEMPLATE NAME=1-Year PKI SSL Browser Certificate>
<TEMPLATE NAME=PKI Browser Certificate> <NICKNAME=1YBSSL>
<CONTENT>

[... ]

<h3><li>Request a New Certificate</h3>
#This ACTION forces userid/pw authentication and runs the task
#under the client's ID
<FORM NAME="CertReq" METHOD=POST ACTION=
"/ application /ssl-cgi-bin/auth/careq.rexx" onSubmit=
[... ]
```



In the template section for 1-Year PKI SSL Browser Certificate uncomment the lines pointed to by the red arrows found in the content subsection.

How to require RACF user authentication

The screenshot shows a web browser window with the URL `https://abps1224.pki.ibm.com/Customers/ssl-cgi-bin/casmpk.r.exe?Template=1-Year+PKI+SSL+Browser+Certificate`. The page title is "1-Year PKI SSL Browser Certificate".

Choose one of the following:

- Request a New Certificate**
Enter values for the following field(s)
Your name for tracking this request (optional)
Email address for notification purposes (optional)
Pass phrase for securing this request. You will need to supply this value when retrieving your certificate
Reenter your pass phrase to confirm
Email address for distinguished name MAIL= attribute (optional)
Common Name
test
Select a key size 2048 (High Grade)
- Pick Up a Previously Issued Certificate**

[email: webmaster@your-company.com](mailto:webmaster@your-company.com)

An authentication dialog box is overlaid on the form, titled "Enter username and password for 'AuthenticatedUser' at https://abps1224.pki.ibm.com". It contains fields for "User Name:" and "Password:", a checkbox for "Use Password Manager to remember this password.", and "OK" and "Cancel" buttons.

This small change will require the user to authenticate himself by his RACF ID and Password first before making a request.

Summary

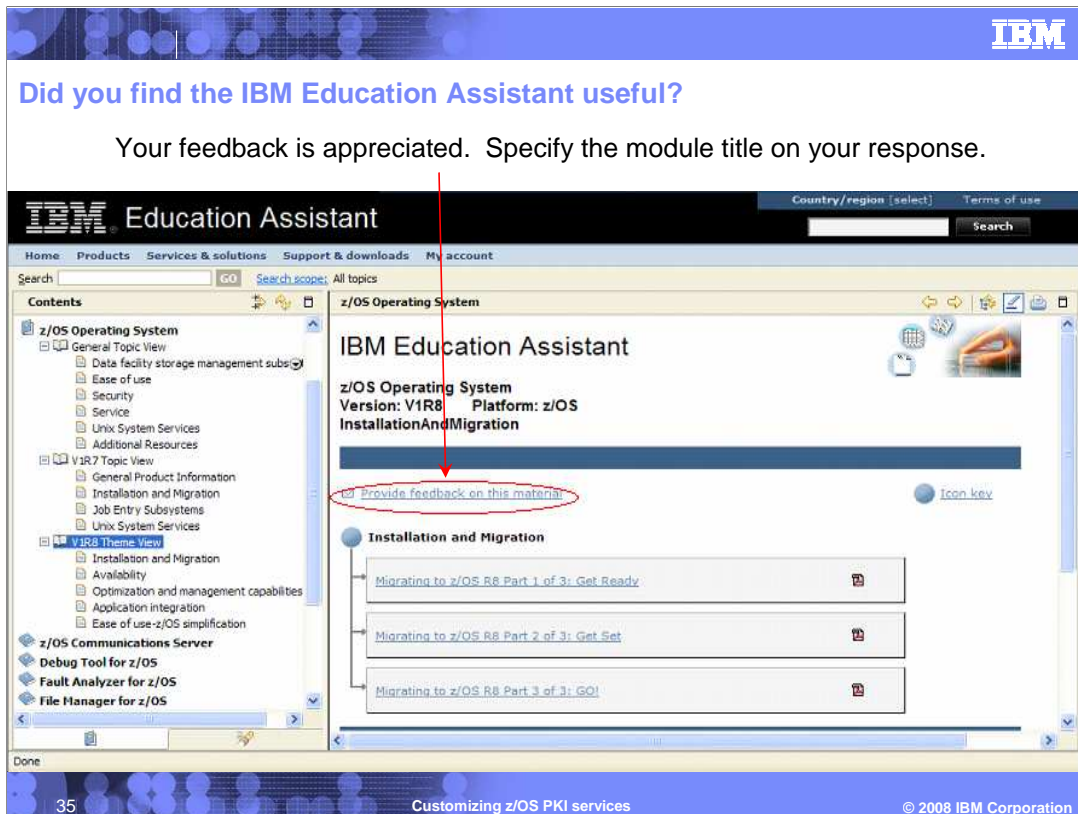
- Familiarizing and defining each element of the certificates template file
 - ▶ Application Section
 - ▶ Template Section
 - ▶ Insert Section
 - ▶ Subsections
 - ▶ Named Fields
- Fully understand Web page customization by doing the examples and adding upon them

In conclusion, by being familiar with the certificates template file and having a better grasp on what each variable, section and subsection defines, you will have the added confidence about modifying the template file. The best way to fully understand Web page customization is to do the simple modifications mentioned and then to use the knowledge gained from this presentation to add upon it.

Resources

- z/OS V1R8.0 Cryptographic Services PKI Services Guide and Reference (SA22-7693-08)
- Implementing PKI Services on z/OS (SG24-6968)
- PKI Services for z/OS
<http://www.ibm.com/servers/eserver/zseries/zos/pki/>

Here is a list of references to learn more about z/OS PKI Services and its customization.



In order to supply you with pertinent and timely information in IBM Education modules, your opinions are important.

Provide your feedback to IBM, answer these questions:

How helpful was this IEA presentation? Give a rating from 1 to 5 where 1 = very helpful and 5 = not at all helpful.

Did this presentation save you a service call to IBM? Yes or No.

If there are any other topics you would like to see covered in IEA, what are they?

Trademarks, copyrights, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM RACF z/OS

Authenticode, Windows, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements or changes in the products or programs described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance 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 or performance improvements equivalent to the ratios stated here.

© Copyright International Business Machines Corporation 2008. All rights reserved.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.