# How to setup SSL with CICS Web Support

## Server and client authentication

## Client Setup with MS Internet Explorer and Mozilla Firefox

Last formatted on: Monday, February 27, 2017

Joerg Schmidbauer
jschmidb@de.ibm.com

Dept. 3252
VSE Development
IBM Lab Böblingen
Schönaicherstr. 220

D-71032 Böblingen
Germany

## Disclaimer

This publication is intended to help VSE system programmers setting up infrastructure for their operating environment. The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM ("vendor") products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk. Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment. Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of other companies:

Firefox and the Firefox Logos are trademarks of the Mozilla Foundation.
Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.
Microsoft, Windows, Windows XP, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

# Contents

## Changes

Jan 31, 2008 – initial version.
Apr 22, 2008 – added PTF info for z/VSE 3.1, added info about client authentication with user ID mapping
Dec 2008 – some textual rework and corrections
May 2009 – info on configuring SSL cipher suites in Mozilla Firefox, see page 24.
November 2010 – added section 6.5
Mar 2012 – updates for z/VSE 4.3 and later, more sections in chapter 9.
January 2016 – added section “Check for latest information” on page 5
Feb 2017 – added new supported cipher suites, removed restriction about RSA keys, and added link to Redbook “Enhanced Networking” in section 10 on page 43

# 1 Introduction

This paper describes the SSL setup for CICS Web Support (CWS) in various scenarios with VSE acting as server. This involves the creation of RSA key pairs and digital certificates on the server and on the client side. For simplification, we do not purchase certificates from official Certificate Authorities (CAs), but create our own set of so called self signed certificates. Self-signed certificates are not signed by an official CA and therefore work only in a closed test environment.

The following software has been used in the test setup.

- z/VSE 4.1.1
- TCP/IP for VSE/ESA 1.5F
- VSE Connector Server as part of z/VSE 4.1.1
- CICS TS 1.1 as part of z/VSE 4.1.1
- Microsoft Windows XP Professional, SP2
- Java 1.6.0_03 from Sun Microsystems
- Keyman/VSE, update from 08/2007
- Microsoft Internet Explorer 6.0
- Mozilla Firefox 2.0.0.11

**Note**: following CICS and TCP/IP PTFs or zaps are necessary for CWS SSL:

- UK20279 / APAR PK29184 (CICS, same PTF for z/VSE 3.1 and z/VSE 4.1)
- UK30576 / APAR PK55026 (TCP/IP **1.5E** on z/VSE 4.1)
- UK30575 / APAR PK55026 (TCP/IP **1.5E** on z/VSE 3.1)
- ZP15F216 (TCP/IP **1.5F**)

When using z/VSE 4.3 or higher, the following zaps are required:

- ZP15F492 – fixes a problem with SSL cipher suite 62
- ZP15F498 – fixes a problem with the TCP/IP get certificate info function

# 2 Check for latest information

The information contained in this White Paper is also available in IBM Redbook *Security on IBM z/VSE*, SG24-7691.

http://www.redbooks.ibm.com/abstracts/sg247691.html?Open

Check the publication dates to see which information is newer. Latest technical update of this White Paper is from February 2017.

Setting up CICS Web Support with the IPv6/VSE product from Barnard Software, Inc. is described in IBM Redbook *Enhanced Networking on IBM z/VSE*, SG24-8091.

http://www.redbooks.ibm.com/abstracts/sg248091.html?Open

# 3 Generating the server key and certificates

The easiest way to generate all necessary keys and certificates for the VSE server side is by using the Keyman/VSE utility which is provided by IBM without warranty for free download from

http://www.ibm.com/servers/eserver/zseries/zvse/downloads/

Keyman/VSE is a Java application, which is typically installed on a Personal Computer. It has the following prerequisites.

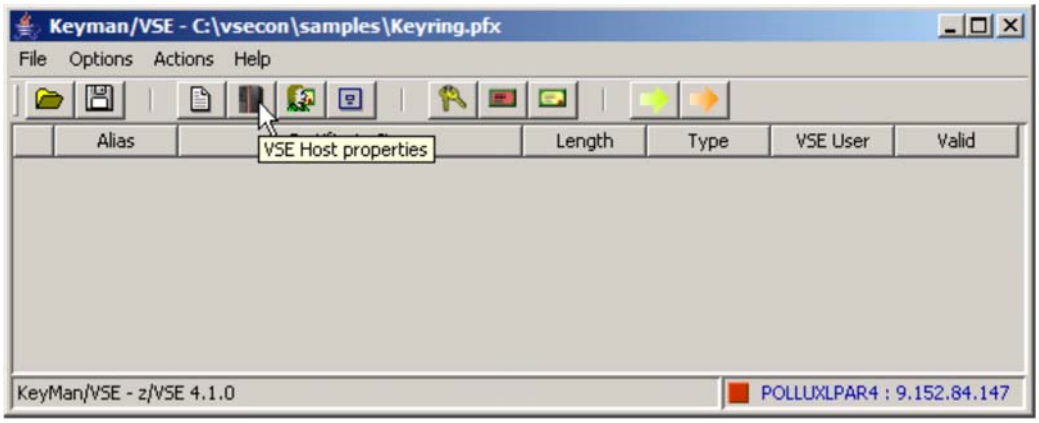
- Java 1.4 or higher on the workstation side
- VSE Connector Client on the workstation side
- TCP/IP for VSE/ESA 1.5E on the VSE side
- VSE Connector Server up and running in non-SSL mode on the VSE side

Although Keyman/VSE provides many functions for manually creating keys and certificates, sign certificate requests, and so on, the easiest way for creating the necessary files on VSE is using the Wizard dialog for creating a self-signed keyring. For details about Keyman/VSE functions refer to the HTML-based help of the Keyman tool.

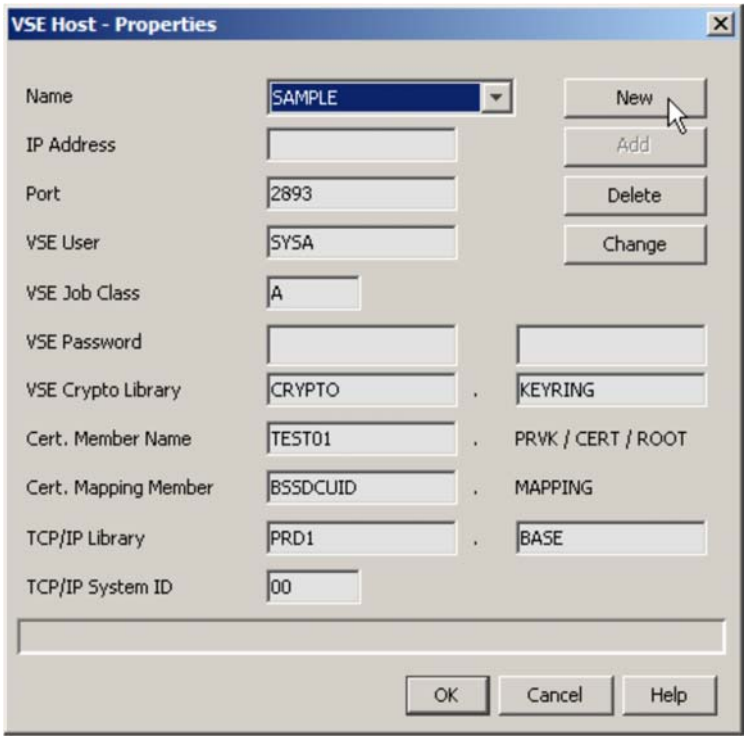
Our first step is to start Keyman/VSE and entering the properties of your VSE system. This information is needed later for sending created keys and certificates to VSE.

## *3.1 Defining the properties of your VSE system*

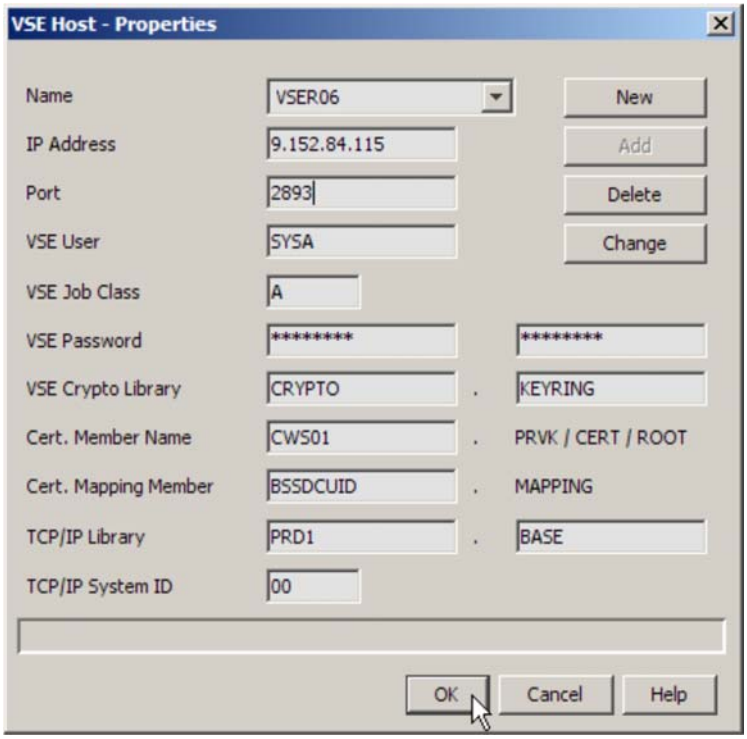
On the main window click on the **VSE host properties** toolbar button.




On the **VSE Host – Properties** dialog box enter the required information for your VSE system. Press the **New** button to create a new VSE host definition.



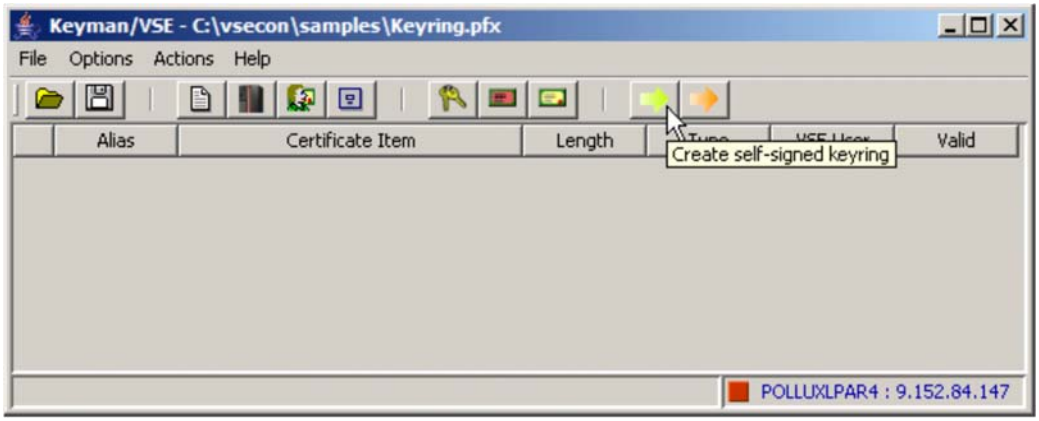

Then enter a unique name for your VSE system, its IP address, the port number of the VSE Connector Server, a VSE user ID together with its password and so on.



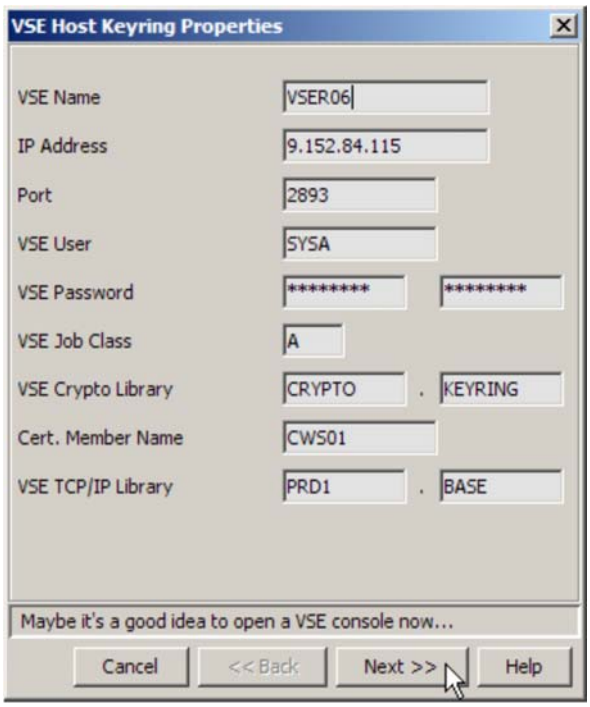

Press the **Add** button and **OK** to add the new definition. We are now ready to create the VSE server key and the necessary certificates.

## 3.2 Creating a self-signed keyring

Click on **the Create self-signed keyring** toolbar button.



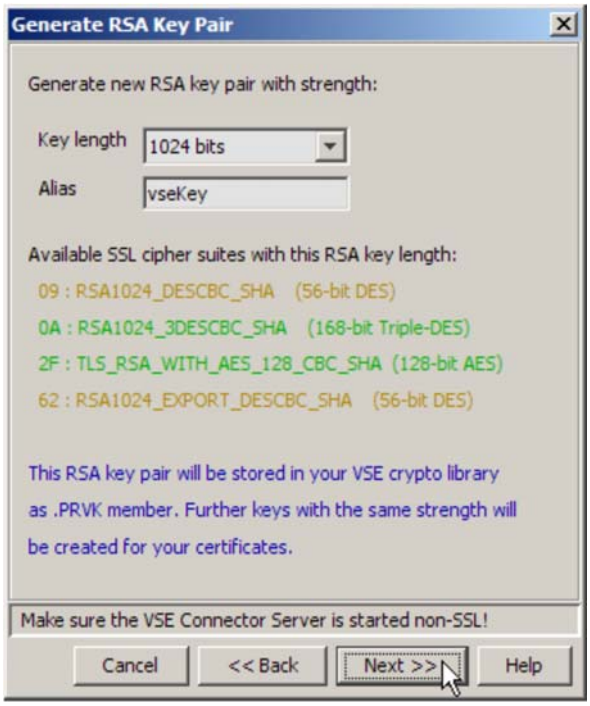

Fill in the required information on the next dialog box



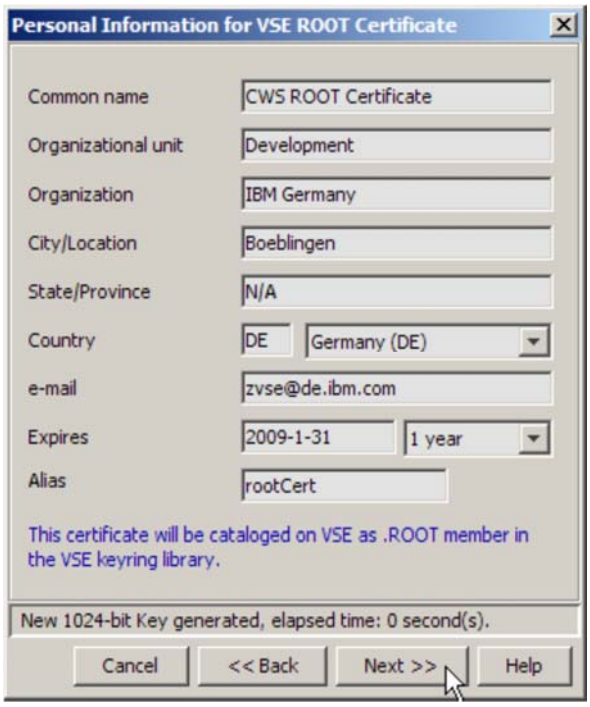

Press **Next**.

On the next dialog specify a password which is used for protecting the local keyring file. You should leave the settings for the encryption of public and private items on **No encryption**. Otherwise there might be problems when reading the file afterwards.


Press **Next**. On the next dialog box specify the key length of your server key and a unique alias string to identify the key. The box shows you a list of available cipher suites with the selected RSA key length (refer to Table 1 on page 17).




Press **Next**. On the following dialog box specify the personal information for the VSE ROOT certificate.




Press **Next**. On the following dialog box specify the personal information for the VSE server certificate.

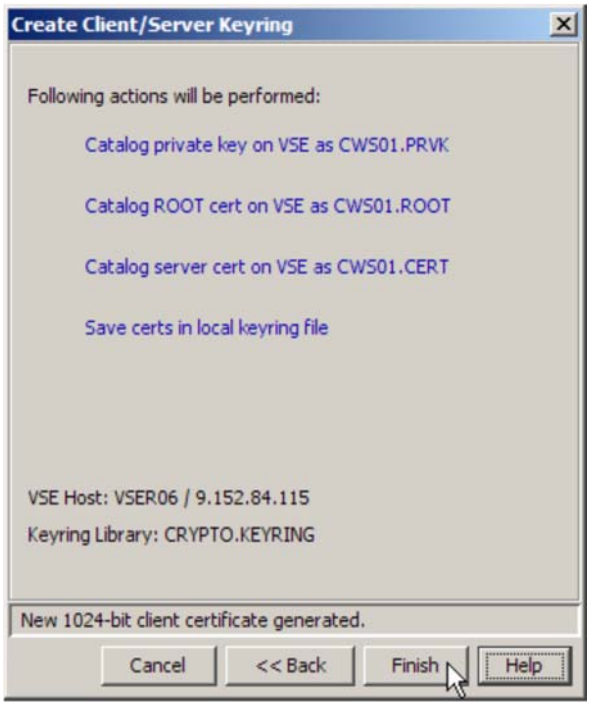

**Note**: in some cases it's required to have the IP address of the server side specified as the Common Name in the server certificate. So let's use our VSE IP address as the Common Name.

Press **Next**.

A client certificate is only needed for client authentication (refer to section Setting up for client authentication on page 33) and for client authentication with user ID mapping (refer to section Client authentication with user ID mapping on page 35.

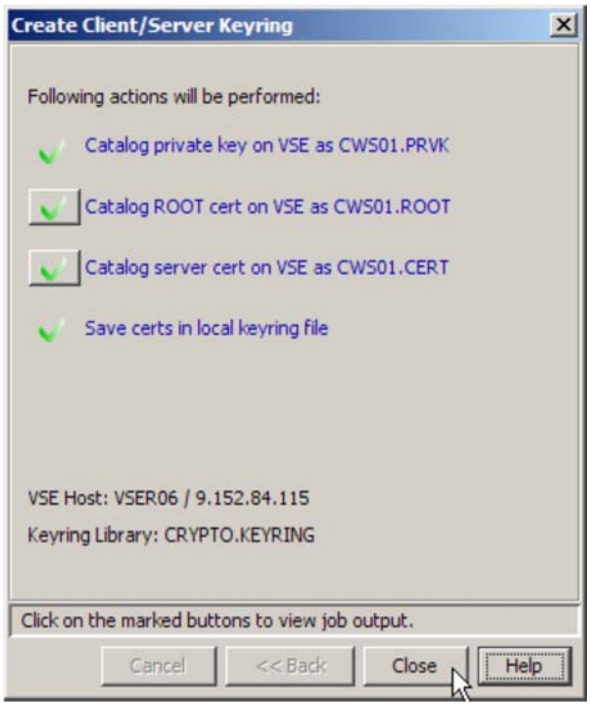

We will do the user ID mapping later, so let's leave the user ID field blank for now.

Press **Next**.




Press **Finish**.

This will send all items to VSE and save the certificates in the local keyring file.




Press **Close**.

Now you have three VSE library members cataloged into CRYPTO.KEYRING. The PRVK member contains the RSA key pair, the ROOT member contains the self-signed VSE ROOT certificate, and the CERT member contains the VSE server certificate.

```
LD CWS*.*

DIRECTORY DISPLAY    SUBLIBRARY=CRYPTO.KEYRING      DATE: 2008-01-31
                                                    TIME: 12:34
-------------------------------------------------------------------
 M E M B E R      CREATION   LAST     BYTES    LIBR CONT SVA  A- R-
NAME     TYPE     DATE      UPDATE   RECORDS   BLKS STOR ELIG MODE
-------------------------------------------------------------------
CWS01    CERT     08-01-31   -  -      714 B       1 YES   -   -   -
CWS01    PRVK     08-01-31   -  -     2048 B       3 YES   -   -   -
CWS01    ROOT     08-01-31   -  -      686 B       1 YES   -   -   -
L113I RETURN CODE OF LISTDIR IS  0
```

You can close the Keyman/VSE tool now. As we don't need the server key on the client side, the key was not saved to the local file.

We will need the client keyring file later in order to import the self-signed root certificate into our Web browser's certificate store.

# 4 Setting up CWS

How to configure CICS Web Support is described in detail in the CICS Enhancements Guide, available online at

http://www.ibm.com/servers/eserver/zseries/zvse/documentation/#cics

Basically, these are the steps for an initial CWS setup.

- Modify the DFHSITSP skeleton

  CWS is activated with a parameter change in skeleton DFHSITSP in CCF library 59. The parameter TCPIP=NO must be changed to TCPIP=YES. After that, the changed configuration skeleton must be processed as a normal job.

- Create a conversion table

  A conversion table phase must be created. It is used by CWS to convert incoming requests to EBCDIC and outgoing responses back to ASCII again. The default table DFHCNV from ICCF library 59 can be used to create such a phase.

- Apply some changes in TCP/IP

  As the last point on the list of changes, TCP/IP needs some modifications. To disable the VSE security check upon session establishment, SET SECURITY=OFF must be passed to the TCP/IP partition. Furthermore, a DNS server should be provided to allow the mapping from IP addresses to host names and vice versa. In addition, TCP/IP must know its own host name and IP address. In our example we add the following statement to the TCP/IP IPINIT member:

  ```
  DEFINE NAME,NAME=VSER06,IPADDR=9.152.84.115
  ```

- Define a TCPIP service

- Recycle CICS

Defining the TCPIP service is shown in more detail in the following section.

## 4.1 Defining the TCP/IP service

The CEDA transaction is used to define a TCPIP service. Note, that SSL is not used at the moment.

```
OVERTYPE TO MODIFY                                        CICS RELEASE = 0411
 CEDA  DEFine TCpipservice( NOSSL     )
  TCpipservice    : NOSSL
  Group           : EXTRACT
  Description  ==>
  Urm          ==> DFHWBADX
  Portnumber   ==> 01082              1-65535
  Certificate  ==>
  STatus       ==> Open               Open ! Closed
  SSl          ==> No                 Yes ! No ! Clientauth
  Attachsec    ==> Verify             Local ! Verify
  TRansaction  ==> CWXN
  Backlog      ==> 00001              0-32767
  TSqprefix    ==>
  Ipaddress    ==>
  SOcketclose  ==> No                 No ! 0-240000
```

Activate your changes:

```
CEMT SET TCPIPS(NOSSL) CLOSED
CEDA INSTALL TCPIPS(NOSSL) GROUP(EXTRACT)
```

It is important that TCP/IP is started **before** CICS is started. Otherwise CICS cannot open the TCP/IP service. This might be a problem during IPL. After defining the TCPIP service you may just recycle CICS and the new TCPIP service should be open when CICS is up again.

After recycling CICS you can use the CEMT transaction to check whether the TCP/IP service is open.

```
171 cemt i tcpips(nossl)
F2-0171
F2 0173
          Tcpipservice(NOSSL)
          Backlog( 00010 )
          Connections(0000)
          Port(01082)
          Ssltype(Nossl)
          Openstatus( Open )
          Transid(CWXN)
          Urm( DFHWBADX )
          Ipaddress(9.152.84.115)
```

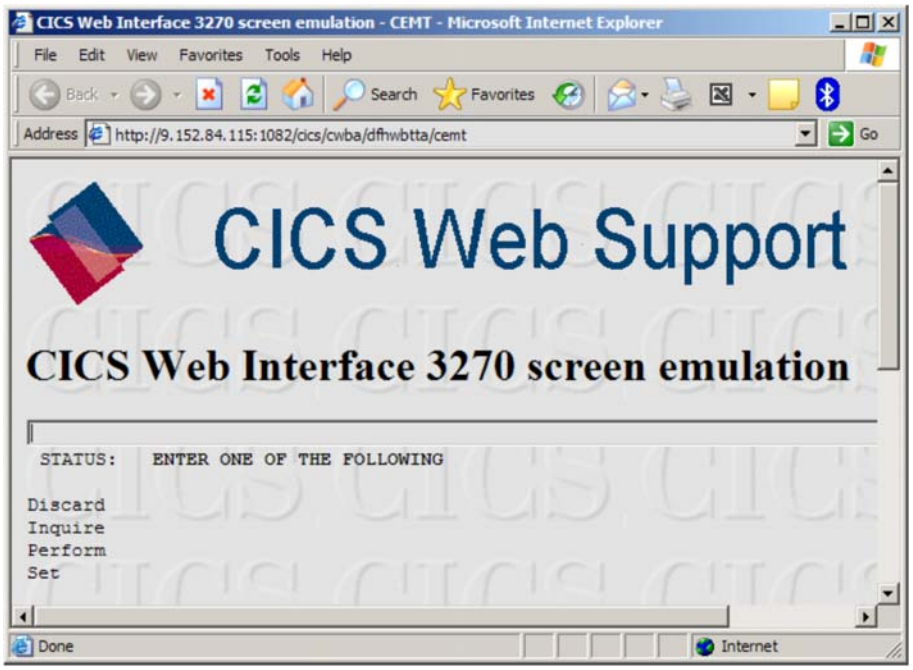
To ensure that TCP/IP is initialized before CICS, you can modify the USERBG procedure (see skeleton SKUSERBG in ICCF library 59) in order to have CICS waiting until TCP/IP is up and running. In the example below, IESWAIT is invoked with parameter 07 indicating the TCP/IP partition (F7).

```
// PWR PRELEASE RDR,TCPIP00 TCP/IP
// EXEC IESWAIT,PARM='07'
```

## 4.2 Connecting to CWS

Let's invoke the CEMT transaction to see whether we can connect to CWS:

http://9.152.84.115:1082/cics/cwba/dfhwbtta/cemt




The next chapter shows how our previously defined CWS is SSL enabled.

# 5 Setting up Secure CWS

We will now duplicate our previously defined NOSSL service and alter the copy in order to setup SSL. This can be done by displaying the service via CEDA V TCPIPS(*) GR(*) and using the copy command.

```
ENTER COMMANDS
 NAME      TYPE          GROUP
 NOSSL     TCPIPSERVICE EXTRACT  copy as(ssl)
```

The newly defined TCP/IP service appears in the list when redisplaying the services.

```
ENTER COMMANDS
 NAME      TYPE          GROUP
 NOSSL     TCPIPSERVICE EXTRACT
 SSL       TCPIPSERVICE EXTRACT
```

## 5.1 Configuring the TCPIP service for SSL

There are three SSL related parameters that must be configured for the TCPIP service.

- SSL: specify *Yes* for SSL server authentication or *Clientauth* for SSL client authentication (refer to Setting up for client authentication on page 33.)

- Certificate name: the member name of the VSE keyring members consisting of a PRVK, a CERT, and a ROOT member.
- Port number: the number of the secure CWS port

The TCPIP service is altered via the CEDA ALTER command. We change the *SSL* parameter to Yes, we change the TCPIP *port number* to a currently free one, and we specify the name of the VSE keyring members in the *Certificate* field (refer to Creating a self-signed keyring on page 8).

```
OVERTYPE TO MODIFY                                          CICS RELEASE = 0411
 CEDA  ALter TCpipservice( SSL      )
  TCpipservice   : SSL
  Group          : EXTRACT
  Description  ==>
  Urm          ==> DFHWBADX
  Portnumber   ==> 01083              1-65535
  Certificate  ==> CWS01
  STatus       ==> Open               Open ! Closed
  SSl          ==> Yes                Yes ! No ! Clientauth
  Attachsec    ==> Verify             Local ! Verify
  TRansaction  ==> CWXN
  Backlog      ==> 00010              0-32767
  TSqprefix    ==>
  Ipaddress    ==>
  SOcketclose  ==> No                 No ! 0-240000
```

After configuring the TCPIP service we have to make additional changes in the CICS initialization.

## 5.2 Configuring system initialization parameters

There are three additional CICS initialization parameters we have to configure for SSL:

- The encryption strength
- The key file
- The SSL delay

These parameters are configured in the DFHSITSP job, see skeleton DFHSITSP in ICCF library 59.

```
* $$ JOB JNM=DFHSITSP,CLASS=A,DISP=D,NTFY=YES
* $$ LST CLASS=Q,DISP=H
// JOB DFHSITSP ASSEMBLE
// LIBDEF *,CATALOG=PRD2.CONFIG
// LIBDEF SOURCE,SEARCH=(PRD1.BASE,PRD1.MACLIB)
// OPTION CATAL,LIST
// EXEC ASMA90,SIZE=(ASMA90,64K),PARM='EXIT(LIBEXIT(EDECKXIT)),SIZE(MAXC
               -200K,ABOVE)'
*****************************************************
*                                                   *
*   5686-CF7 (C) COPYRIGHT IBM CORP. 1984, 2004     *
*                                                   *
*****************************************************
         TITLE 'DFHSITSP  FOR CICS TS APPLID DBDCCICS'
         PUNCH ' CATALOG DFHSITSP.OBJ REP=YES'
         DFHSIT TYPE=CSECT,                                          *
               ...
               ENCRYPTION=STRONG,       SSL ENCRYPTION             *
               ...
               KEYFILE=CRYPTO.KEYRING,  KEY RESIDENCE FOR SSL      *
               ...
               SSLDELAY=600,            DELAY FOR SSL CONNECTION   *
               ...
               DUMMY=DUMMY              TO END MACRO
         END   DFHSITBA
```

```
/*
// IF $MRC GT 4 THEN
// GOTO NOLINK
// EXEC LNKEDT,PARM='MSHP'
/. NOLINK
/*
/&
```

### 5.2.1 Encryption strength

Unlike configuring SSL for HTTP, Telnet, or FTP, where client and server specify the SSL cipher suites explicitly, CICS Web Support specifies three levels of encryption strength: weak, normal, and strong. These levels are mapped to the list of SSL cipher suites like shown in table

| CICS parameter | Hex code | Cipher suite | Encryption strength |
|---|---|---|---|
| WEAK | 01 | SSL_RSA_WITH_NULL_MD5 | No encryption |
| | 02 | SSL_RSA_WITH_NULL_SHA | No encryption |
| NORMAL | 08 | SSL_RSA_EXPORT_WITH_DES40_CBC_SHA | 40 bits |
| | 09 | SSL_RSA_WITH_DES_CBC_SHA | 56 bits |
| STRONG | 0A | SSL_RSA_WITH_3DES_EDE_CBC_SHA | 112 bits |
| | 2F | TLS_RSA_WITH_AES_128_CBC_SHA | 128 bits |
| | 35 | TLS_RSA_WITH_AES_256_CBC_SHA | 256 bits |

**Table 1: available cipher suites for CWS**

As shown above, you should always use STRONG in your SIT.

### 5.2.2 Key file

The key file parameter specifies the library and sublibrary name of the VSE keyring library. In our case this is CRYPTO.KEYRING. Refer to section Creating a self-signed keyring on page 8 where we cataloged our keyring members into this sublibrary.

### 5.2.3 SSL delay

The SSL delay parameter specifies the length of time in seconds for which CICS retains session IDs for secure socket connections. Session IDs are tokens that represent a secure connection between a client and an SSL server. While the session ID is retained by CICS within the SSLDELAY period, CICS can continue to communicate with the client without the significant overhead of an SSL handshake. The value is a number of seconds in the range 0 through 86400. The default value is 600.

After cataloging the changes in DFHSITSP and recycling CICS, the SSL setup is complete. We now have to configure the client side, which means to import our certificates into our Web browsers.

# 6 Client setup with Mozilla Firefox

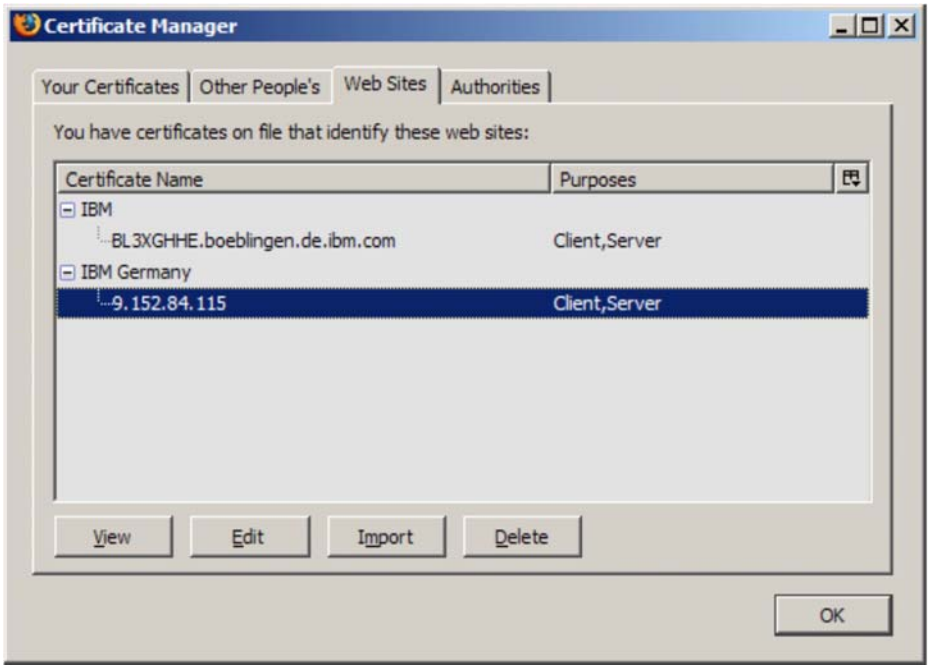
Basically, we have to import our self-signed root certificate into the Mozilla Firefox certificate store. It is important to import the whole PFX file into Firefox to not loose the contained private keys.

**The important thing first**: Mozilla Firefox does not accept **normal** or **weak** encryption as specified in the DFHSITSP. You must specify **strong** encryption. Obviously, Firefox does not use the SSL cipher suites related to normal or weak encryption. However, there is no information about how and where cipher suites can be configured for Firefox.

## *6.1 Importing the VSE certificates during session establishment*

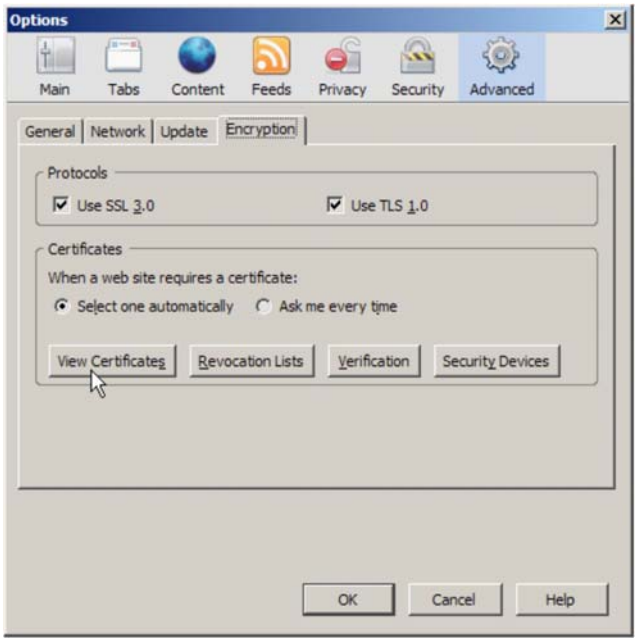
One possibility to import the VSE certificates into the Firefox certificate store is to just connect. You will be prompted to either accept or reject the received server certificate.


You may accept the VSE server certificate permanently and click **OK**. When opening the Firefox certificate store, you will see the imported certificate under tab Web Sites.




## 6.2 Manually Importing the VSE certificates into Firefox

Another possibility is to import the certificate manually. On the Firefox main window click on **Tools** – **Options**. On the Options dialogbox select **Advanced** – **Encryption**.



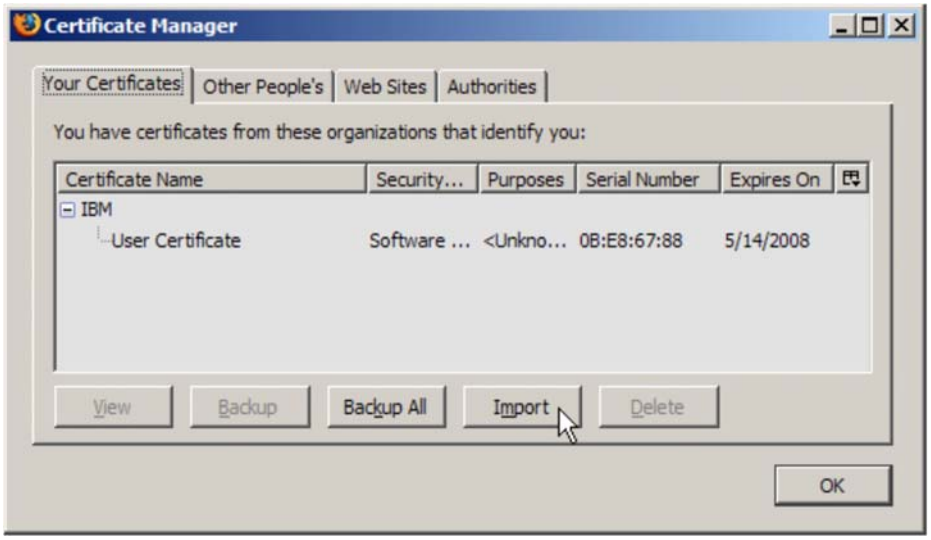

Click on **View Certificates**.

Now we again have two choices:

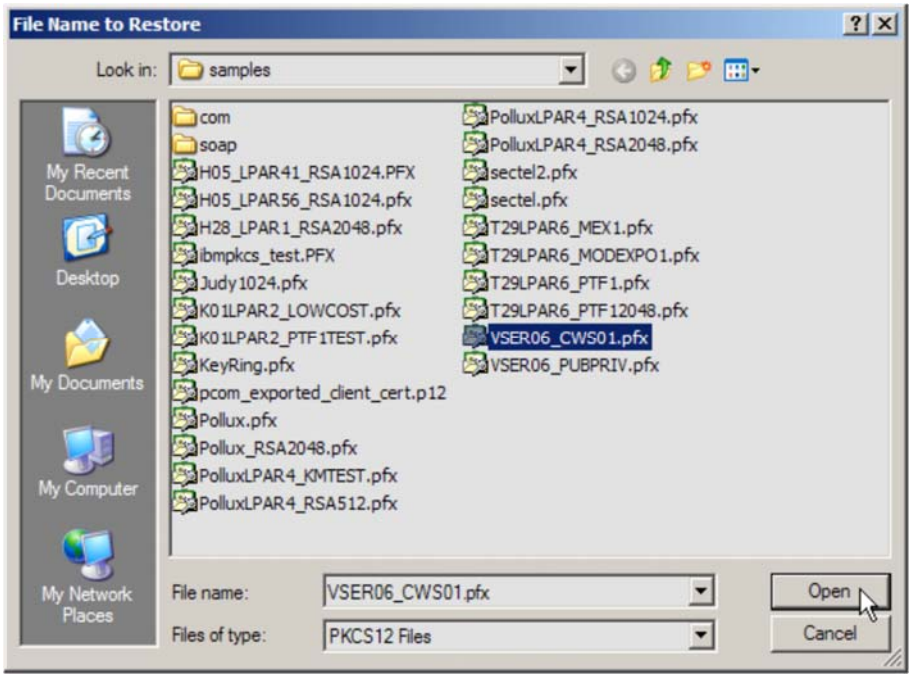
- Importing the complete VSE keyring file
- Importing the selected VSE server certificate

### 6.2.1 Importing the complete VSE keyring file

Select tab **Your Certificates** and click on **Import**.



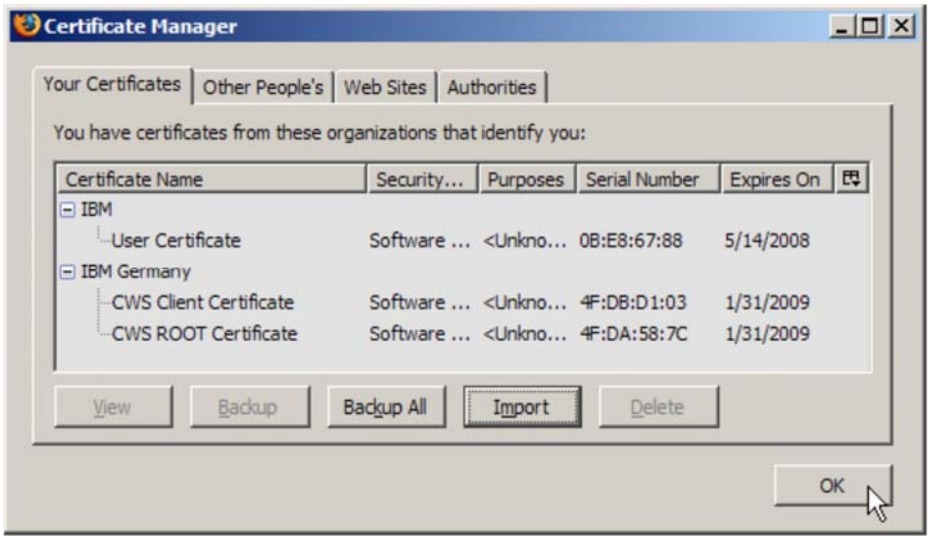

In the file dialog browse to the VSE keyring file and click on **Open**.




You are prompted for the VSE keyring file password that you specified when creating the file with Keyman/VSE (refer to section Creating a self-signed keyring on page 8).


Click **OK**.


Click **OK**.



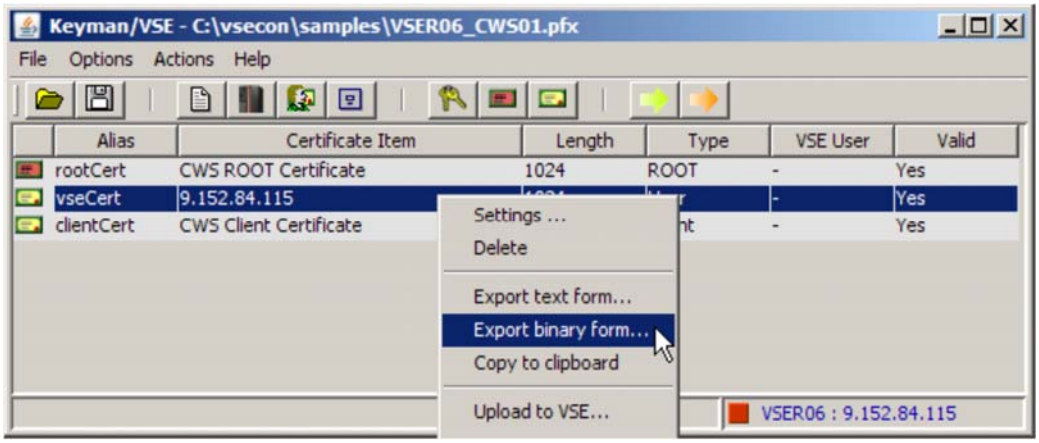

Two certificates are now imported: the CWS root certificate and the client certificate. The root certificate can now be used to verify the VSE server certificate when establishing an SSL connection.

## 6.2.2 Importing the VSE certificate selectively

When importing the complete VSE keyring file, the root certificate has been imported. However, another way is to only import the VSE server certificate into the certificates under tab **Web Sites**. Trust must then be established manually. The VSE root certificate is not needed in this case.

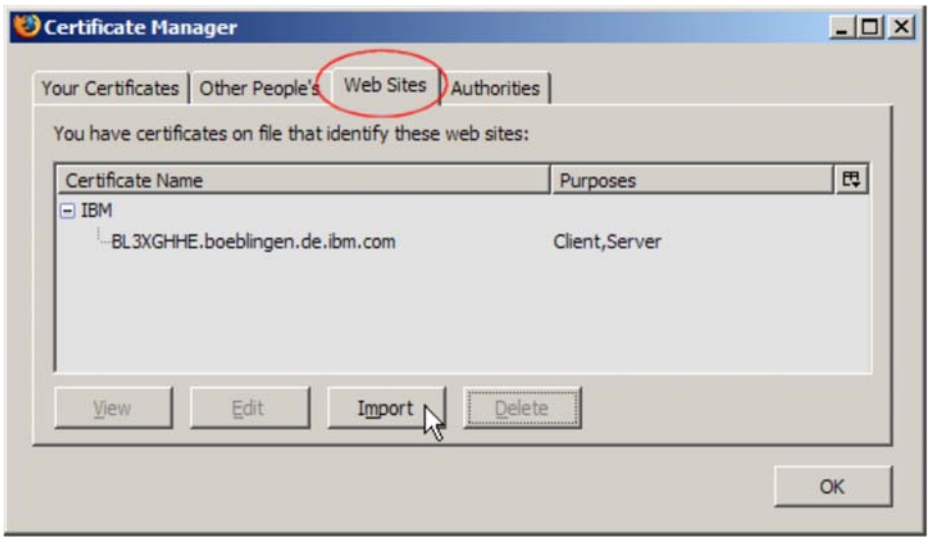
The import dialog under Web Sites does not accept complete keyring files (PFX), but wants a binary certificate file containing only one certificate. You can use Keyman/VSE to export the VSE server certificate into a binary file.

Start Keyman/VSE again and open the VSE keyring file.

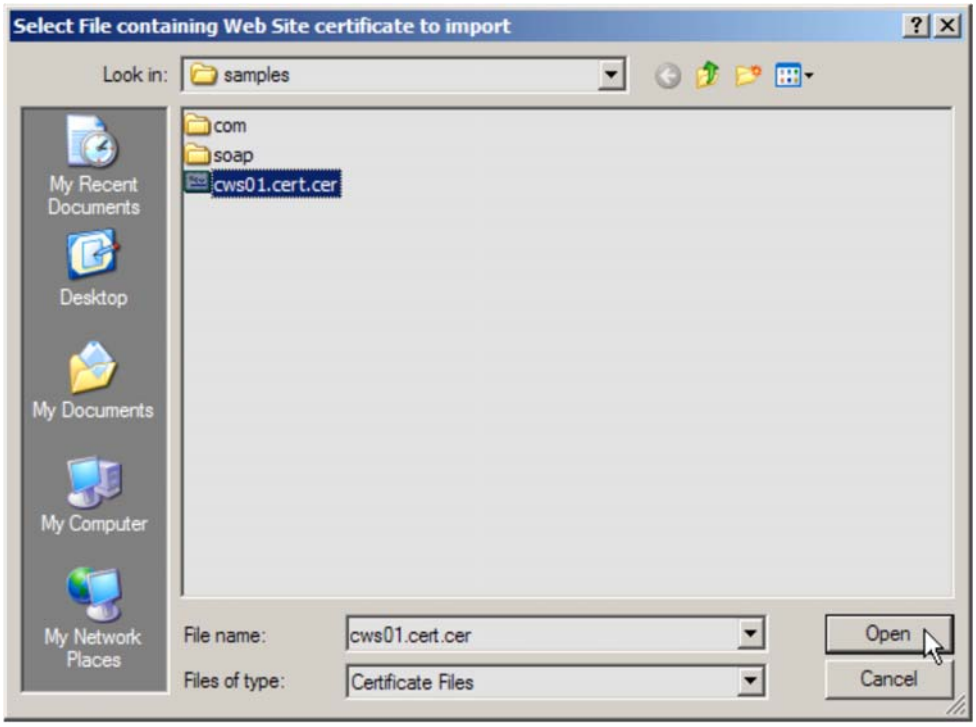



Right-click the VSE certificate and select **Export binary form**. Specify a filename with file extension **cer** and save the file.

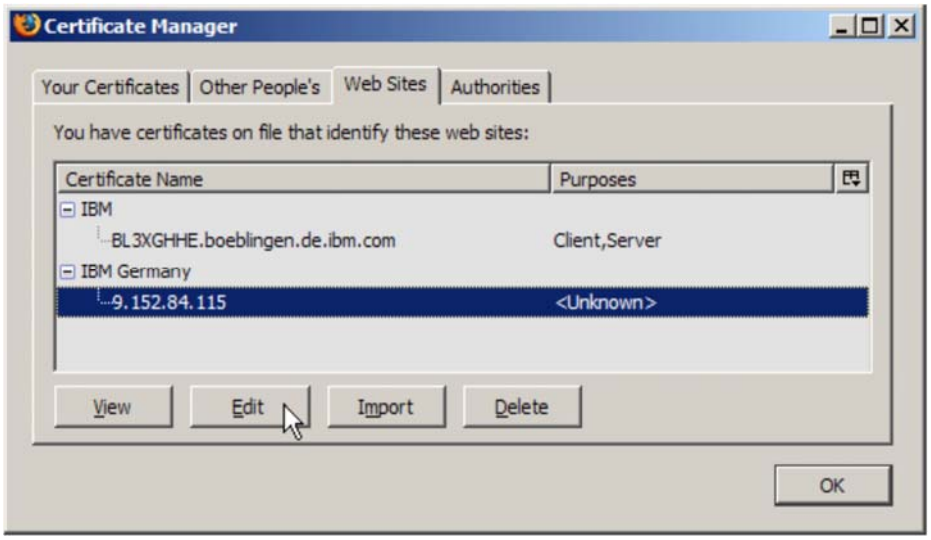
You can now import this binary certificate file into Firefox. Make sure that tab Web Sites is selected.




Browse to the binary certificate file and press **Open**.

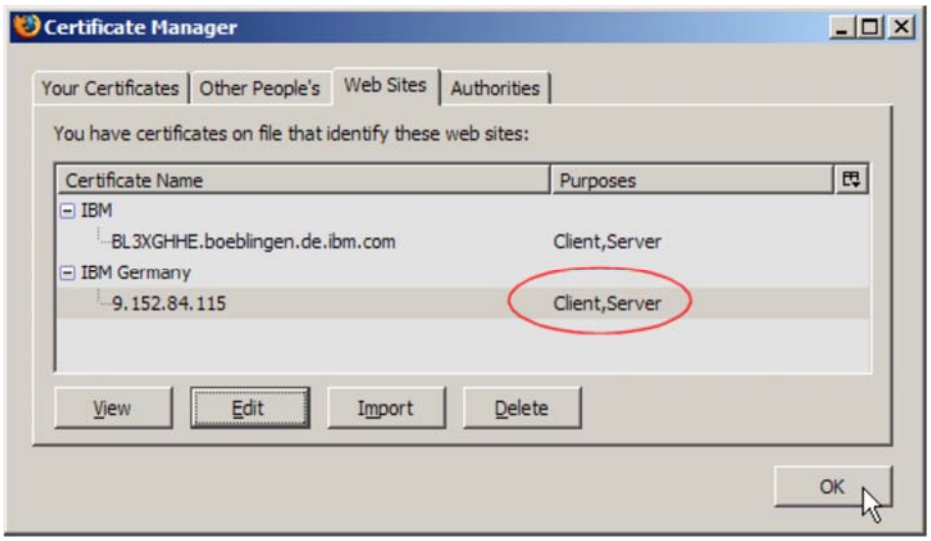



The VSE certificate is now imported, but the SSL connection will not work until you specify to trust this certificate. When importing the complete VSE keyring file, the trust had been established during the import step, because the process did read also the VSE root certificate.




Note that **<Unknown>** is displayed in column Purposes. This means that the certificate is not trusted. The connection would not work in this case. To establish trust click on **Edit**.


Select the upper radio button and press **OK**. The certificate is now shown as trusted.




Now we have imported the VSE server certificate into Firefox and manually trusted this certificate.

Firefox is now ready for connecting to CWS via SSL server authentication.

## 6.3 Configuring cipher suites in Firefox

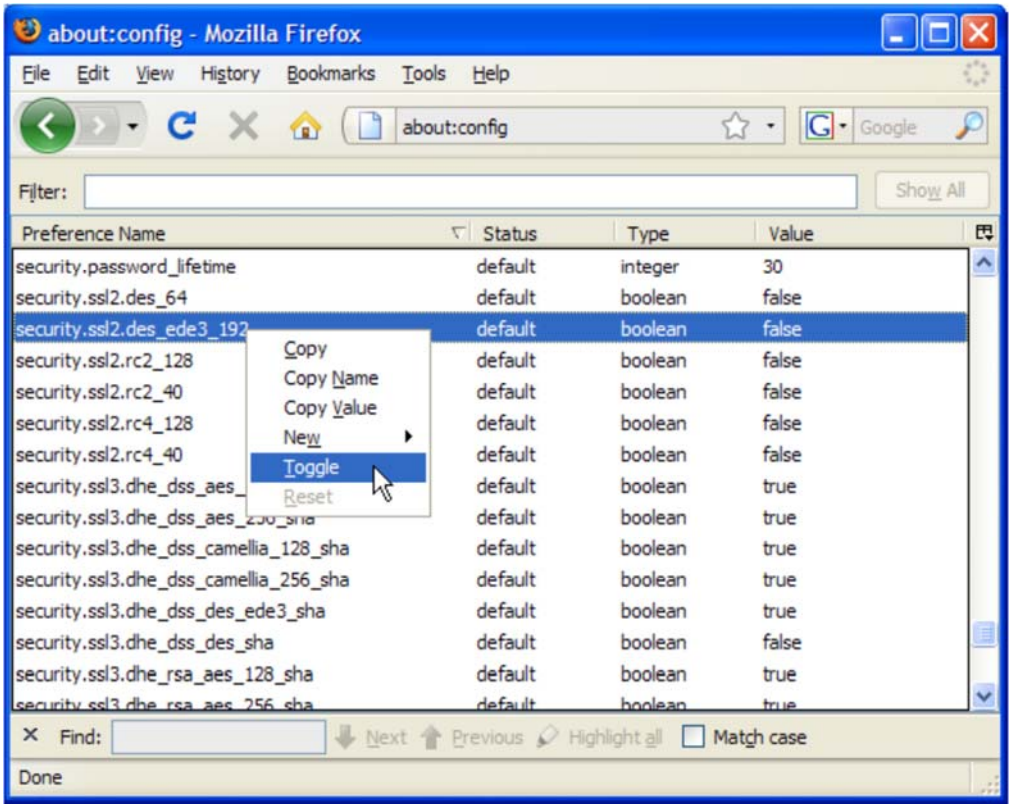
You can find some information of configuring SSL cipher suites in Mozilla Firefox on

https://developer.mozilla.org/en/Security_in_Firefox_2

Basically, you just enter

about:config

in the browser's address field. You are then prompted with some warning message. After proceeding with the dialog, you can view and change the entire browser configuration.




You can change displayed values by right-clicking an entry.

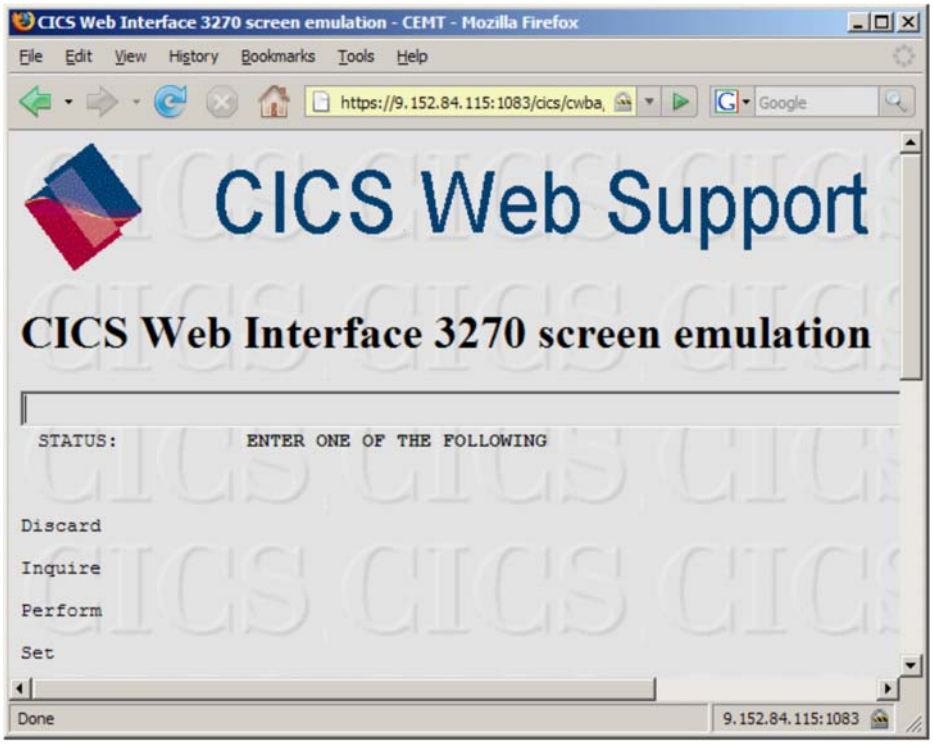
## 6.4 Starting a secure session

Once CICS is restarted on the VSE side and the SSL TCPIP service is open we can connect to CWS via SSL.

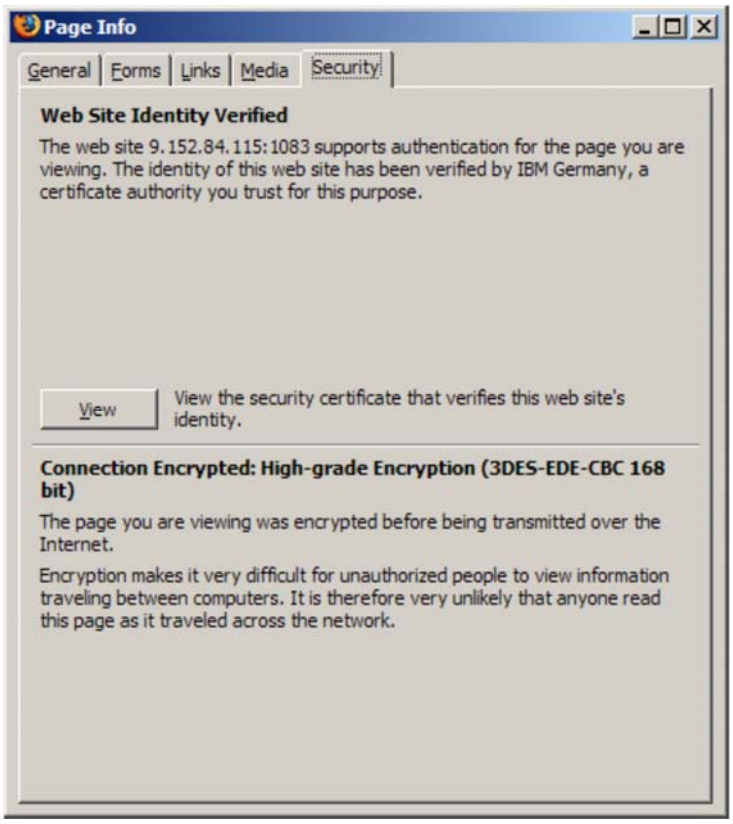
```
cemt i tcpips
F2-0171
F2 0173
         Tcpips(NOSSL    ) Bac( 00010 ) Con(0000) Por(01082)
         Ope Tra(CWXN) Urm( DFHWBADX ) Ipa(9.152.84.115   )              Wai
         Tcpips(SSL      ) Bac( 00010 ) Con(0000) Por(01083) Ssl
         Ope Tra(CWXN) Urm( DFHWBADX ) Ipa(9.152.84.115   )              Wai
         RESPONSE: NORMAL TIME:  13.17.15  DATE: 01.31.08
```

Note that we now specify https and the secure port number 1083:

https://9.152.84.115:1083/cics/cwba/dfhwbtta/cemt




When double-clicking on the closed lock icon at the right bottom corner of the browser window, you can view the properties of the current SSL session.

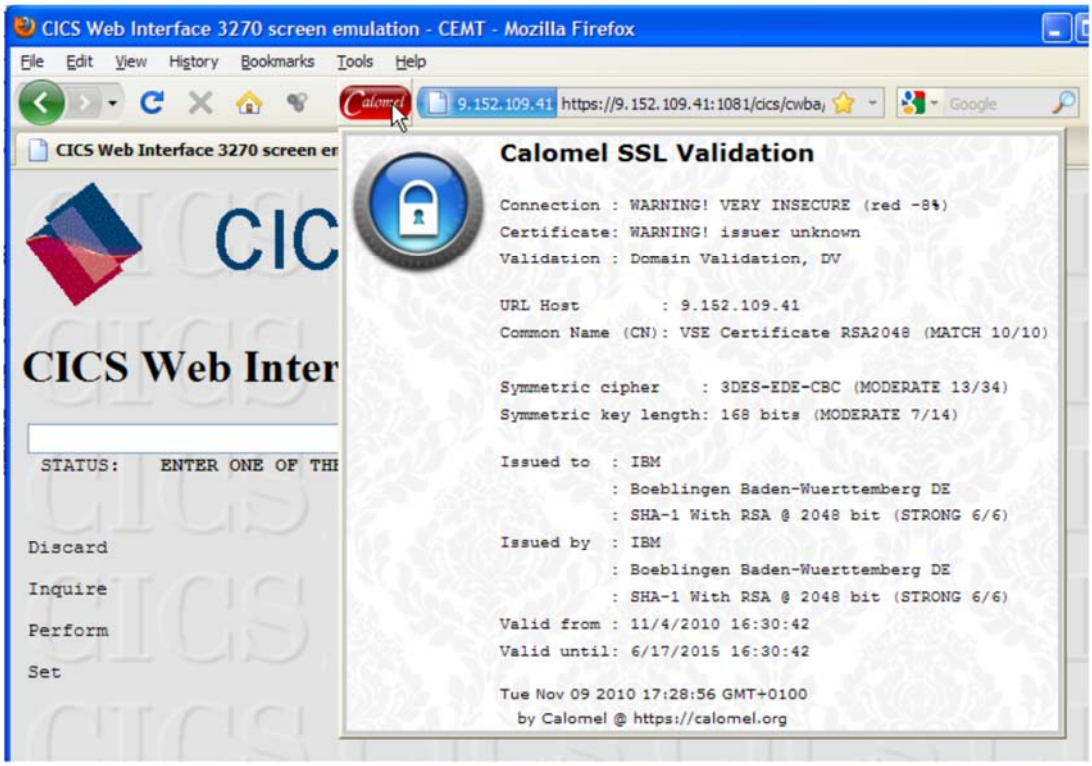


## 6.5 Displaying SSL properties in Mozilla Firefox

There is a variety of add-ons available for the Mozilla Firefox browser. One of them, called “Calomel”, can display a detailed summary of the SSL connection. You can download the add-on from

https://addons.mozilla.org/de/firefox/addon/207653/

When being connected via SSL, the Calomel toolbar button toolbar button will change its color depending on the strength of encryption from red (weak) to green (strong). The drop down window shows a detailed summary of the SSL connection.




# 7 Client setup with MS Internet Explorer

This chapter describes the client setup with Microsoft Internet Explorer. The main difference to Mozilla Firefox is that we now import our keyring file into the Windows certificate store.

In contrast to Firefox, Internet Explorer also works with WEAK or NORMAL encryption as specified in the DFHSITSP.

Like for Mozilla Firefox there are two ways of getting the VSE certificates imported into the browser’s certificate store.

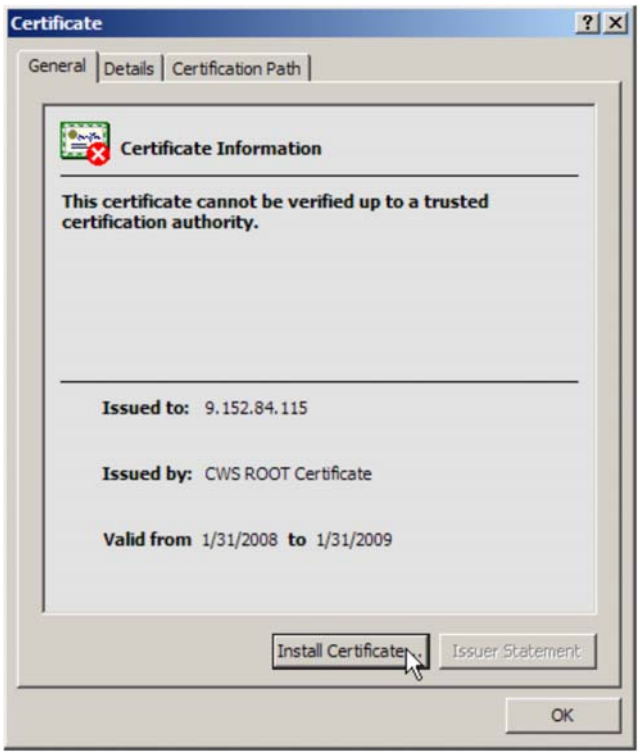
- Just connect and let Internet Explorer import the necessary certificates while establishing the SSL session
- Import the certificates manually

## 7.1 Importing the VSE certificates during session establishment

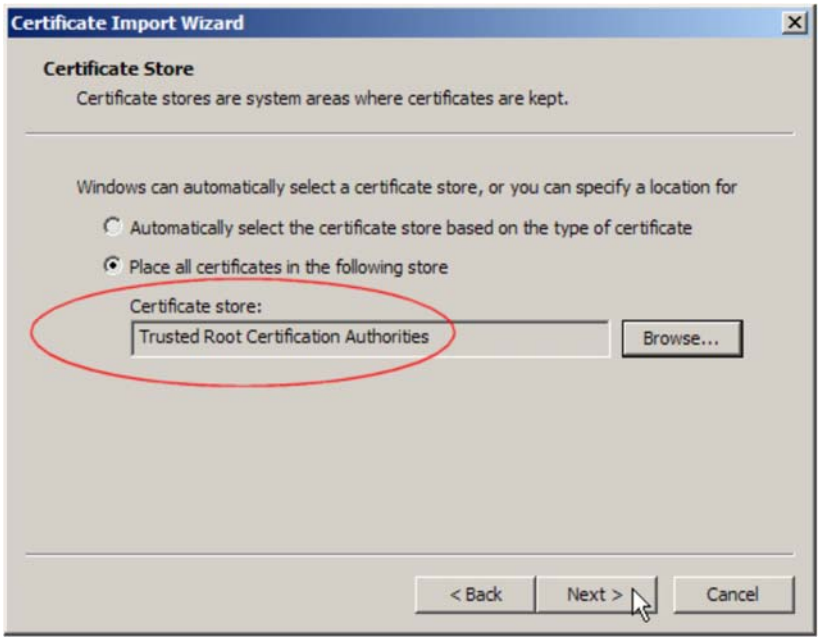
The following dialogbox is displayed by Internet Explorer when the received server certificate cannot be verified.


Click **Yes** to just go ahead and connect. The certificate would not be imported in this case.

To import the certificate, click on **View Certificate**. On the next dialog box click on **Install Certificate**.

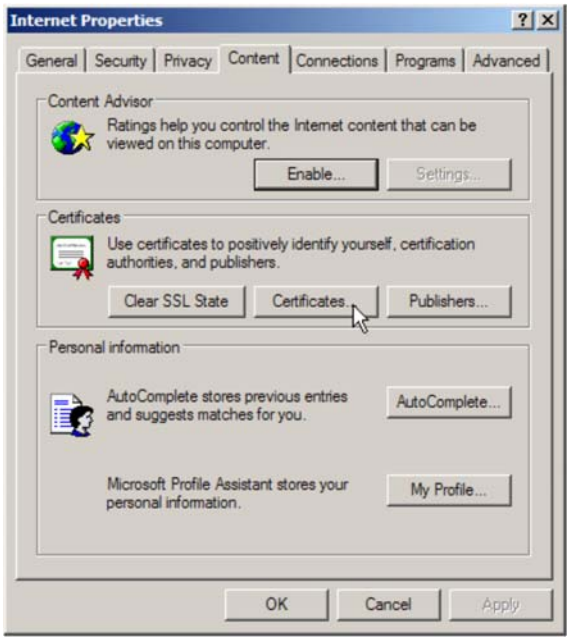



Press the **Browse** button to place the certificate in the Trusted Root Certification Authorities store.

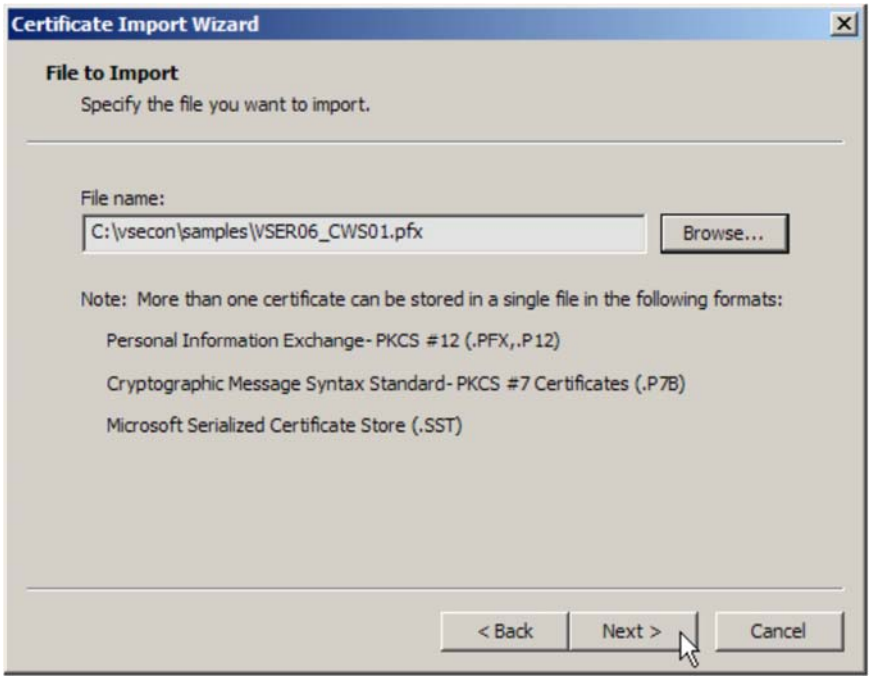



## 7.2 Manually Importing the VSE certificates into Internet Explorer

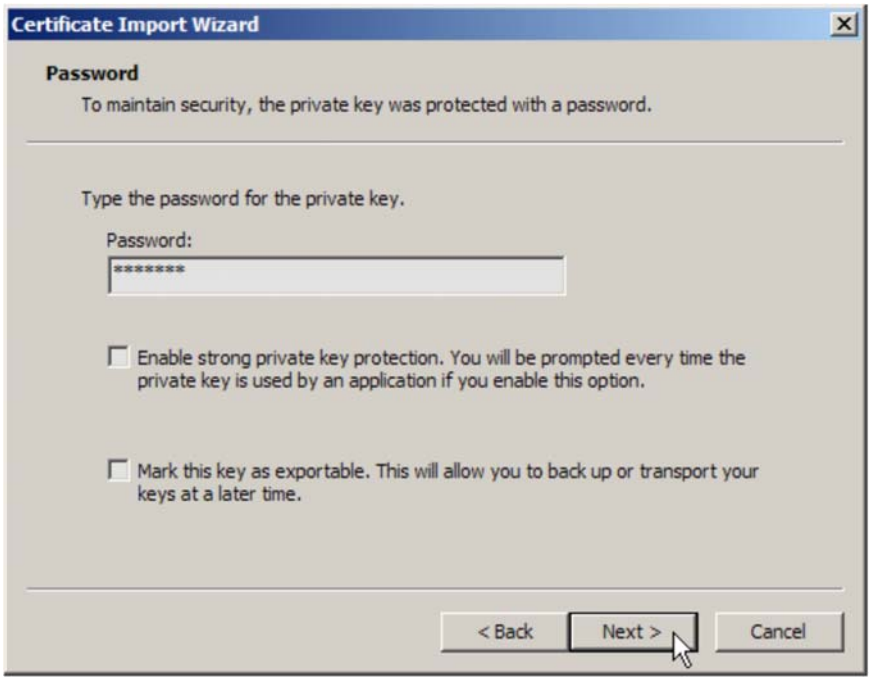
To import the certificates created in section Creating a self-signed keyring on page 8, open the Windows **Control Panel** and double-click **Internet Options**. On tab **Content** click on **Certificates**.



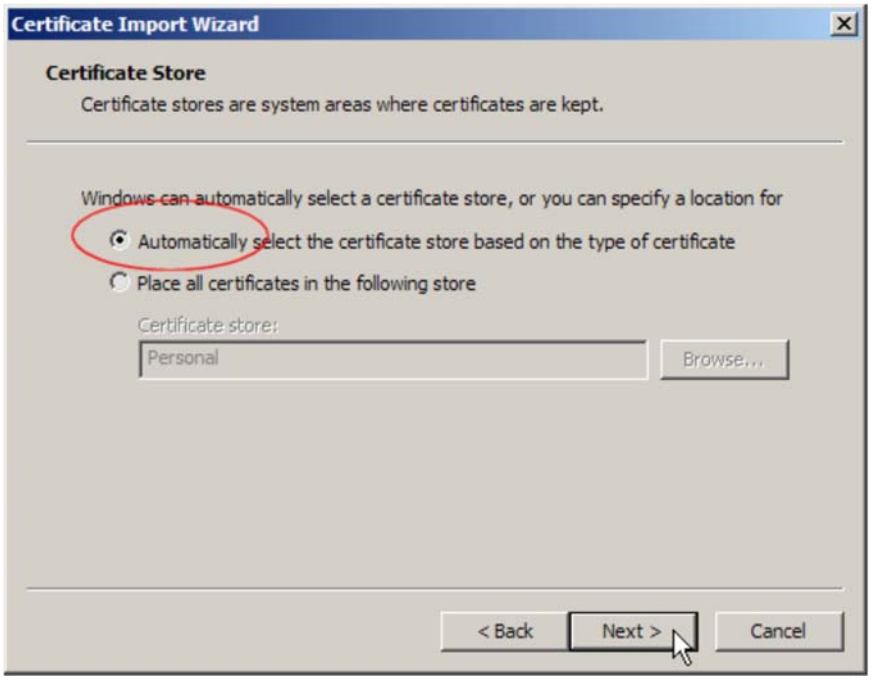

In the next box click on **Import**… and follow the Import Wizard dialogs.



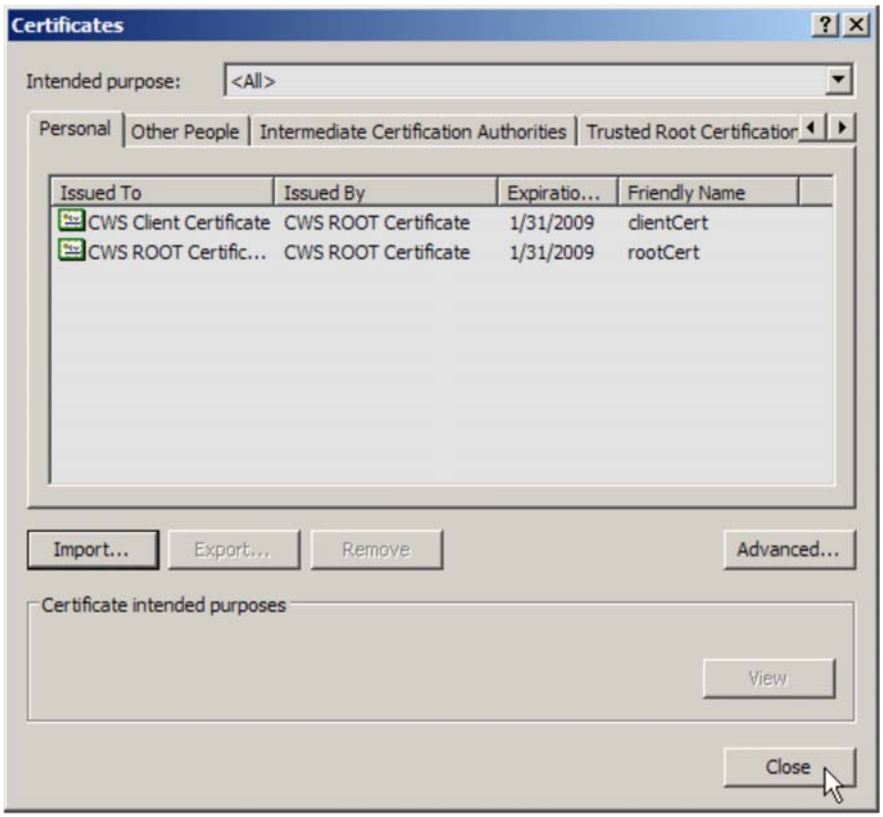

Enter the keyring file password and press **Next**.




In the following box select the upper radio button.




Press **Next.** The VSE certificates are now imported as Personal certificates.




Press **Close**.

You will see in section Using Internet Explorer on page 34 that in this case you are asked to select the client certificate during session establishment, because Internet Explorer does not know which one of the two certificates shall be sent to the server as the client certificate.

## 7.3 Configuring cipher suites in Internet Explorer

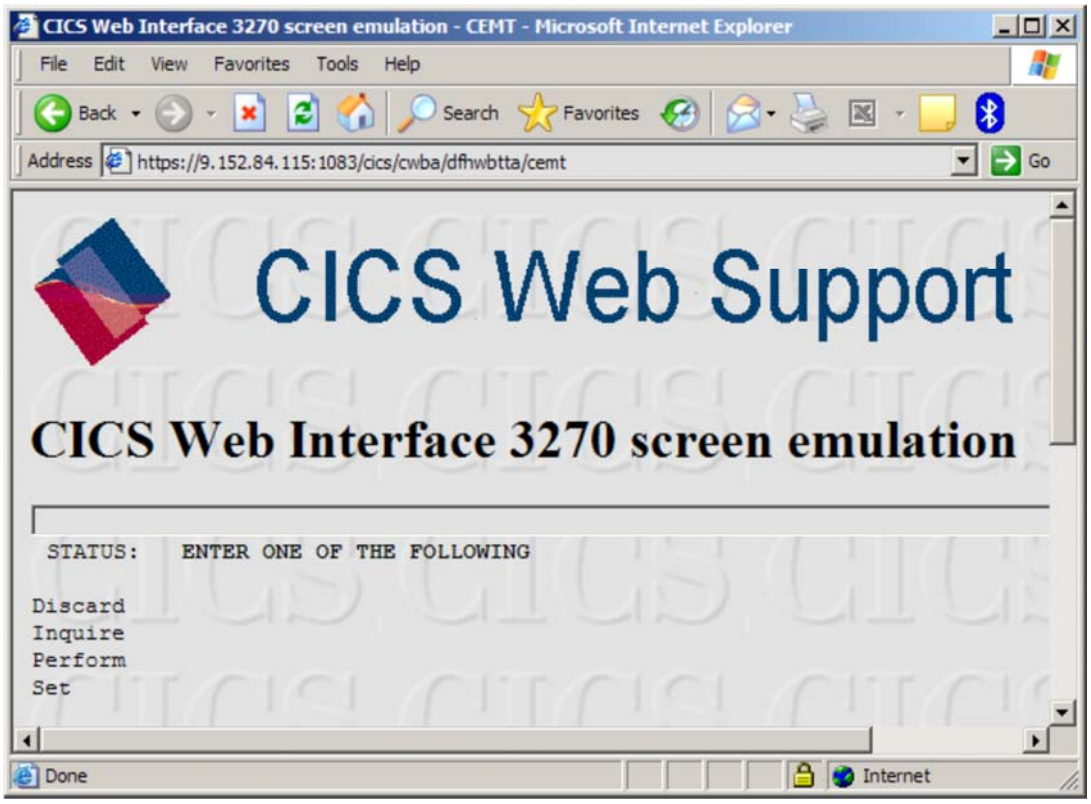
SSL cipher suites are not visible through any Internet Explorer dialogs. Instead, they are defined in the Windows registry and therefore affect your entire computer. This is described on

http://support.microsoft.com/

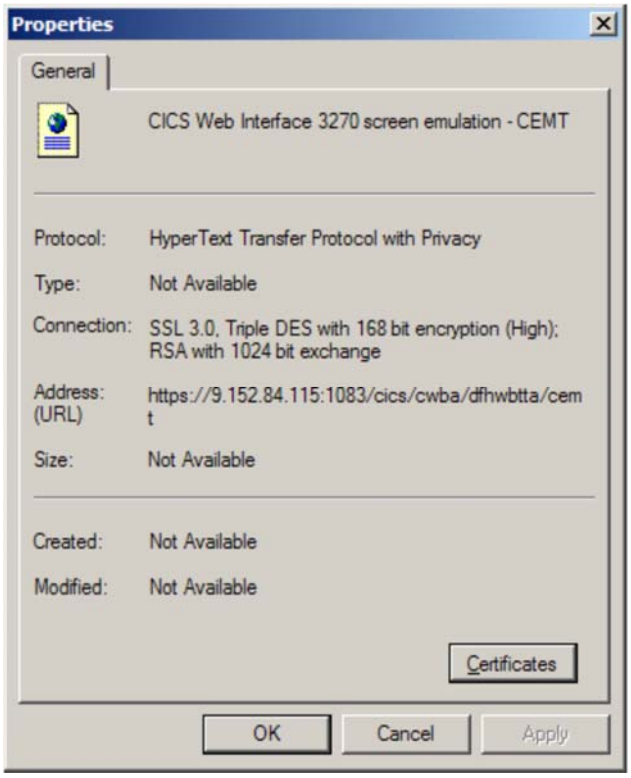
Search for “SSL cipher suites” and you are directed to the most current knowledge base entry.

## 7.4 Starting a secure session

We can now use MS Internet Explorer to connect to CWS via SSL server authentication.




You can view the actual encryption by selecting **File** – **Properties** in the Internet Explorer main window.




# 8 Setting up for client authentication

SSL client authentication provides more security than server authentication, because both communication partners provide a certificate in order to establish trust. To setup client authentication for CICS Web Support we have to change the TCPIP service on the VSE side to enable client authentication. This is done via the SSL parameter of the TCPIP service definition.

```
OVERTYPE TO MODIFY                                      CICS RELEASE = 0411
 CEDA  ALter TCpipservice( SSL      )
  TCpipservice    : SSL
  Group           : EXTRACT
  Description  ==>
  Urm          ==> DFHWBADX
  Portnumber   ==> 01083              1-65535
  Certificate  ==> CWS01
  STatus       ==> Open               Open ! Closed
  SSl          ==> Clientauth         Yes ! No ! Clientauth
  Attachsec    ==> Verify             Local ! Verify
  TRansaction  ==> CWXN
  Backlog      ==> 00010              0-32767
  TSqprefix    ==>
  Ipaddress    ==>
  SOcketclose  ==> No                 No ! 0-240000
```

Activate your changes:

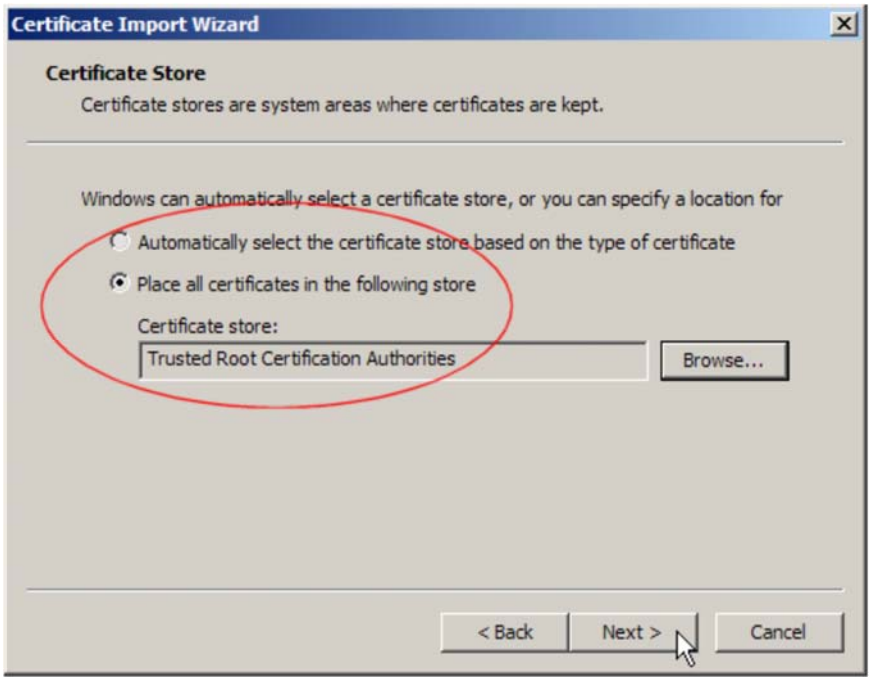
```
CEMT SET TCPIPS(SSL) CLOSED
CEDA INSTALL TCPIPS(SSL) GROUP(EXTRACT)
```

Make sure the VSE client certificate is imported into the browser's certificate store. When using Firefox, refer to section "Importing the complete VSE keyring file" on page 20, when using Internet Explorer, refer to section "Manually Importing the VSE certificates into Internet Explorer" on page 29.

## 8.1 Using Internet Explorer

As mentioned in section Manually Importing the VSE certificates into Internet Explorer on page 29, Internet Explorer cannot determine which personal certificate to use as the client certificate. Therefore you are prompted with this dialog box to select the client certificate.


To get around this prompt, you can manually delete the CWS root certificate from the Personal store and import the VSE keyring file once again, this time selecting to place all certificates in the Trusted Root Certification Authorities store.



This will in fact only import the CWS root certificate, because this is the only root certificate in the keyring file. You can now connect using Client Authentication without being prompted.

## 8.2 Client authentication with user ID mapping

Mapping a client certificate to a VSE user ID enables the VSE Security Manager to check all actions against the authorization of this user.

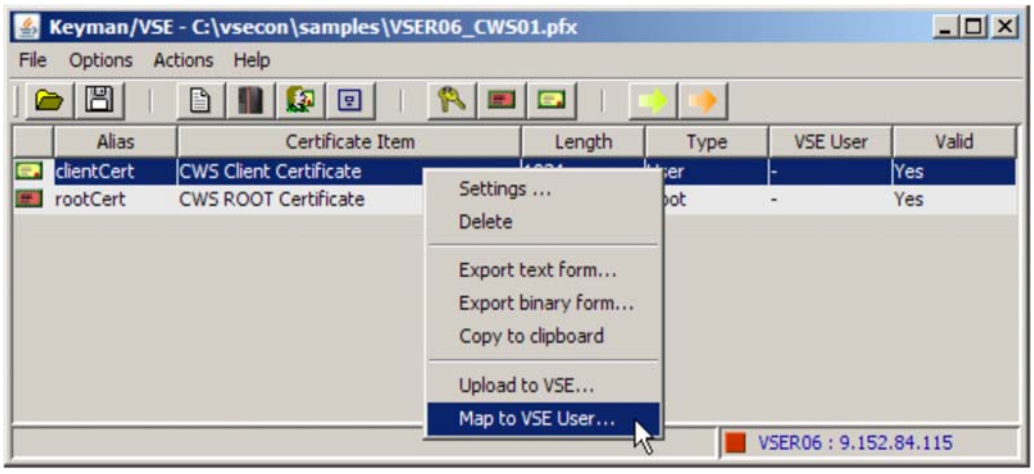
Following tasks are necessary to enable user ID mapping.

- Map the client certificate to a VSE user
- Upload the client certificate to VSE
- Activate the mapping on VSE

All tasks can be performed using the Keyman/VSE tool.

### 8.2.1 Mapping the client certificate to a VSE user

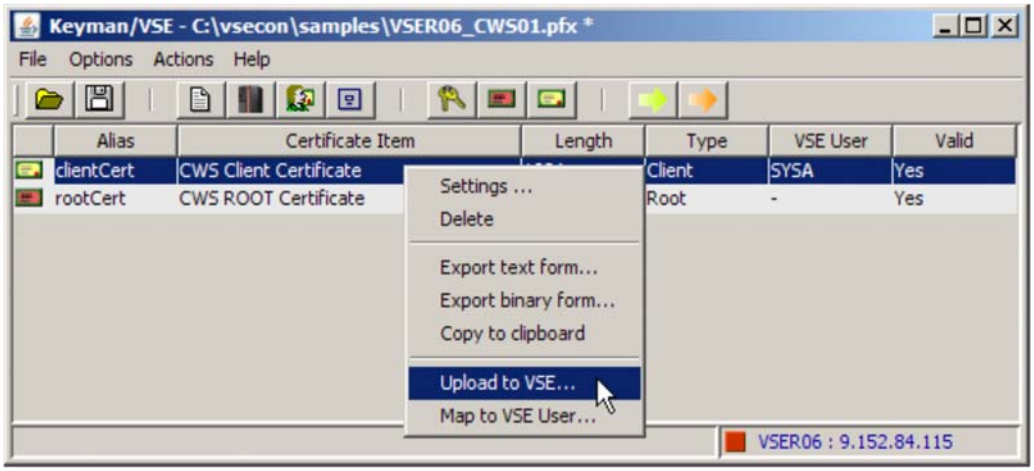
First, we map our already created client certificate to a VSE user ID.



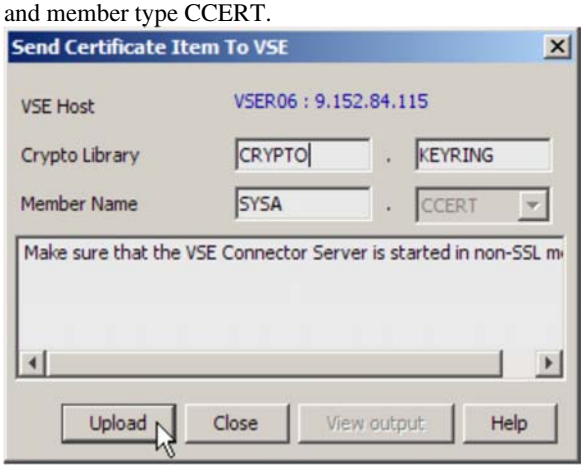


### 8.2.2 Uploading the client certificate to VSE

Then we upload the client certificate to VSE.



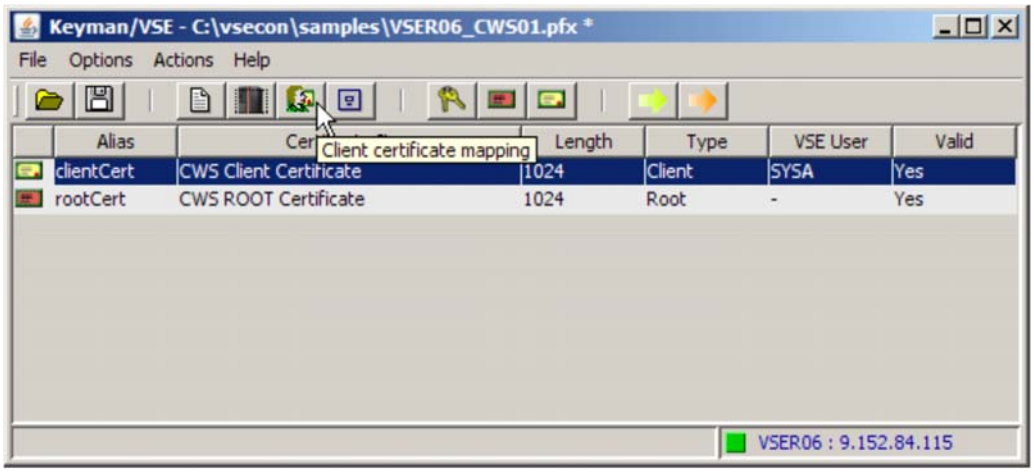

Keyman uploads the client certificate to a VSE library member with member name equal to the VSE user ID and member type CCERT.



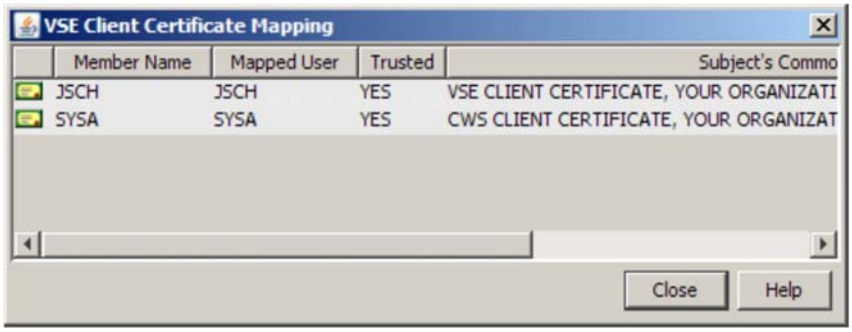

Uploading the client certificate results in two actions.

- Submitting a BSSDCERT job to catalog the certificate
- Submitting a second BSSDCERT job to activate the table of certificates

Keyman/VSE can now show the table of mapped certificates. This function is equal to the Interactive Interface dialog 2.8.4 (Maintain Certificate - User ID List).



Click on toolbar button **Client certificate mapping**.




All actions of this CWS client are now checked by the VSE Security Manager against the user's authorizations.

You can use the CICS EXTRACT CERTIFICATE command to get information about a received client certificate. This is described in the CICS Internet Guide, which is available online at:

http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/Shelves/DFHWSH0P

Check for program DFH0WBCA in PRD1.BASE, which is a COBOL sample program showing the use of the EXTRACT CERTIFICATE function.

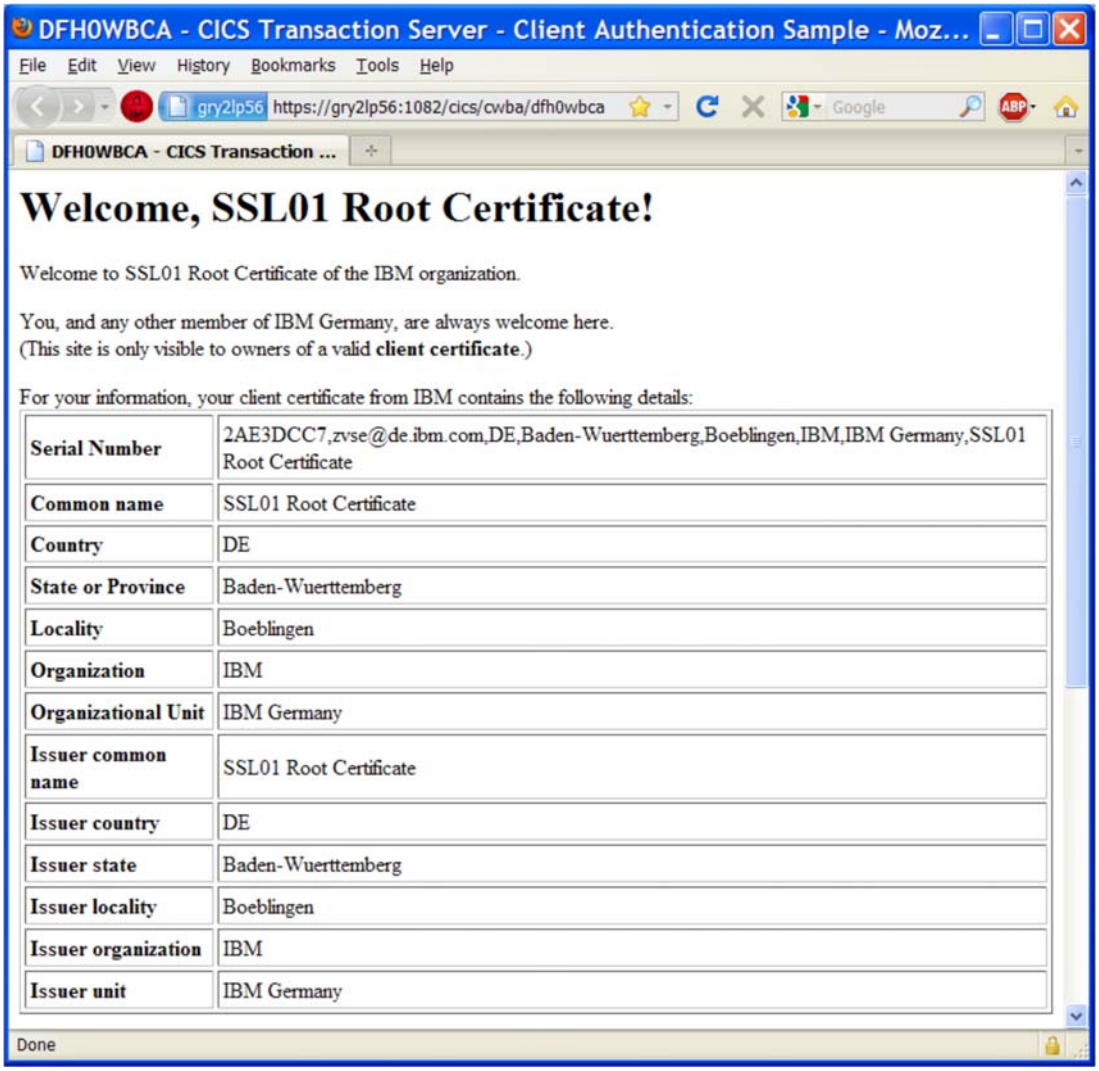
**Note:** this requires TCP/IP zap 1.5F 498.

### 8.2.3 Using the DFH0WBCA sample

To use the DFH0WBCA sample, compile the COBOL program and do a DEFINE PROGRAM in CICS. Then you can invoke the program directly via the TCP/IP service with SSL client authentication. In our test we used the following URL:

https://gry2lp56:1082/cics/cwba/dfh0wbca

The browser window then shows a table with the client certificate properties.




# 9 Known problems and workarounds

This chapter describes some known problems and workarounds.

## 9.1 Abend AKEA in DFHSOSE

**Symptom:**

Following error occurs when trying to connect to CWS via SSL.

```
F2 0173  SYSID=CIC1 APPLID=DBDCCICS
F2 0173 DFHSO0001 DBDCCICS An abend (code 0C2/AKEA) has occurred at offset
        X'FFFF' in module DFHSOSE .
```

**Possible reasons:**

- PTFs UK30576 (z/VSE 4.1) or UK30575 (z/VSE 3.1) are missing

- An abend in DFHSOSE is sometimes caused by previous CICS or TCP/IP related problems.

**Workaround:**

If UK30576 / UK30575 is applied, it might help to clean the CICS local and global catalogs. Following job does a cleanup on the two catalogs.

```
// JOB DEDE
// ID USER=FORSEC,PWD=FORSEC
// OPTION SADUMP=5
// OPTION SYSDUMPC
   LOG
* ------------------------------------------------------------------
*   REDEFINE CLUSTER FOR CICS LOCAL CATALOG DATASET (LCD)
* ------------------------------------------------------------------
// EXEC IDCAMS,SIZE=AUTO
   DELETE (CICS.LCD) CL NOERASE PURGE       -
   CATALOG(VSESP.USER.CATALOG)
   DEFINE CLUSTER(NAME(CICS.LCD)            -
   RECORDSIZE (45 124)                      -
   RECORDS (3000 200)                       -
   KEYS   (28 0)                            -
   REUSE                                    -
   INDEXED                                  -
   FREESPACE (10 10)                        -
   SHR(2)                                   -
   VOL(DOSRES SYSWK1))                      -
   DATA(NAME(CICS.LCD.§D§)                  -
   CISZ   (8192))                           -
   INDEX(NAME(CICS.LCD.§I§))                -
   CATALOG(VSESP.USER.CATALOG)
/*
* INITIALIZE THE LOCAL CATALOG DATASET
// LIBDEF *,SEARCH=(PRD2.CONFIG,PRD2.SCEEBASE,PRD1.BASE)
// EXEC DFHCCUTL,SIZE=300K
/*
* ------------------------------------------------------------------
*   REDEFINE CLUSTER FOR CICS GLOBAL CATALOG DATASET (GCD)
* ------------------------------------------------------------------
// EXEC IDCAMS,SIZE=AUTO
   DELETE (CICS.GCD) CL NOERASE PURGE       -
   CATALOG(VSESP.USER.CATALOG)
   DEFINE CLUSTER(NAME(CICS.GCD)            -
   RECORDSIZE (4089 4089)                   -
   RECORDS (2000 200)                       -
   KEYS   (28 0)                            -
   REUSE                                    -
   INDEXED                                  -
   FREESPACE (10 10)                        -
   SHR(2)                                   -
   VOLUMES(DOSRES SYSWK1))                  -
   DATA(NAME(CICS.GCD.§D§)                  -
   CISZ   (8192))                           -
   INDEX(NAME(CICS.GCD.§I§))                -
   CATALOG(VSESP.USER.CATALOG)
/*
* INITIALIZE GLOBAL CATALOG DATASET (GCD)
// EXEC IDCAMS,SIZE=AUTO
   REPRO INFILE                                    -
            (SYSIPT                                -
            ENVIRONMENT                            -
              (RECORDFORMAT(FIXUNB)                -
               BLOCKSIZE(80)                       -
               RECORDSIZE(80)))                    -
         OUTFILE(DFHGCD)
  ACTL 0002
/*
/&
```

## 9.2 Abend code x'080C' in module DFHSOSE

**Symptom:**

Following error occurs when trying to connect to CWS via SSL.

```
F2 0173 DFHSO0002 DBDCCICS A severe error (code X'080C') has occurred in
        module DFHSOSE .
F2 0173 DFHME0116 DBDCCICS
        (Module:DFHMEME) CICS symptom string for message DFHSO0002 is
        PIDS/564805400 LVLS/411 MS/DFHSO0002 RIDS/DFHSOSE PTFS/UK20279
        PRCS/0000080C.
```

**Possible reasons:**

Your TCP/IP is not licensed for the cryptographic features on VSE. See following link:

http://www.ibm.com/support/docview.wss?uid=swg21213579

Check your LIBDEFs and make sure the right license key is accessed first.

## 9.3 Error DFHWB0723

**Symptom:**

Following error occurs when trying to connect to a CICS program.

```
DFHWB0723 02/07/12 11:39:55 DBDCCICS CWXN The CICS Web analyzer program returned an
error response. Program name: DFHWBADX. RESPONSE: 4. REASON: 1. Host IP address:
9.152.86.91    . Client IP address: 9.152.222.71   .
TCPIPSERVICE: SSL3
```

**Possible reason:**

You are using a web browser version that does not work here. Try another browser.

## 9.4 Error DFHWB0726

**Symptom:**

Following error occurs when trying to connect to CWS. SSL was not used in this case.

```
DFHWB0726 01/18/12 11:49:44 DBDCCICS CWXN CICS Web attach processing cannot link to
the analyzer user replaceable program. No analyzer specified. Host IP address:
9.152.86.91    . Client IP address: 9.152.222.71   .
          TCPIPSERVICE: NOSSL
```

**Possible reason:**

You did not specify an URM in the TCP/IP service definition.

When searching for DFHWB0726 via Google, you will find some more details on this error:

https://publib.boulder.ibm.com/infocenter/cicsts/v4r1/index.jsp?topic=%2Fcom.ibm.cics.ts.messages.doc%2Fcics_mc%2Fdfhwb%2FWB0726.html

## 9.5 Error DFHWB0732

**Symptom:**

Following error occurs when trying to connect to CWS via SSL.

```
DFHWB0732 01/18/12 12:53:12 DBDCCICS CWXN CICS Web attach processing encountered a
sockets I/O error while receiving a client request. Client IP address: 9.152.86.91
. Host IP address: 9.152.222.71   . TCPIPSERVICE: SSL1
```

**Possible reason:**

You did not specify ENCRYPTION=STRONG in DFHSITSP and you are using a Web browser that requires strong encryption (e.g. Firefox).

## 9.6 500 Internal server error on browser screen

**Symptom:**

On your browser screen you get CICS web support error 500 and following line appears on the VSE console:

```
F2 0115 DFHSO0113 DBDCCICS
        The IP address 9.152.222.71    cannot be resolved to a host name by
        the gethostbyaddr function.
```

**Possible reason:**

You did not define your client IP address as a symbolic name in TCP/IP. To resolve the problem add a DEFINE NAME statement like:

```
DEFINE NAME,NAME=SYSA,IPADDR=9.152.222.71
```

## 9.7 404 Program Not Found

**Symptom:**

Error “404 Program Not Found” is displayed on web browser.

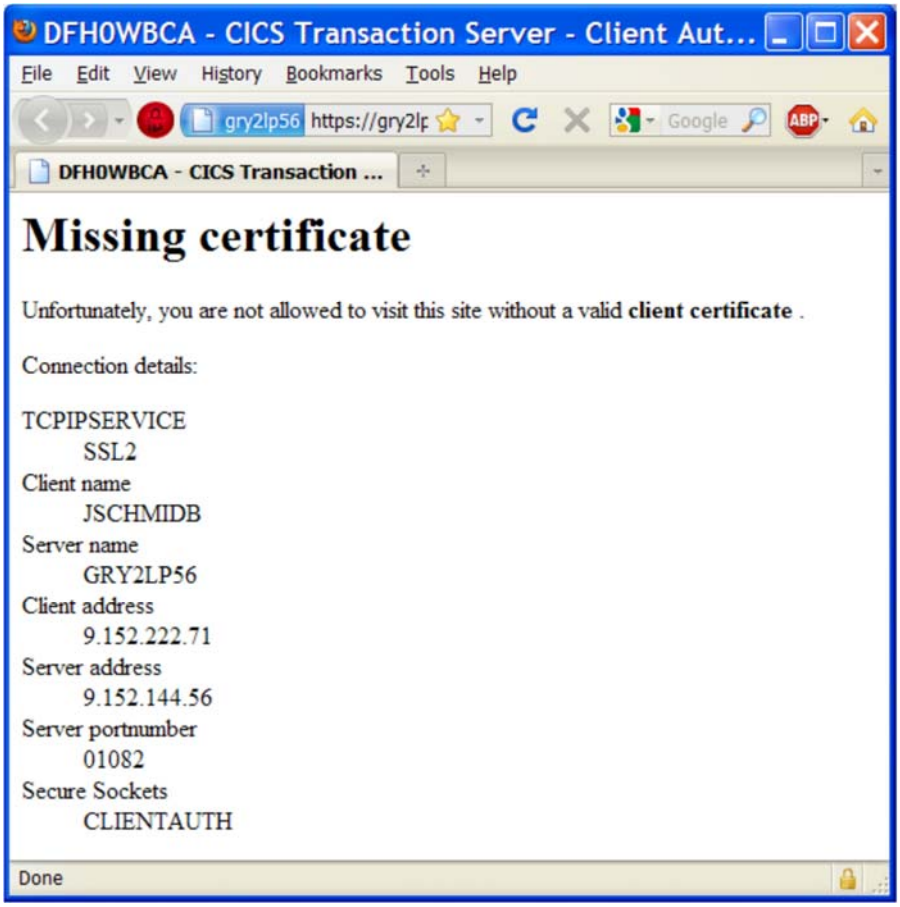
**Possible reason:**

Program DFH0WBCA is not defined in CICS or the DFH0WBCA phase is missing or cannot be found in the LIBDEF chain. You may also try a CEMT SET PROGRAM(DFH0WBCA) NEW.

## 9.8 Missing certificate

**Symptom:**

A web page similar to the following is displayed:




**Possible reason:**

You did not apply ZP15F498.

# 10 More information

You can find more information on the web pages below.

CICS Enhancements Guide, GC34-5763
http://www.ibm.com/servers/eserver/zseries/zvse/documentation/#cics

Redbook: Implementing CICS Web Services, SG24-7206
http://www.redbooks.ibm.com/abstracts/sg247206.html?Open

Redbook: CICS Transaction Server for VSE/ESA: CICS Web Support, SG24-5997
http://www.redbooks.ibm.com/abstracts/sg245997.html?Open

TCP/IP Optional Features (GPS, NFS, SSL, CAF, SecureFTP, and See-TCP/IP for VSE)
http://www.csi-international.com/download.htm

TCP/IP for VSE Commands Reference
http://www.csi-international.com/download.htm

Download Keyman/VSE from the VSE Internet homepage
http://www.ibm.com/servers/eserver/zseries/zvse/downloads/

### Further technical articles:

How to setup Secure FTP with VSE, Technical Article, downloadable as PDF from
http://www.ibm.com/servers/eserver/zseries/zvse/documentation/documents.html

How to setup Secure Telnet with VSE, Technical Article, downloadable as PDF from
http://www.ibm.com/servers/eserver/zseries/zvse/documentation/documents.html

How to setup cryptographic hardware for VSE, Technical Article, downloadable as PDF from
http://www.ibm.com/servers/eserver/zseries/zvse/documentation/documents.html

**If you are a Barnard Software Inc. customer:**

Redbook: Enhanced Networking on IBM z/VSE, SG24-8091
https://www.redbooks.ibm.com/abstracts/sg248091.html?Open