



**optiPoint 410/420 family**

**XML and/or IEEE 802.1x  
Certificate over secure link**

**Administration Manual**

**SIEMENS**

Global network of innovation



# Contents

|                                                        |            |
|--------------------------------------------------------|------------|
| <b>1 Introduction</b>                                  | <b>1-1</b> |
| 1.1 PRINCIPLE                                          | 1-2        |
| 1.2 What is needed                                     | 1-5        |
| <b>2 SETTING UP</b>                                    | <b>2-1</b> |
| 2.1 Installing the web server                          | 2-1        |
| 2.2 Installing a Certificate Authority                 | 2-3        |
| 2.2.1 Creating a server certificate request file (CSR) | 2-7        |
| 2.2.2 Signing the server certificate by the CA         | 2-15       |
| 2.2.3 Import and activate the Server certificate       | 2-18       |
| 2.3 Setup the phone for HTTPS connection               | 2-22       |
| 2.3.1 Check and test the HTTPS connection              | 2-24       |
| 2.4 802.1X certificates in the XML configuration files | 2-25       |
| <b>3 Abbreviations</b>                                 | <b>3-1</b> |



# 1 Introduction

This document is a description of how to implement and set up a secure environment, to provide the phones with configuration data by the use of XML files via secure Web server (Secure Configuration Download feature)

To provide secure connection to the Download Web Server, configuration data will be transferred using the HTTPS protocol instead of HTTP (or FTP). HTTPS runs HTTP over a TLS V1 (or SSL V3) connection, with all configuration data transferred in encrypted form. During the establishment of the connection the phone will authenticate the Download Web Server and the Download Web Server will authenticate the phone. This will use the mutual certificate based TLS authentication option. The phone and web server can also authenticate in a secure way without using the mutual certificate based TLS authentication option

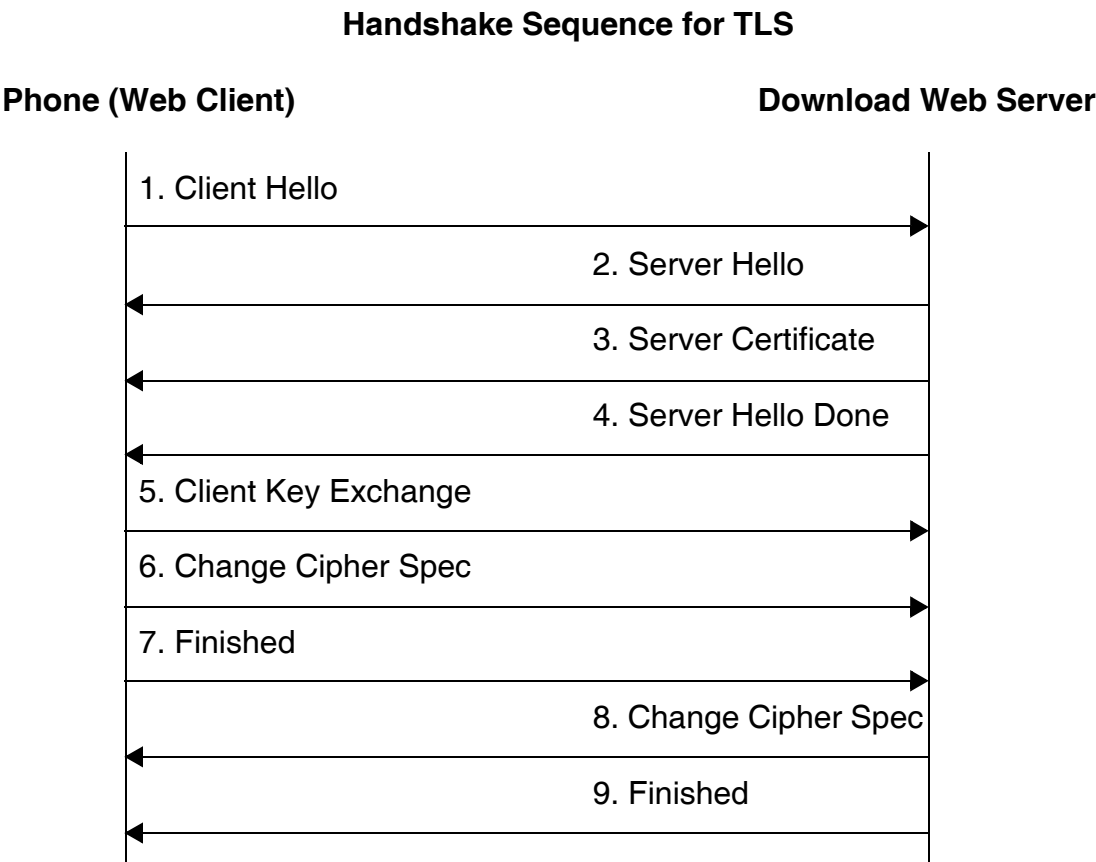
This document describes the needed steps and overall setup, to be able to configure all components for sending the XML configuration file, and if needed the 802.1X certificates over a secure connection to the phone.

This document is an supplementary document to the already existing documentation, please refer to the XML configuration manual for building XML configuration files.

1.1 PRINCIPLE

XML over secure link works on the same principle as XML over FTP (non secure). The only exception is that the data send between the two parties will be encrypted after that the two parties have authenticated each other. So if the data is captured in between this data cannot be read by the other parties.

The following diagram illustrates the stages in establishing a TLS connection from the phone to the secure web server in order to start the download of the requested XML files in a secure way.



In the “Client Hello” (step 1) the phone will offer to support TLS V1 or SSL V3 and will offer the following cipher suites that are already supported for encrypting signalling on the SIP interface:

- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_RSA\_3DES\_EDE\_CBC\_SHA
- TLS\_RSA\_DES\_CBC\_SHA

The Download Web Server selects TLS or SSL and one of the cipher suites for use in the “Server Hello” (step 2) in accordance with its policy.

In the “Server Certificate” (step 3) the server sends its self signed digital X.509 certificate to allow the phone to authenticate the server.

In the “Client Key Exchange” (step 5) the phone generates a symmetric session key (using the RSA method) and encrypts it with the server’s public key (taken from the server certificate) before sending it.

The “Change Cipher Spec” messages (steps 6 and 8) indicate that all future communications will be encrypted (using the established symmetric session key).

The TLS resume method is supported by the phone using the same session key for a follow-on TLS connection. A session key can only be re-used for a limited period, for a maximum amount of data transfer or until either end requires a new key to be negotiated. The server policy will determine whether use of the Resume method is permissible. The server may have scalability issues in storing the associated credentials for a large number of phones.

See compact line trace example:

| Source               | Destination          | Protocol | Info                                                                           |
|----------------------|----------------------|----------|--------------------------------------------------------------------------------|
| 498972213007.gvs.lab | securexml.gvs.lab    | TCP      | 1024 > https [SYN] Seq=0 Ack=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=11 TSER=0      |
| securexml.gvs.lab    | 498972213007.gvs.lab | TCP      | https > 1024 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=0 TSV=0 TSER=0 |
| 498972213007.gvs.lab | securexml.gvs.lab    | TCP      | 1024 > https [ACK] Seq=1 Ack=1 Win=8192 Len=0 TSV=11 TSER=0                    |
| 498972213007.gvs.lab | securexml.gvs.lab    | TLS      | Client Hello                                                                   |
| securexml.gvs.lab    | 498972213007.gvs.lab | TLS      | Server Hello, Certificate, Server Hello Done                                   |
| 498972213007.gvs.lab | securexml.gvs.lab    | TCP      | 1024 > https [ACK] Seq=61 Ack=888 Win=8192 Len=0 TSV=12 TSER=70086061          |
| 498972213007.gvs.lab | securexml.gvs.lab    | TLS      | Client Key Exchange                                                            |
| securexml.gvs.lab    | 498972213007.gvs.lab | TCP      | https > 1024 [ACK] Seq=888 Ack=200 Win=65336 Len=0 TSV=70086064 TSER=12        |
| 498972213007.gvs.lab | securexml.gvs.lab    | TLS      | Change Cipher Spec, Encrypted Handshake Message                                |
| securexml.gvs.lab    | 498972213007.gvs.lab | TLS      | Change Cipher Spec, Encrypted Handshake Message                                |
| 498972213007.gvs.lab | securexml.gvs.lab    | TLS      | Application Data                                                               |
| securexml.gvs.lab    | 498972213007.gvs.lab | TCP      | https > 1024 [ACK] Seq=931 Ack=297 Win=65239 Len=0 TSV=70086066 TSER=12        |
| 498972213007.gvs.lab | securexml.gvs.lab    | TLS      | Application Data                                                               |
| securexml.gvs.lab    | 498972213007.gvs.lab | TLS      | Application Data                                                               |
| securexml.gvs.lab    | 498972213007.gvs.lab | TCP      | https > 1024 [FIN, ACK] Seq=2005 Ack=363 Win=65173 Len=0 TSV=70086067 TSER=12  |
| 498972213007.gvs.lab | securexml.gvs.lab    | TCP      | 1024 > https [ACK] Seq=363 Ack=2006 Win=7118 Len=0 TSV=12 TSER=70086067        |
| 498972213007.gvs.lab | securexml.gvs.lab    | TCP      | 1024 > https [FIN, ACK] Seq=363 Ack=2006 Win=8192 Len=0 TSV=13 TSER=70086067   |
| securexml.gvs.lab    | 498972213007.gvs.lab | TCP      | https > 1024 [ACK] Seq=2006 Ack=364 Win=65173 Len=0 TSV=70086067 TSER=13       |
| 498972213007.gvs.lab | securexml.gvs.lab    | TCP      | 1025 > https [SYN] Seq=0 Ack=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=13 TSER=0      |



# Introduction

## PRINCIPLE

| Source               | Destination          | Protocol | Info                                                                           |
|----------------------|----------------------|----------|--------------------------------------------------------------------------------|
| securexml.gvs.lab    | 498972213007.gvs.lab | TCP      | https > 1025 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=0 TSV=0 TSER=0 |
| 498972213007.gvs.lab | securexml.gvs.lab    | TCP      | 1025 > https [ACK] Seq=1 Ack=1 Win=8192 Len=0 TSV=13 TSER=0                    |
| 498972213007.gvs.lab | securexml.gvs.lab    | TLS      | Client Hello                                                                   |
| securexml.gvs.la     | 498972213007.gvs.lab | TLS      | Server Hello, Change Cipher Spec, Encrypted Handshake Message                  |
| 498972213007.gvs.lab | securexml.gvs.lab    | TLS      | Change Cipher Spec                                                             |
| securexml.gvs.lab    | 498972213007.gvs.lab | TCP      | https > 1025 [ACK] Seq=123 Ack=99 Win=65437 Len=0 TSV=70086071 TSER=13         |
| 498972213007.gvs.lab | securexml.gvs.lab    | TLS      | Encrypted Handshake Message, Application Data, Application Data                |
| securexml.gvs.lab    | 498972213007.gvs.lab | TCP      | [TCP segment of a reassembled PDU]                                             |
| securexml.gvs.lab    | 498972213007.gvs.lab | TCP      | [TCP segment of a reassembled PDU]                                             |
| securexml.gvs.lab    | 498972213007.gvs.lab | TCP      | [TCP segment of a reassembled PDU]                                             |
| securexml.gvs.lab    | 498972213007.gvs.lab | TCP      | [TCP segment of a reassembled PDU]                                             |
| 498972213007.gvs.lab | securexml.gvs.lab    | TCP      | 1025 > https [ACK] Seq=268 Ack=4503 Win=8192 Len=0 TSV=13 TSER=70086071        |
| securexml.gvs.lab    | 498972213007.gvs.lab | TLS      | Application Data                                                               |
| 498972213007.gvs.lab | securexml.gvs.lab    | TCP      | 1025 > https [ACK] Seq=268 Ack=5076 Win=7620 Len=0 TSV=13 TSER=70086071        |
| 498972213007.gvs.lab | securexml.gvs.lab    | TCP      | 1025 > https [FIN, ACK] Seq=268 Ack=5076 Win=8192 Len=0 TSV=13 TSER=70086071   |
| securexml.gvs.lab    | 498972213007.gvs.lab | TCP      | https > 1025 [ACK] Seq=5076 Ack=269 Win=65268 Len=0 TSV=70086071 TSER=13       |



## **1.2 What is needed**

Before you can provide the phones configuration items over a secure link, you need to have or install at least the following components and or software packages. Under the chapter → SETTING UP you find some more information and screenshots of this specific item.

### **1. The server**

There are no special server requirements, please refer to the requirements of the software packages you choose to setup your environment.

### **2. Web server**

As web server you can take any application who support secure web services, the web server must support the standard protocols: TCP, TLS, HTTP over TLS (HTTPS), X.509 certificates and XML. However, the XML schema used is proprietary; please refer to the XML configuration manual for building a XML configuration file.

In this example we use the Microsoft Internet Information Server (IIS) installed on a Windows 2003 server.



In case you want to install the Microsoft CA (see below) It is important that you install the IIS software **BEFORE** the Certificate Authority software package.

In case you want to install an apache web server, or other similar web servers you probably don't need to install the Microsoft CA (please refer to the individual documentations)

## Introduction

*What is needed*

### 3. Installing a Certificate Authority

To be able to setup a secure web server, the web server needs a root- and server certificate which can be created and signed by a trusted authority, or by use of some applications e.g. "Open SSL". Creating and signing certificates by official trusted authority's not free of charge. However you can choose to create your own private root- and server certificate, there are many applications available to do this (e.g. Open SSL).

In this example we use the Microsoft Certificate Authority (CA) which we installed on the same server as the IIS.



If CA is installed after IIS then the CA will add the necessary add on to enable the `http://[IP addr.]/certsrv` access.

### 4. Creating a server certificate request file.

Depending on the used web server service or application, the procedure of how to create a certificate request can be totally different.

In this example we show the procedure of how to create the request file within the previous installed IIS.

### 5. Signing the server certificate by the CA

The certificate request file needs to be signed, this can be done by an official authority or by use of a private root- and server certificate. In this example we use the Microsoft CA to sign the certificate request.

### 6. Import and activate the Server certificate

Once you received the certificate from a official authority or created your own, then you just need to import and activate this certificate.

### 7. Setup the phone for HTTPS connection

On the phone you must configure the needed parameters to connect to the secure web server either via the GUI, or over the web interface of the phone.

It is also possible to send the secure web server address to the phone by use of a DHCP server (vendor specific information element), in this case it is best to name the XML files on the secure web server as defined standard by the phones. The example below shows the configuration via web interface.

### 8. Check and test the HTTPS connection

To be sure that the web server sends the requested file to the phone, or to verify the contents of the XML files, you can simply use a web browser to do this. The web browser however must support XML.

## **9. 802.1X certificates in the XML configuration files**

In case that the phone needs 802.1X authentication, is it possible to send the needed 802.1X server- and client certificates to the phone via the XML configuration file(s). This allows the phone to response at the 802.1X request from the Layer 2 switch, and to negotiate with radius server to obtain a released port on the Layer 2 switch. The server Radius server CA certificate is stored in the XML file in PEM format, and the client certificate is stored in binary 64 format with pass phrase protection (B64). In the XML file(S) those certificates are XML items like all other items. Cut and paste has to be used to create the data in the XML write items: "802.1x-certificate" and "radius-server-ca1".

Please refer to the „IEEE 802.1x Configuration Management“ Administration Manual “A31003-J4200-M100-\* -76A9.pdf” for more information about 802.1X Authentication.



In SIP version 6.0.xx it is not possible to sent the Pass Phrase to the phone as a XML item, for that reason must the certificates be encoded with a specific pass phrase which is only known by some Siemens personal members.

In case that the content of the “**system OR device-config-version**” item changes (Example from 1 to 2) the phone will reboot every time regardless of what item is changed. This is because of the certificate included in the XML file E. g.

```
<Item name="system-config-version">1</Item>
```

## **Introduction**

*What is needed*

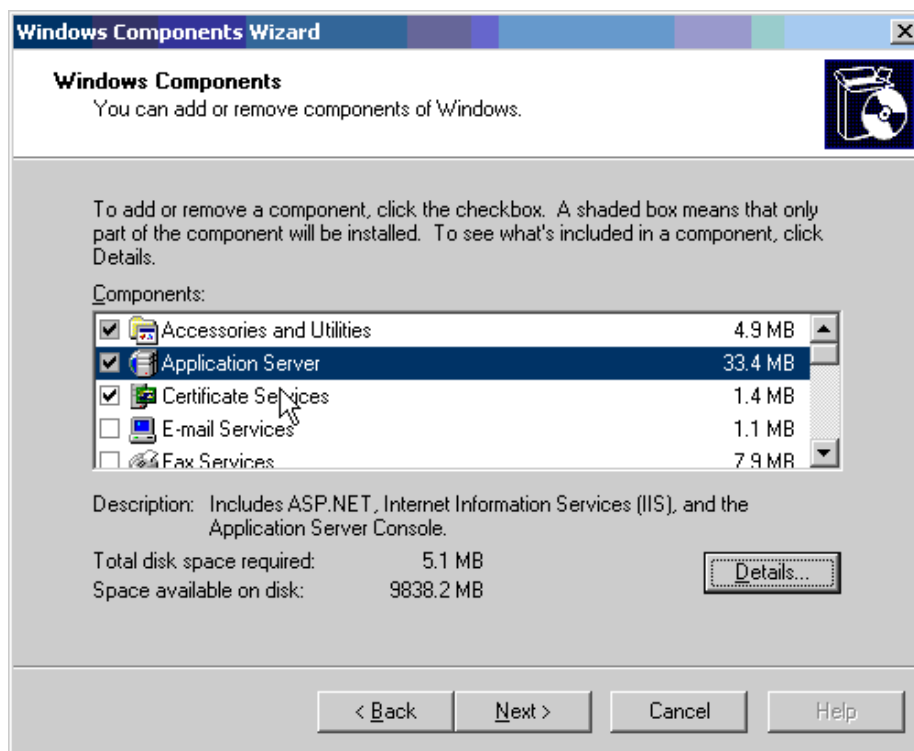
## 2 SETTING UP

### 2.1 Installing the web server

IIS is an additional package that can be installed Windows CD. Launch to the “**Control Panel**” and select “**Add or Remove Programs**” and then select the option “**Add/Remove Windows Components**”, from the list select “Internet Information Services”.



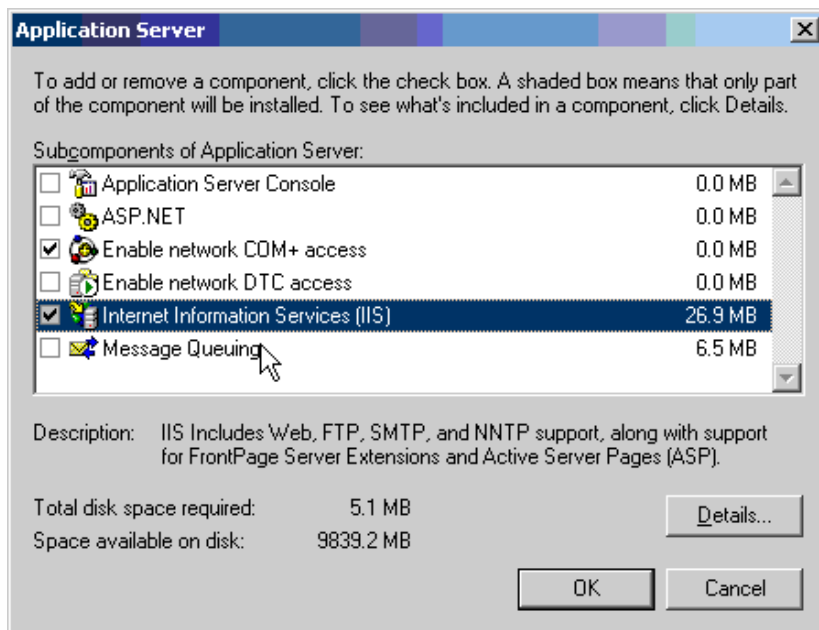
Depending on the Windows version the location of the IIS can differ, either the IIS can be found directly, or under the group “Application Group” (see below).



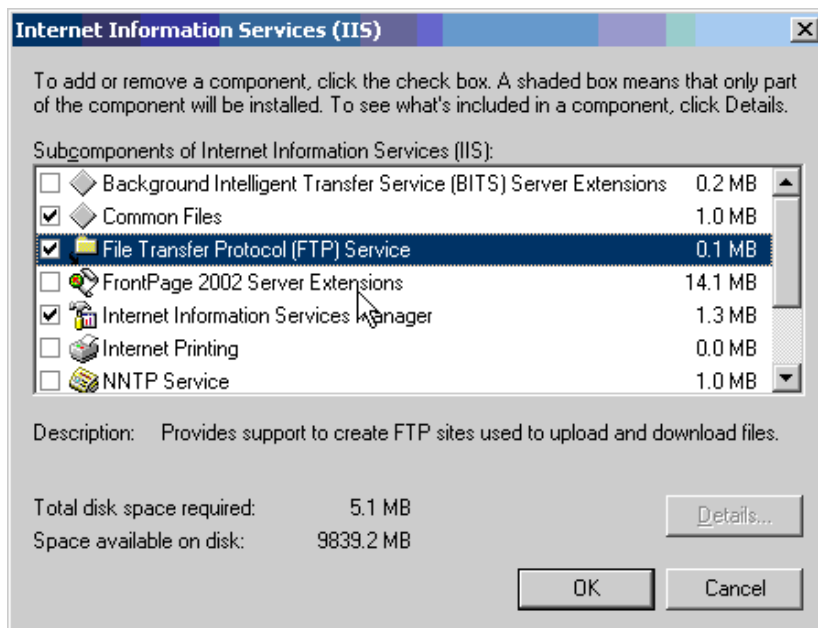
In the main mask of the “**Windows Components Wizard**” select “**Application Server**” and Click on “**Details**” => go to next screen.

## SETTING UP

### *Installing the web server*



In the detailed list select **“Internet Information Services”** and here again **“Details”** => go to next screen.



Select here at least **“Internet Information Services Manager”**, the **“File Transfer Protocol”** is not needed to let your web server function for the **Secure Download**.

The FPT application can eventually be useful to use as web server for the phones, e.g. music on hold file, save IINI file etc.

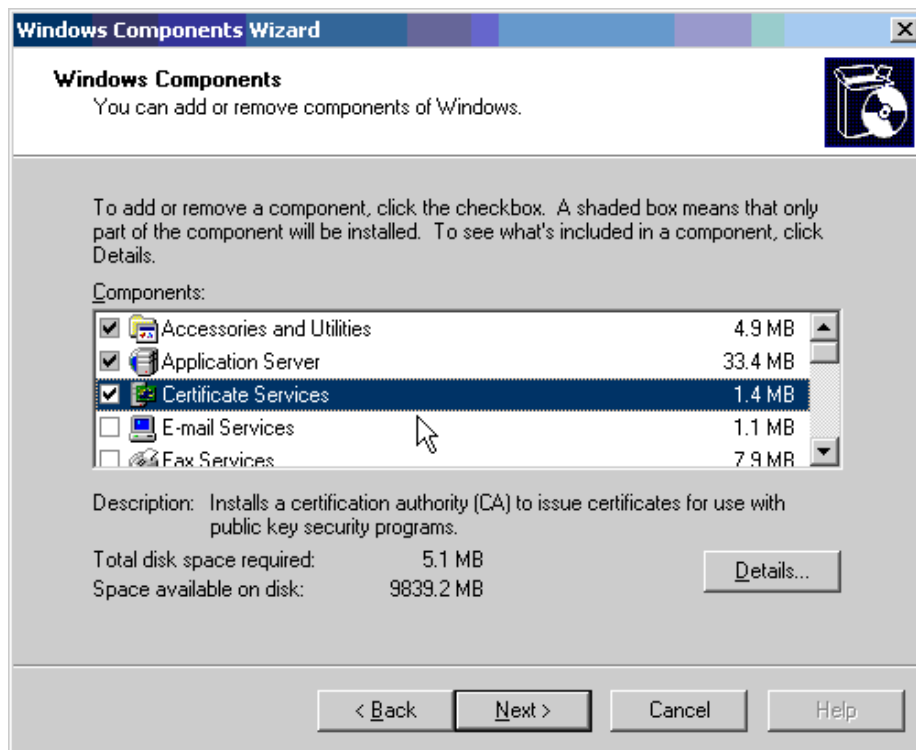
Click **“OK”** to finish the IIS installation

## 2.2 Installing a Certificate Authority

Certificate Authority (CA) is an additional package that can be installed Windows CD. Launch to the “**Control Panel**” and select “**Add or Remove Programs**” and then select the option “**Add/Remove Windows Components**”, from the list select “**Certificate Authority**”.



CA is only available on Windows Sever versions. This CA will be installed as a root standalone CA.

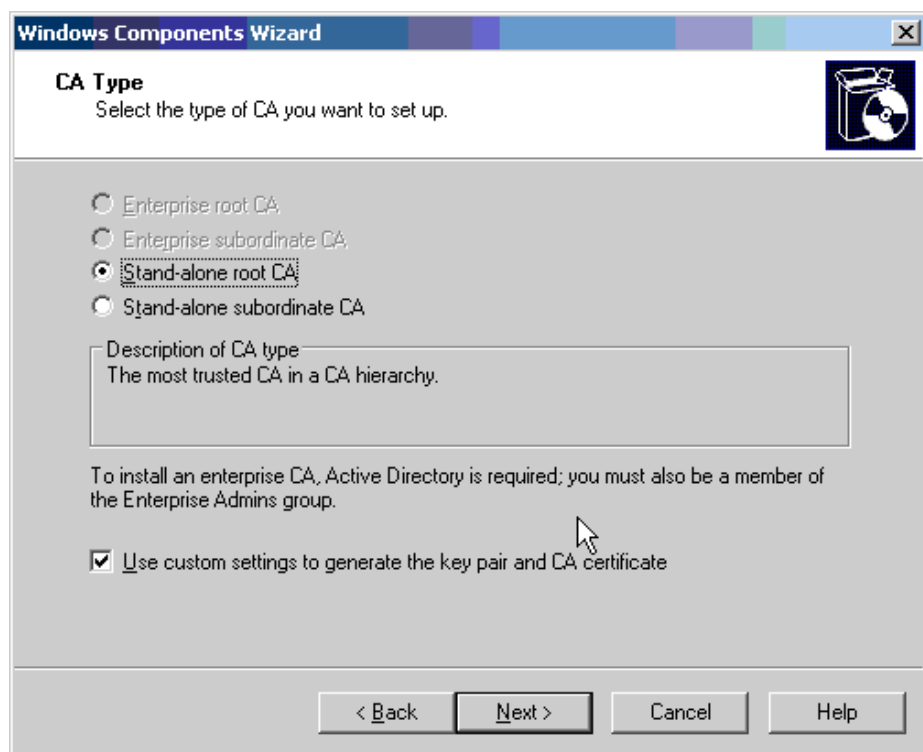


In the main mask of the “**Windows Components Wizard**” select “**Certificate Services**” and => go to next screen.

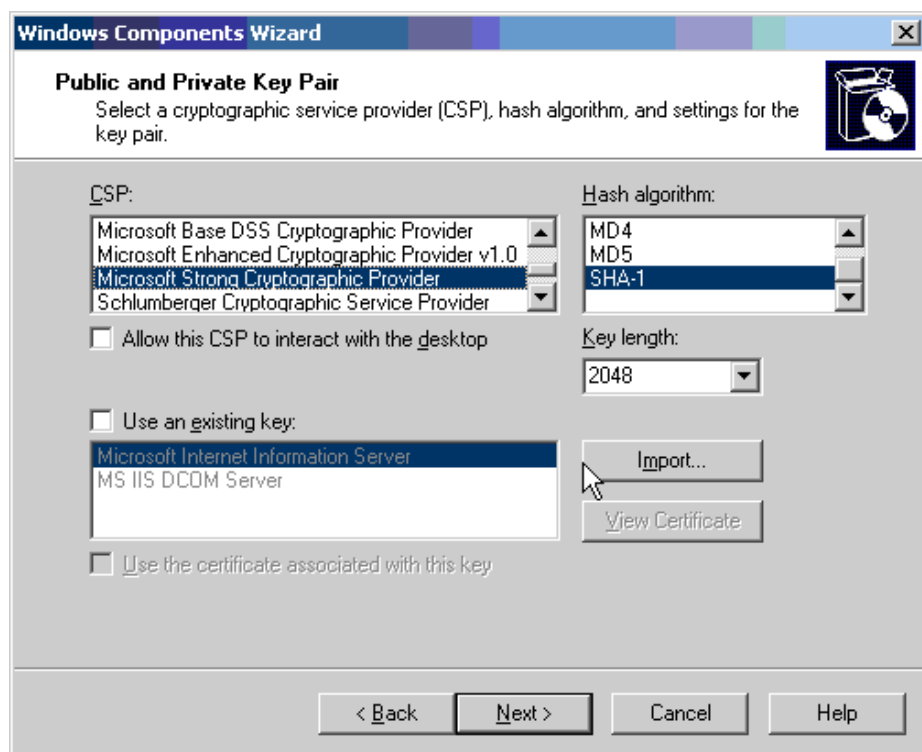


## SETTING UP

### Installing a Certificate Authority



Select here the option “**Stand-alone root CA**” and activate the option to generate the key pair and CA certificate. and => go to next screen.



Set the requested parameters as shown in the above screen. The length of the shortened if wanted.

The screenshot shows the 'CA Identifying Information' window of the Windows Components Wizard. The title bar reads 'Windows Components Wizard'. The window has a blue header with the title and a close button. Below the header, the title 'CA Identifying Information' is followed by the instruction 'Enter information to identify this CA.' and a CD icon. The main area contains several input fields: 'Common name for this CA:' with the text 'PhoneXML'; 'Distinguished name suffix:' with an empty field; 'Preview of distinguished name:' with the text 'CN=PhoneXML'; 'Validity period:' with a dropdown set to '5' and 'Years'; and 'Expiration date:' with the text '29.05.2011 01:32'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. A mouse cursor is pointing at the 'Next >' button.

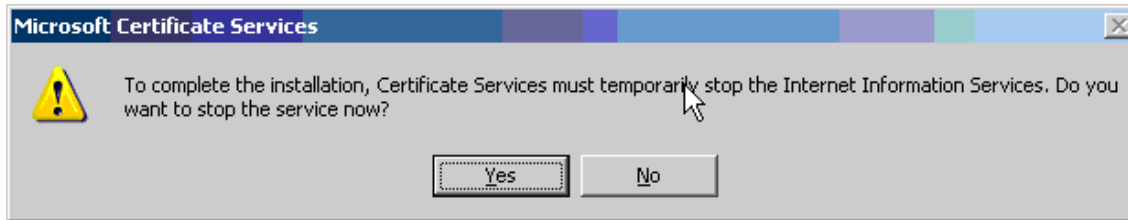
Administrate a common name and the validly period for your CA => go to next screen.

The screenshot shows the 'Certificate Database Settings' window of the Windows Components Wizard. The title bar reads 'Windows Components Wizard'. The window has a blue header with the title and a close button. Below the header, the title 'Certificate Database Settings' is followed by the instruction 'Enter locations for the certificate database, database log, and configuration information.' and a CD icon. The main area contains several input fields and checkboxes: 'Certificate database:' with the text 'C:\WINDOWS\system32\CertLog' and a 'Browse...' button; 'Certificate database log:' with the text 'C:\WINDOWS\system32\CertLog' and a 'Browse...' button; a checked checkbox 'Store configuration information in a shared folder' with a 'Shared folder:' field containing 'C:\CAConfig' and a 'Browse...' button; and an unchecked checkbox 'Preserve existing certificate database'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. A mouse cursor is pointing at the 'Next >' button.

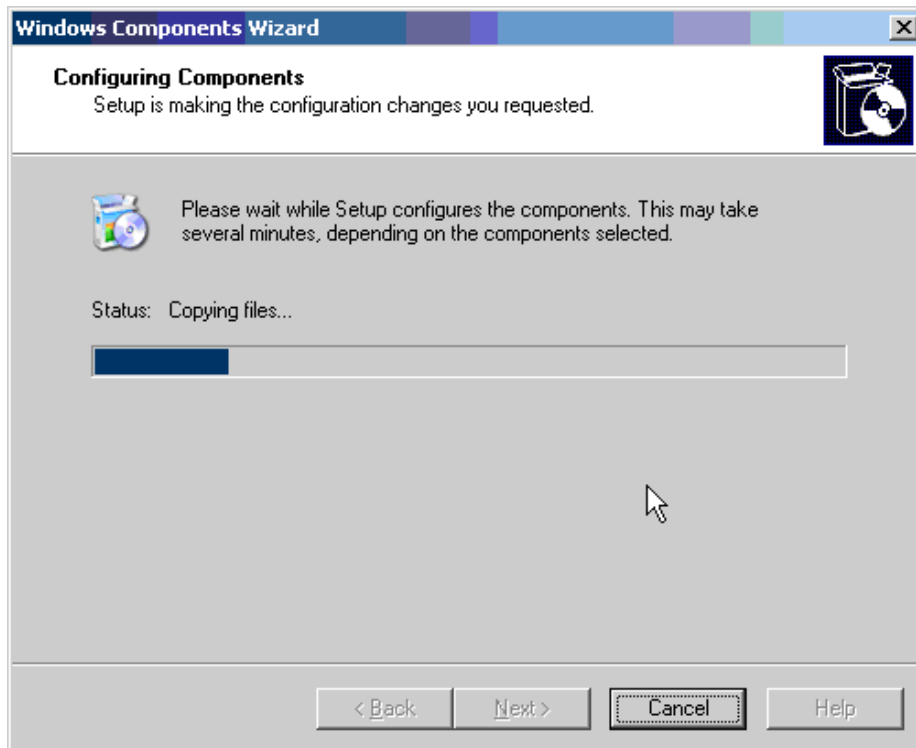
## SETTING UP

### *Installing a Certificate Authority*

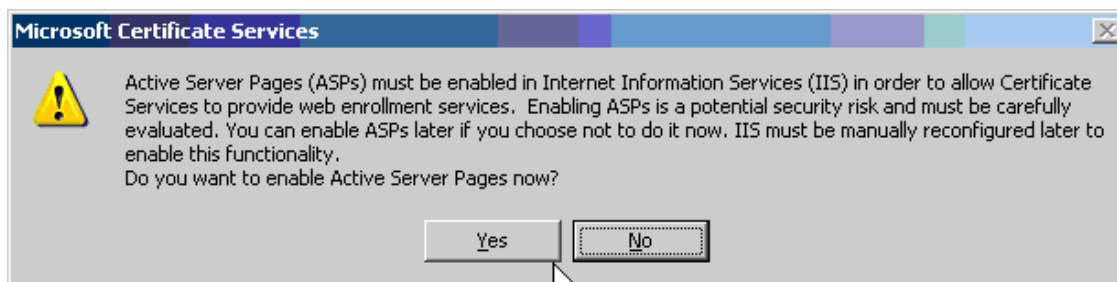
If desired you can change the locations for the database file and others. => go to next screen.



Just click **"Yes"** here



All needed files will be installed



Select **"Yes"** to activate the Active Server Pages.



Click **“Finish”**

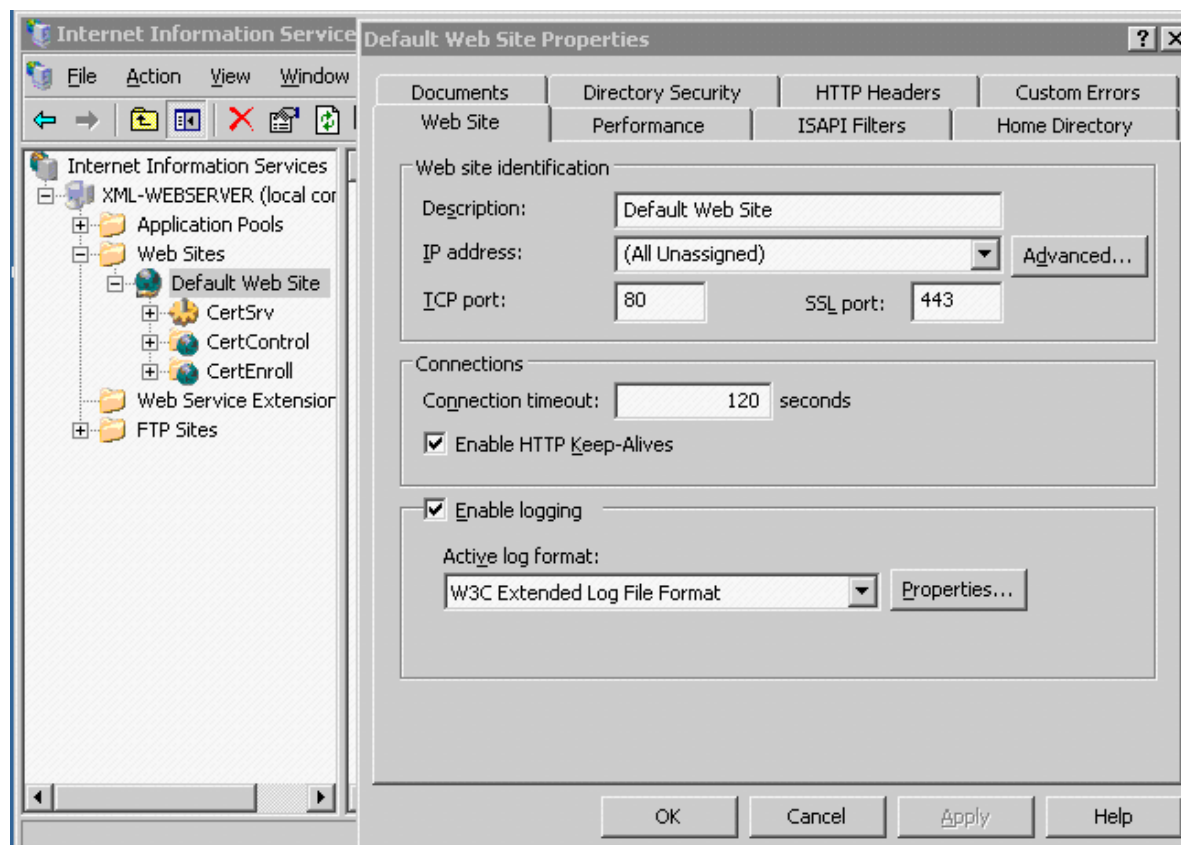
### **2.2.1 Creating a server certificate request file (CSR).**

In this example no separate web site is build, we used the default web site in our example, if you want you can of course first create a new web site and then execute all steps from your created website.

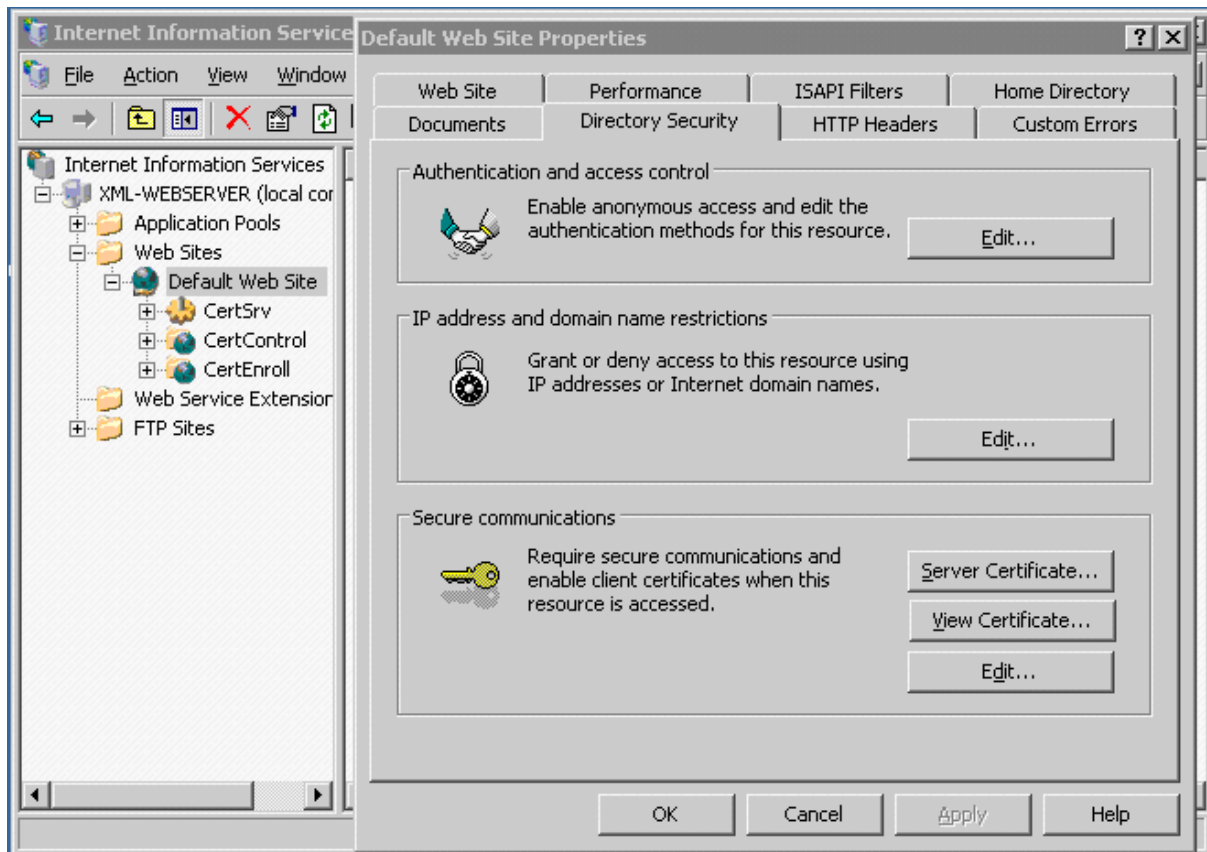
Launch to the IIS application and highlight the requested web site (default web site in example), from there select **“Properties”** by clicking right mouse.

## SETTING UP

### *Installing a Certificate Authority*



In the “**Web Site**” tab of the properties page administrate the port number you want to use for “**SSL port**”, Standard secure web server port is “443”. If you want you can also deactivate the “**TCP port**”



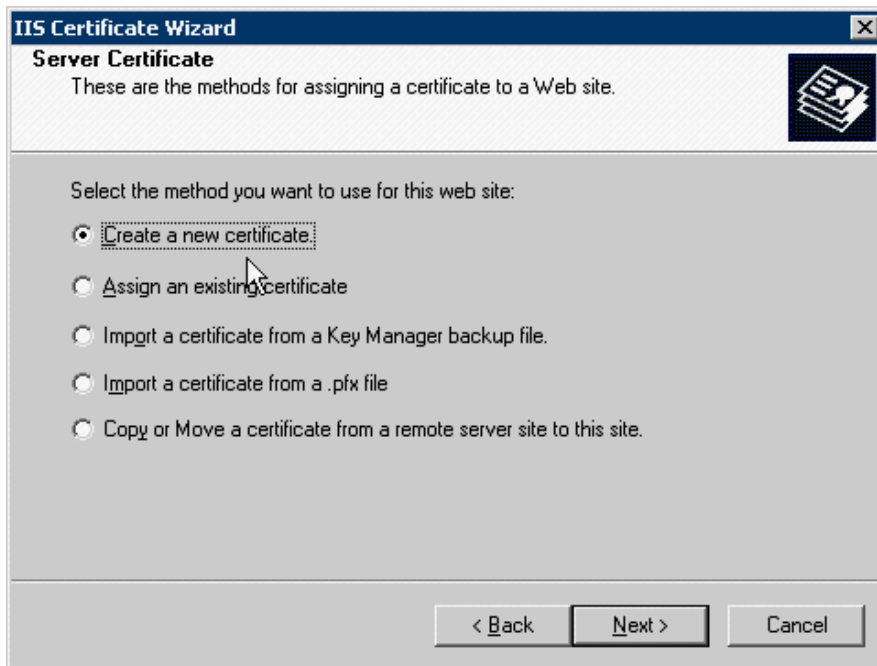
In the **“Web Site”** tab of the properties page click on the **“Server Certificate”** button.



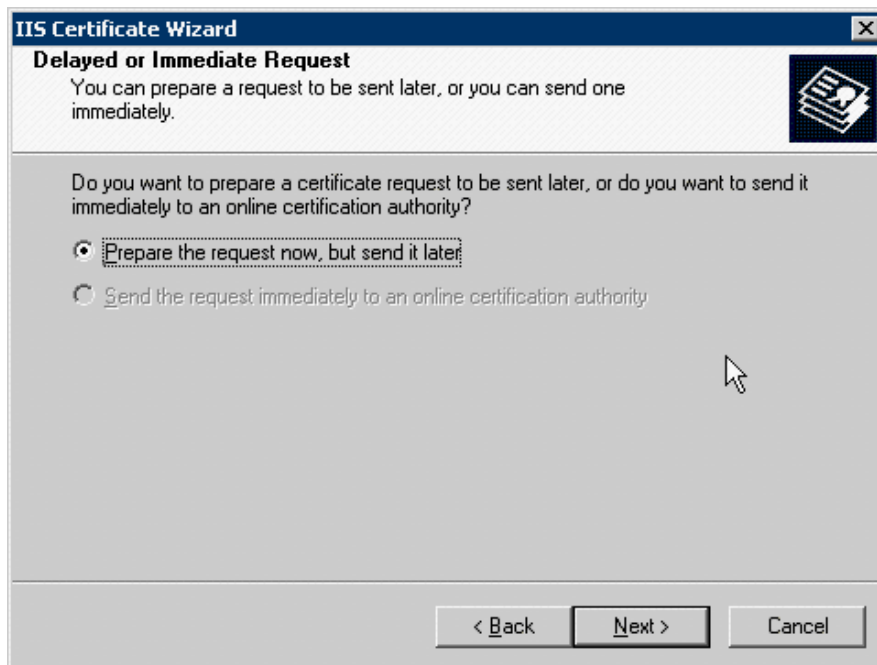
Click **“Next”** to start the Certificate Wizard

## SETTING UP

### *Installing a Certificate Authority*

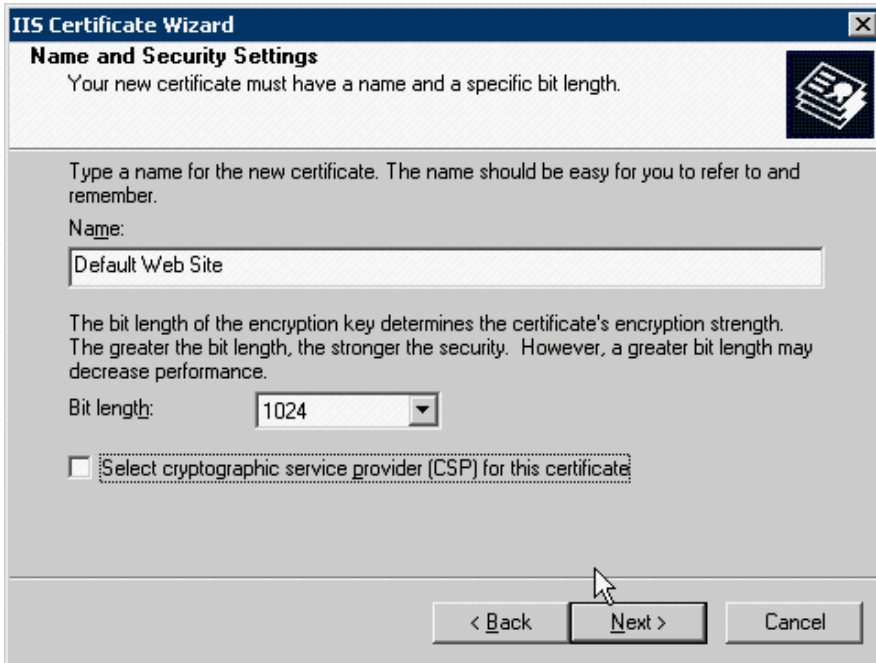


Select the **“Create a new certificate”** option here.



Select the **“Prepare the request now, but send it later”** option here. => click next





**IIS Certificate Wizard**

**Name and Security Settings**

Your new certificate must have a name and a specific bit length.

Type a name for the new certificate. The name should be easy for you to refer to and remember.

Name:

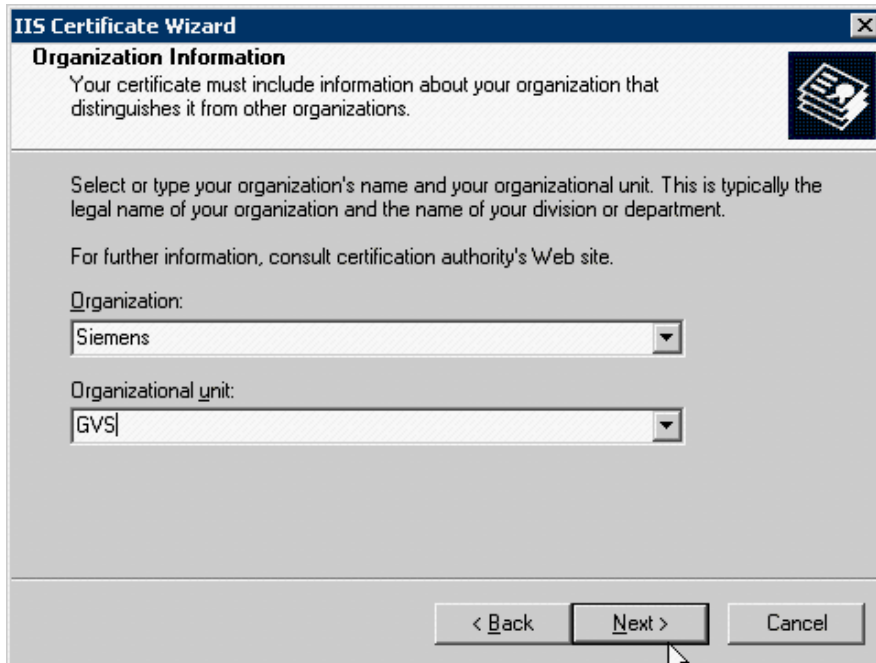
The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Bit length:

☐ Select cryptographic service provider (CSP) for this certificate

< Back   Next >   Cancel

Define the name of your certificate and the length of the key. => Click Next.



**IIS Certificate Wizard**

**Organization Information**

Your certificate must include information about your organization that distinguishes it from other organizations.

Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.

For further information, consult certification authority's Web site.

Organization:

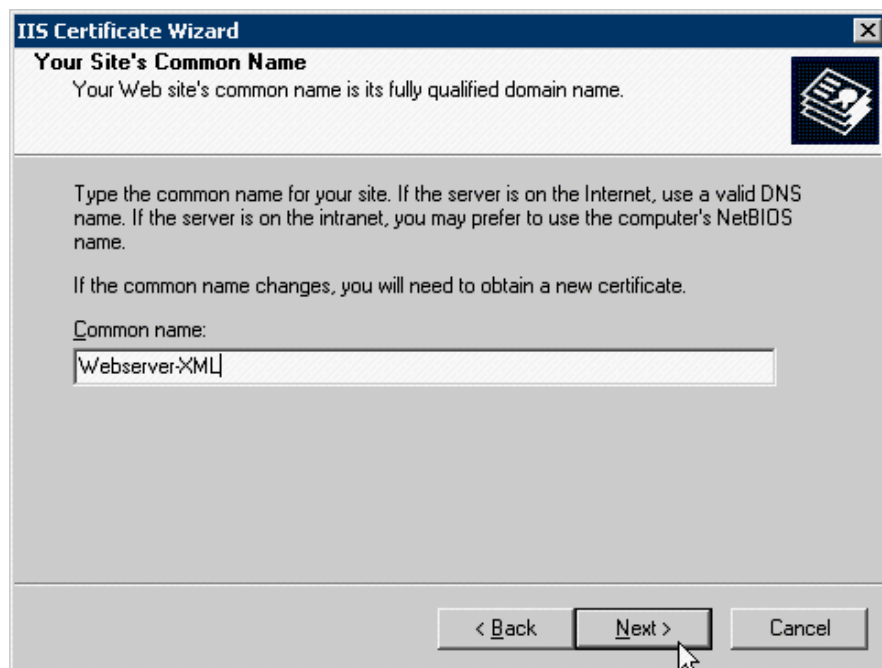
Organizational unit:

< Back   Next >   Cancel

Administrate the “**Organization**” and “**Organization unit**”. => Click Next.

## SETTING UP

### *Installing a Certificate Authority*



**IIS Certificate Wizard**

**Your Site's Common Name**  
Your Web site's common name is its fully qualified domain name.

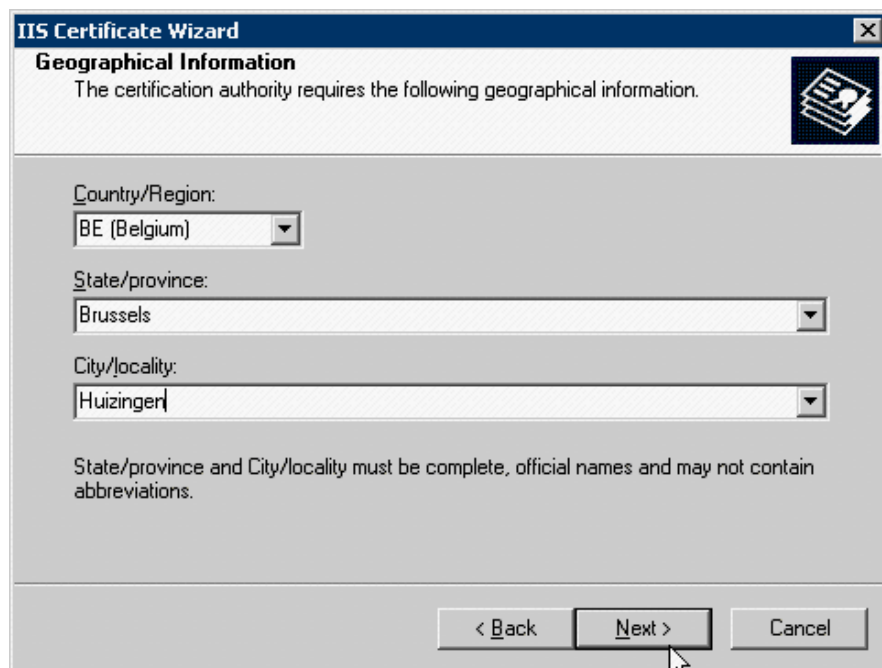
Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.

If the common name changes, you will need to obtain a new certificate.

Common name:

< Back   **Next >**   Cancel

Administrate the “**Common name**” => Click Next.



**IIS Certificate Wizard**

**Geographical Information**  
The certification authority requires the following geographical information.

Country/Region:

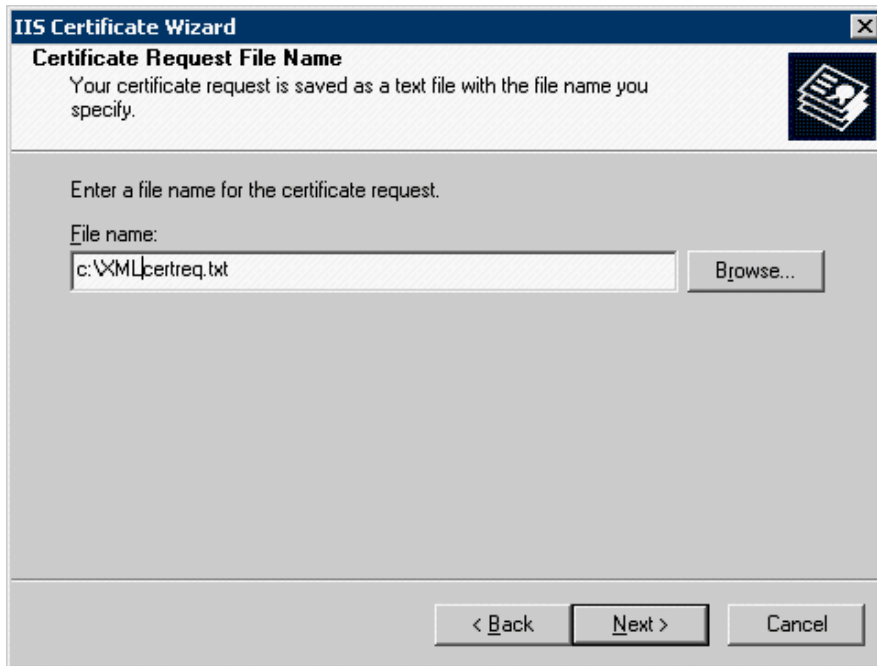
State/province:

City/locality:

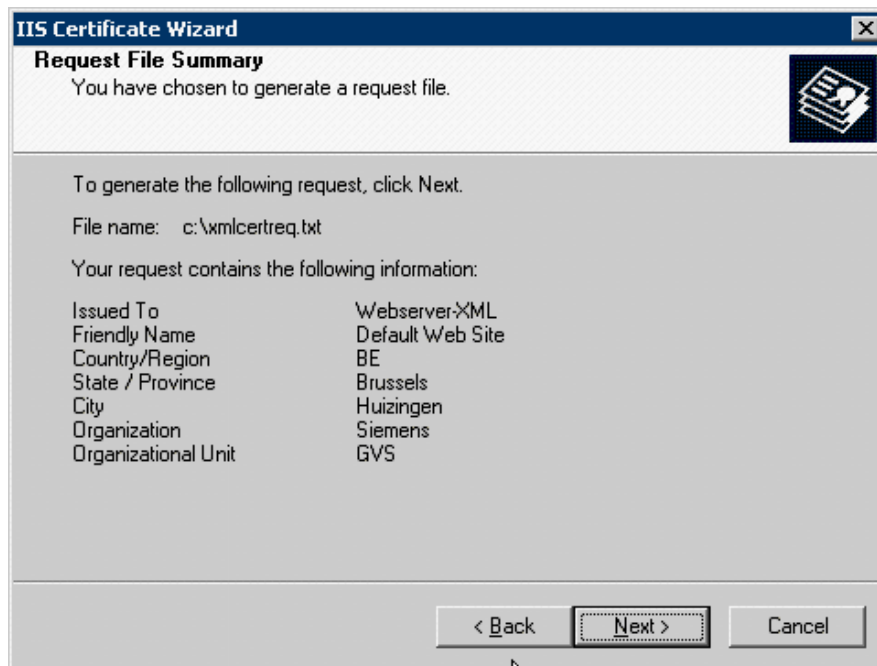
State/province and City/locality must be complete, official names and may not contain abbreviations.

< Back   **Next >**   Cancel

Administrate the “**Country**” and “**State**” and “**City**”. => Click Next.



Administrate the destination path and file name of your request file => Click Next.



Check the parameters, and if all is ok => Click Next, otherwise go back and correct.

## Installing a Certificate Authority

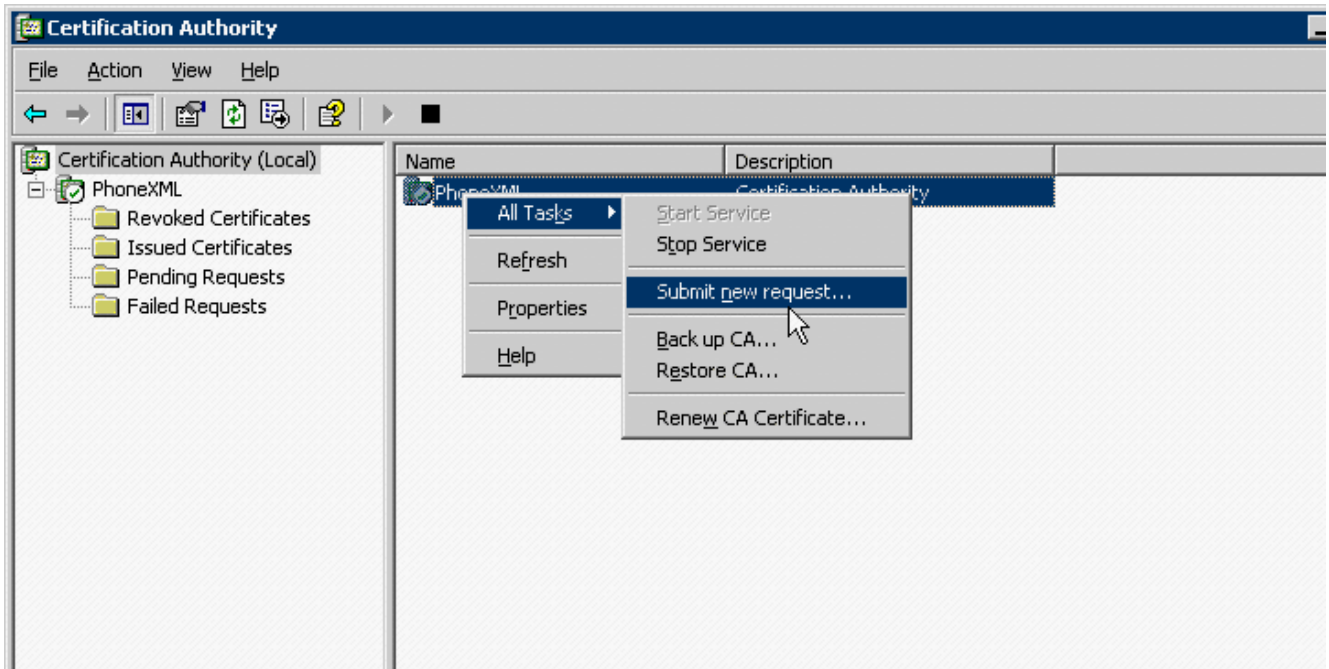


See an example of the contents of such a request file.

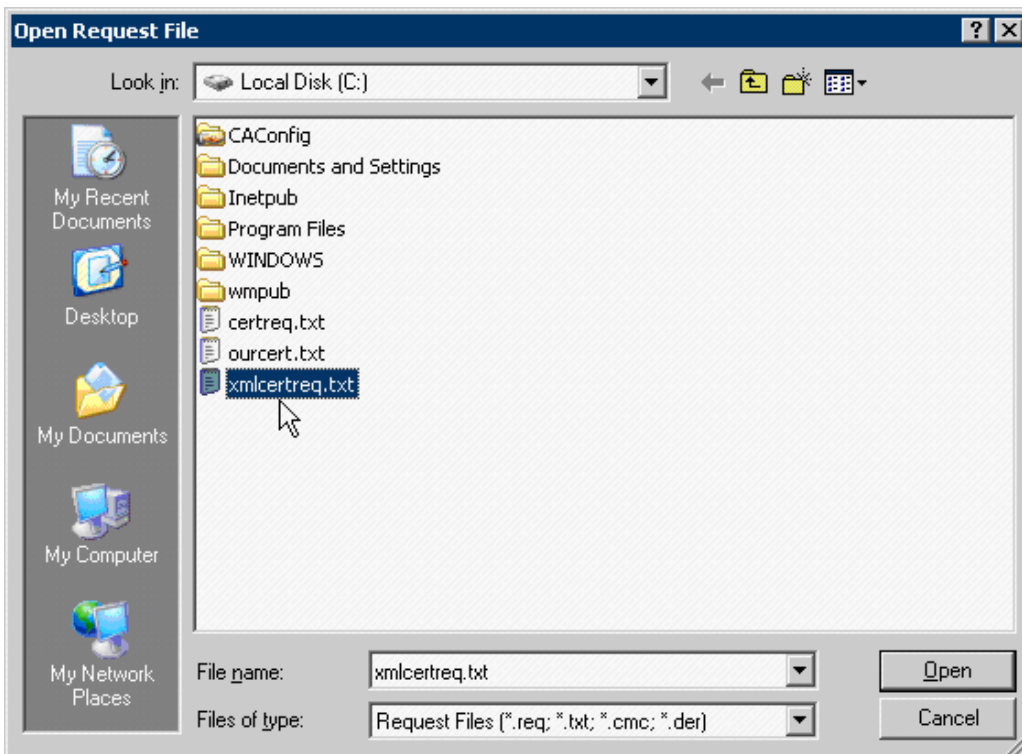
**2-14**

## 2.2.2 Signing the server certificate by the CA

Launch to the CA



In the right panel select the root CA, right click on the “**Phone XML**” and select “**All Tasks**” => “**Submit new request**”.



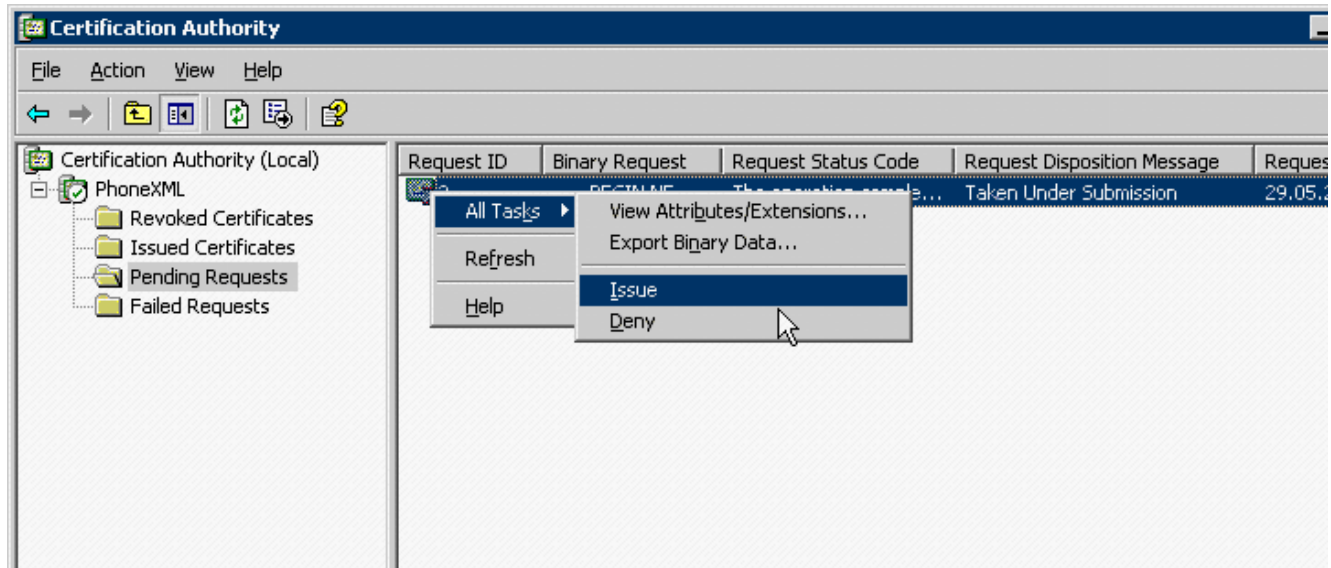
## SETTING UP

### Installing a Certificate Authority

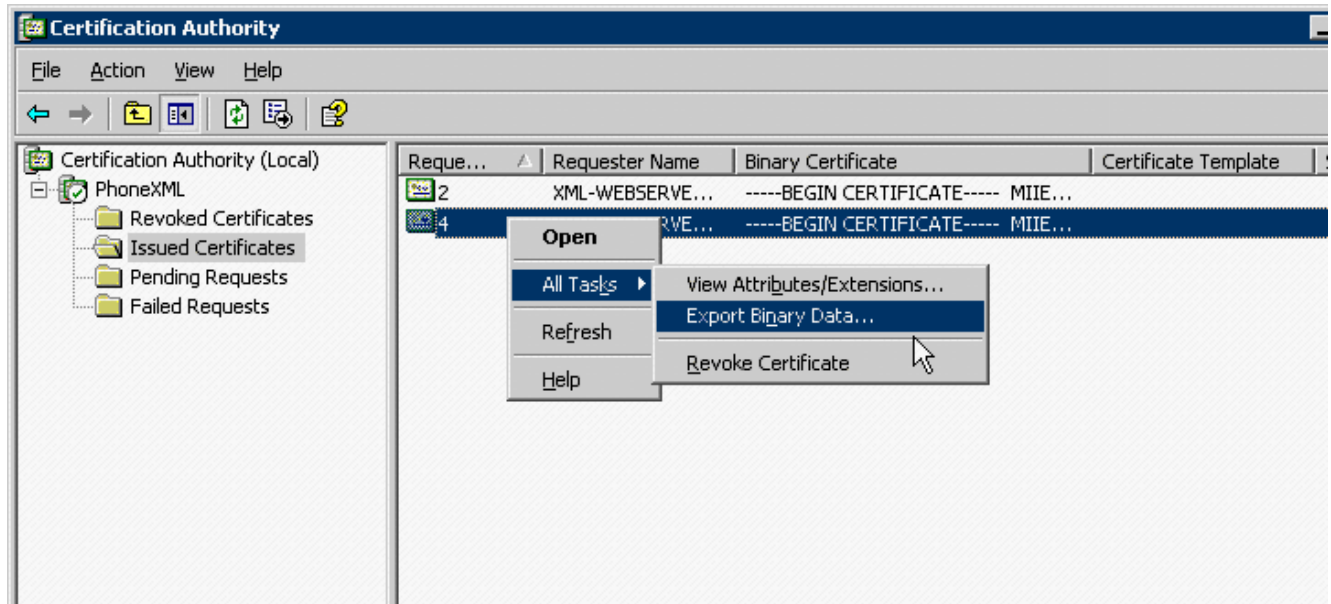
Launch to the CA request file and press “open”



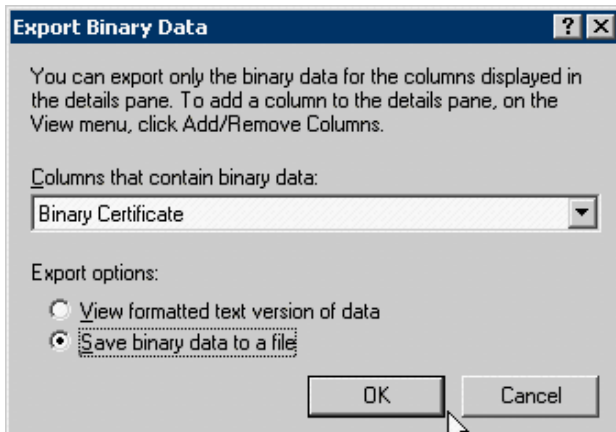
The “xmlcertreq.txt” file is the request file previous created in IIS



Once the request file is imported select “**Pending Request**” in the left panel, this will list the previous imported request. On the right panel select your request and choose “**All Tasks**” by pressing right mouse and select “**Issue**”



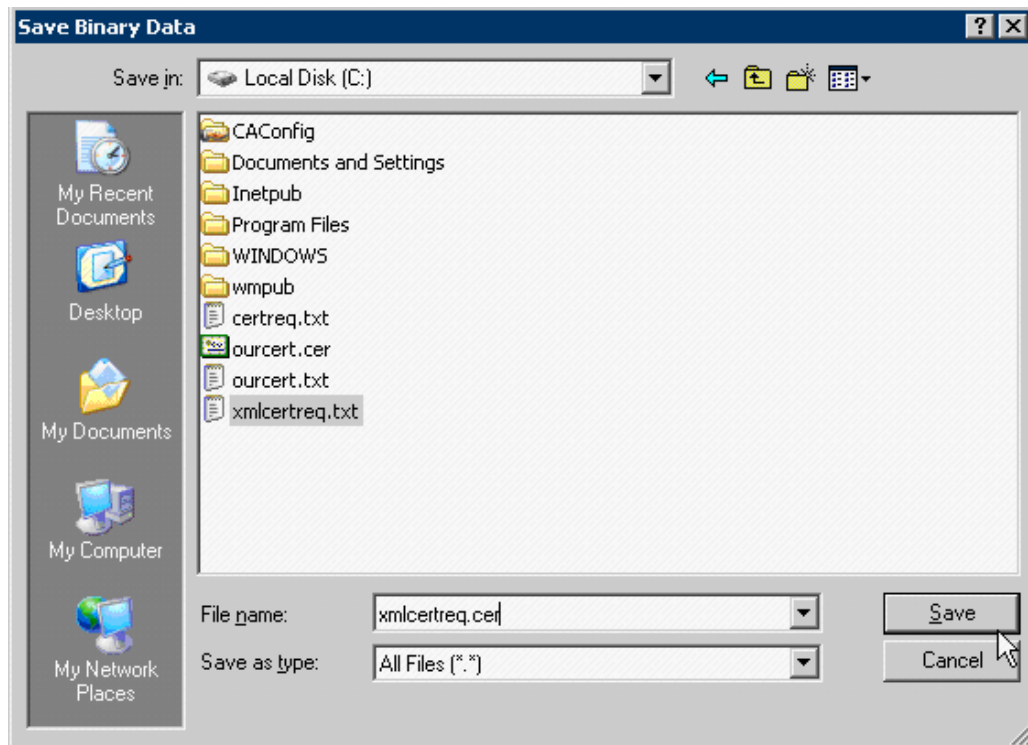
After the request file is issued select “**Issued Certificates**” in the left panel, this will list the issued certificates. On the right panel select your certificate and choose “**All Tasks**” by pressing right mouse and select “**Export Binary Data**”



Here choose the “**Binary Certificate**” and “save this to binary file.”



If wanted you can also view the certificate by selecting the option “**View formatted text version of data**”.



Launch to the directory where you want to save your exported certificate and save this certificate.



Use as extension of your file “**cer**”, this is the standard extension for certificates files.

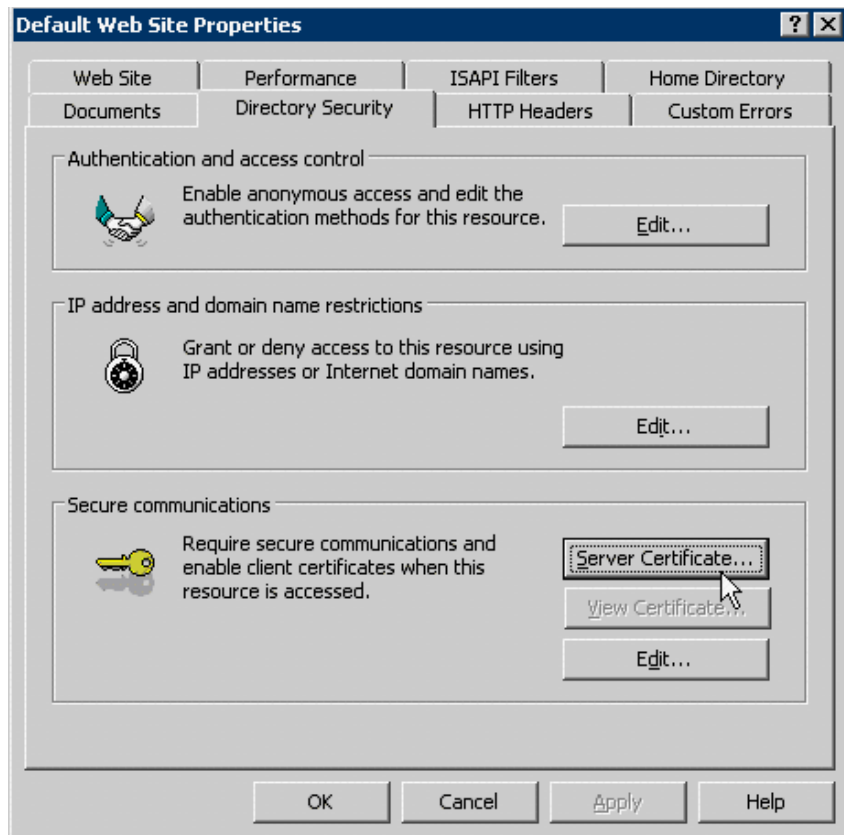


## SETTING UP

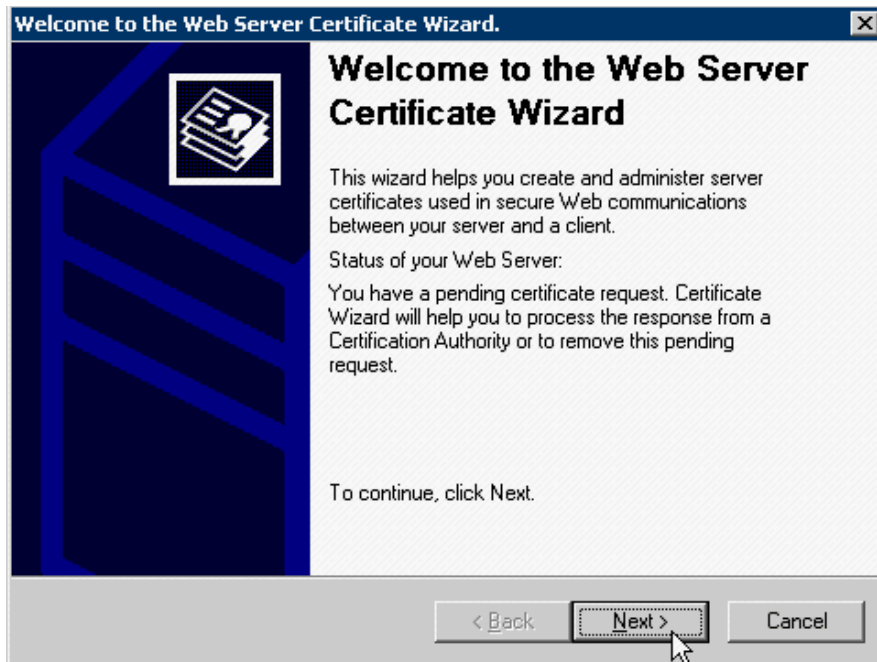
### *Installing a Certificate Authority*

#### 2.2.3 Import and activate the Server certificate

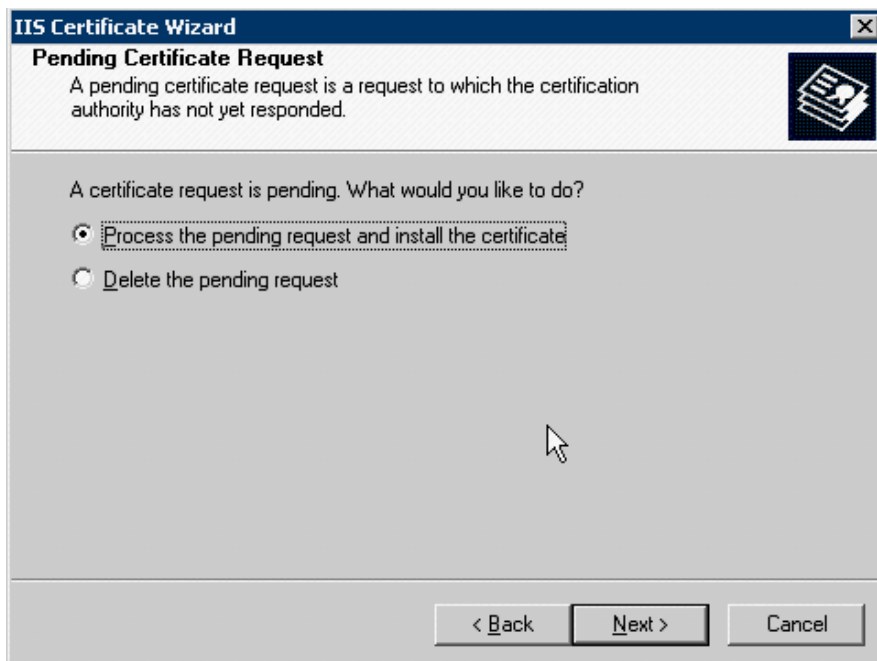
Launch to the IIS application and highlight the requested web site (default web site in example), from there select “**Properties**” by clicking right mouse.



Select the “**Directory Security**” tab and press the “**Server Certificate**” button



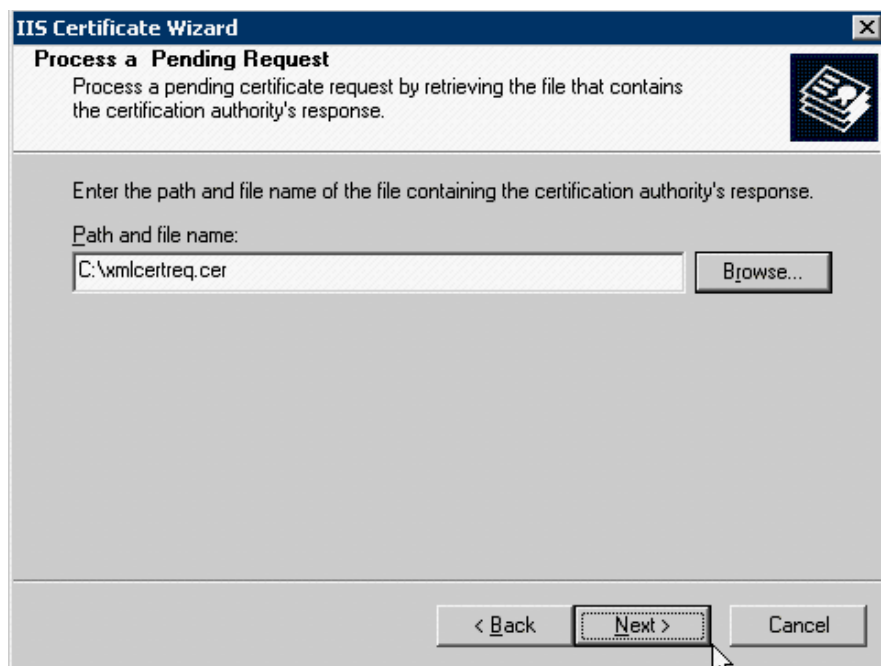
On Wizard screen press **“Next”**



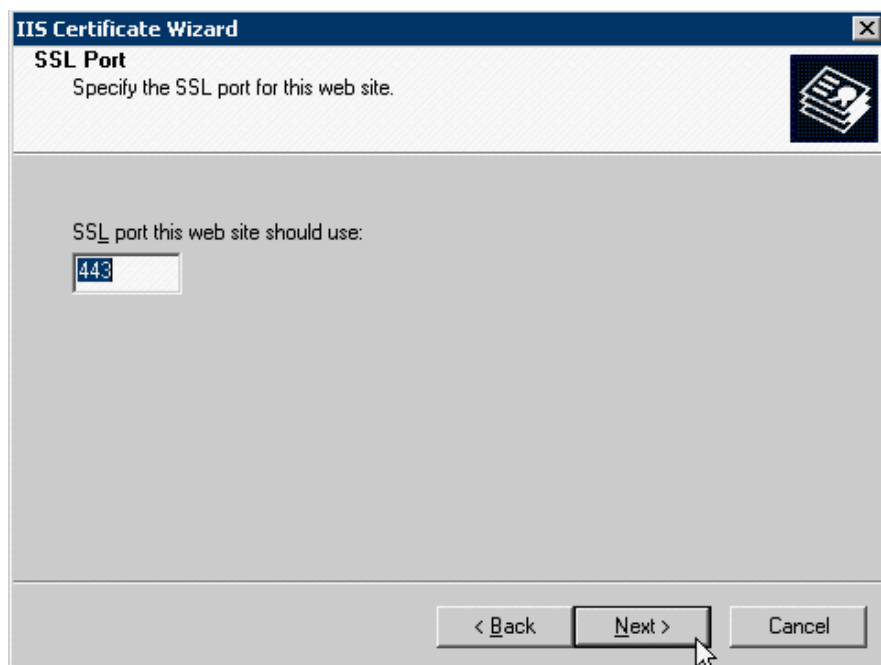
Select the option to **“Process the pending request and install the certificate”**

## SETTING UP

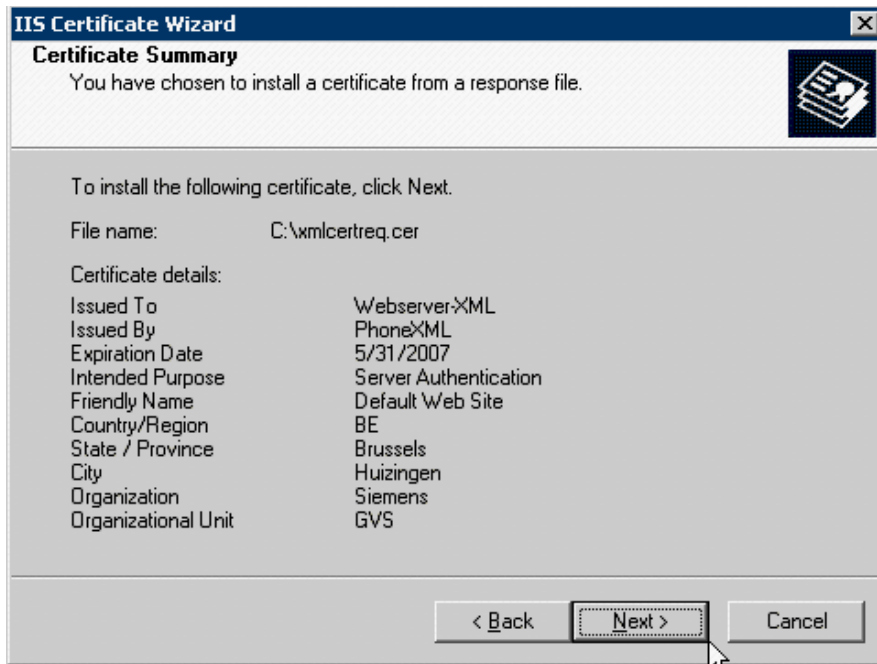
### *Installing a Certificate Authority*



Launch to the location of your certificate file, and press “**Next**”.



Administrate the “**SSL port**” your will use and press “**Next**”



Verify the certificate and press “Next



Press “Finish

## SETTING UP

Setup the phone for HTTPS connection


### 2.3 Setup the phone for HTTPS connection

Browse to the phone URL and launch to the “administrator” page.

- Configuration management...
  - [Settings](#)
  - [Check for updates](#)
  - [Error Log](#)

In the administrator main menu select “**Settings**” of the configuration management.

**Configuration management settings**

 Auto-discovery has selected HTTPS as the download mechanism; administration changes to fields marked with an asterisk (\*) have been locked out.

**Deployment service (DLS) (Not in use)**

IP address or DNS name:  \*

Port:  \*

**Secure configuration download (HTTPS) (In use)**

IP address or DNS name:  \*

Port:  \*

File path for URL:

**Non-secure configuration download (FTP) (Not in use)**

In the “Secure configuration download (HTTPS)” section you need to configure the web server “**IP address or DNS name**”, of the secure web server.

The “**Port**” number as configured on the web server, 443 is the standard HTTPS port number.

The “**File path for URL**” is the path where you XML files are stored, in case that the XML files are stored on the web server root address just enter “/”, in all other cases the to administrate path is the path starting from the server root path.

This configuration can also be provided by a DHCP server by use of “Vendor Specific Information Element” and/or “Vendor Classes”. In this case the provided information by the DHCP server cannot be changed via GUI or WEB (see example of settings above).

See format of vendor specific information element: “https://[base URL of link on Download Web Server][:Port#]”

**Common settings (HTTPS and FTP)**

Configuration file name:

Configuration file type:

After registration, check for updates every:  seconds (0 = don't check)

If registration fails, check for updates every:  seconds

Authentication enabled: ☐

The **Configuration file name** is the name of the “device file” without extension. The “User file” must not be configured because the user file name has the same name + the MAC address (see the XML documentation).

The **Configuration file type** is the extension name of the file (standard “xml”).

The „Authentication Enabled“ flag will enable the phone to download- and to synchronise with the configuration files upon a SIP NOTIFY (check\_sync) message. This flag should only be activated if your SIP provider support this function.



The **Configuration file name** and **Configuration file type** cannot be provided by DHCP.

## SETTING UP

Setup the phone for HTTPS connection

### 2.3.1 Check and test the HTTPS connection

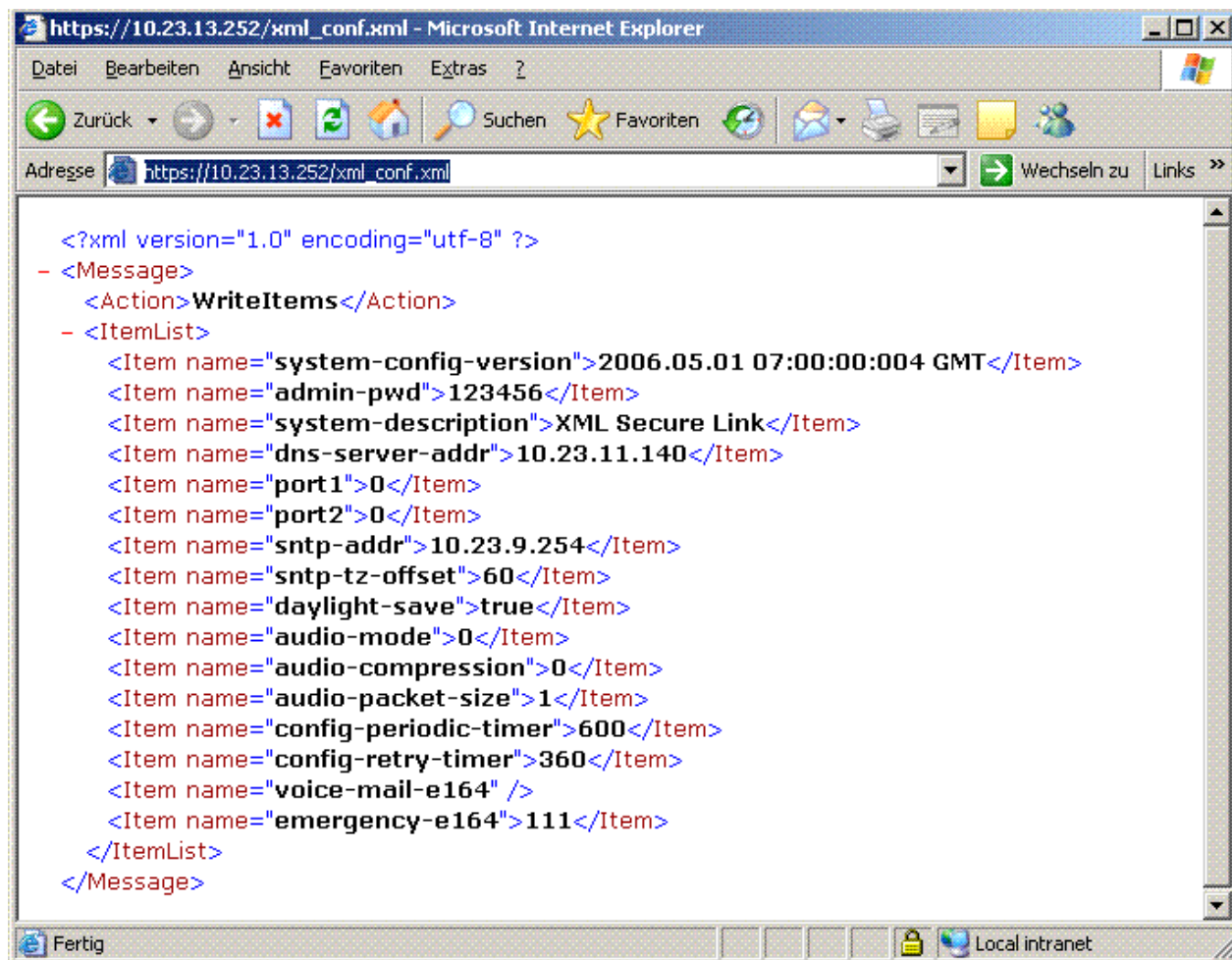
To Test the XML webserver you need to open a browser, and launch to the IP address as administrated in the “administrator” page, when typing the correct file names you must be able to see the contents of the XML files.

The URL to type is:

- `https:// [IP XML web server]/[Name of config file +extension]` for the System file, and
- `https:// [IP XML web server]/[Name of config file[MAC addr] +extension]` for the device file.

When submitting the requested URL you will receive a security warning message in your browser Click “Yes” to proceed. You just receive this message because the typed URL don’t match the administrated URL of the certificate. If this works you can be sure that the web server works and the files are present.

See example below.





## 2.4 802.1X certificates in the XML configuration files



In SIP version 6.0.xx it is not possible to send the Pass phrase to the phone as a XML item, for that reason must the client certificate be encoded with a specific pass phrase which is only known by some Siemens personal members.

Like all other XML items are the certificates normal items, however every time that the "contents" of the XML file change will this lead to a restart of the phone. That's because the XML parser in the phone will restart if it detects a certificate. Therefore it is advisable to put the certificates in the "System wide" file because in normal operations the contents of that file will not change so frequently as the "Device file".

The server certificate must be created in PEM format, and the client certificate in binary 64 format. The client certificate must be encrypted with the build in pass phrase of the phone. This client certificate can therefore only be converted to B64 format by Siemens personal.

If the customer wants an 802.1X client certificate then he needs to hand over the Client certificate in PK12 format together with the pass phrase. This client certificate needs to be converted to the requested B64 format with the phone build in pass phrase, and can then be handed over to the customer again.

This conversion will be done in three steps by using "OpenSSL" and can only be done by Siemens personal (see note)

1. Read the PK12 file and convert to PEM (here we need the customer PK12 password)

**OpenSSL>** pkcs12 -in [Delivered customer certificate filename] -out certconv.pem

2. **Convert the PEM back into P12 but with the Phone build in Pass Phrase**

**OpenSSL>** pkcs12 -export -in certconv.pem -out certnew.p12

3. **Convert the P12 with the phone Build in Pass Phrase to the requested B64 format.**

**OpenSSL>** base64 -in certnew.p12 -out [Customer requested filename].b64

See the XML items containing the certificate(s).

This is an example of the server certificate in PEM format

```
<Item name="radius-server-ca1">-----BEGIN CERTIFICATE-----
MIICrDCCAhhWgAwIBAgIJANv25GBRph+iMA0GCSqGSIb3DQEBAUAMIGKMQswCQYD
VQQGEwJERTEPMA0GA1UECBMGMmF5ZXJ1MQ8wDQYDVQQHEwZNdW5pY2gxEDAOBgNV
BAoTB1NpZW11bnMxEzARBgNVBAsTC1N5c3R1bXRlc3QxDzANBgNVBAMTBkx1ZHdp
ZzEhMB8GCSqGSIb3DQEJARYSTHVkd2lnLnNpZW11bnMuY29tMB4XDTA1MDYwODA5
MTk0MFoXDTA2MDYwODA5MTk0MFOwYsxCzAJBgNVBAYTAkRFRMQ8wDQYDVQQIEwZC
```

## SETTING UP

### 802.1X certificates in the XML configuration files

```
YX1lcm4xDzANBgNVBACTBk11bm1jaDEQMA4GA1UEChMHc2l1bWVtczEUMBIGA1UE
CxMLZW5naW5lZXJpbmcxDzANBgNVBAMTBnN1cnZlcjEhMB8GCSqGSIb3DQEJARYS
c2VydMvYQHNPZW11bnMuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCa
jFqWTqGOUwzb39NDjFnkomTFA6+8IlxKmbyTq+U6aW3RX88aWn1JbOcMH7sOz0kk
NkxBQO/ErnvMlwPEk11Lx4oexz+gpk63hlbi6jUs/ovraYyCl/sDqihXR6ldyHya
hiAfkZRzpdclrPzFtdX3ENE52j8KTdqdY0oWZabbUwIDAQABoxcwFTATBgNVHSUE
DDAKBggrBgEFBQCcDATANBgkqhkiG9w0BAQQFAA0BgQAhrbTPB40v6xGrdfYDyy2s
nUBjsHhyB5yRIcZb2LX5aK9DmFPPSF93Xj20XVOrQKIq5QjmnAidkPXQyNNNcYv4I
N06Ujy2YdnNdkJFX+ihQfnA5KzGYeVN2FMTh3RFvPF94HwNt1ry1jdza2ywj/h/g
keRyV/blKtcJeexS6kZOlG==
-----END CERTIFICATE-----</Item>
```

This is an example of the client certificate in B64 format

```
<Item name="802.1x-certifi-
cate">MIIGQQIBAzCCBm8GCSqGSIb3DQEHAaCCBmAEEggZcMIIGWDCCA1cGCSqGSIb3DQEH
BqCCA0gwggNEAgEAMIIDPQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQI2IDu
BBdjnd4CAggAgIIDEEG9w263Sd2V1MYUHeU11JTJ6BoMVk1B3q6+rix0MCfnR70a
aj9n1dP2ZJPXL1nRZJQ9QKvZrxoqrP/v7NV+TSiOwRVqQH6NYo/AmKQlertFbde
ZYkBIkszt2S9C9DhD/ACuZHw3cmHb3N3yqkQ6gjPwXFylfeYYuoasoxadn36Dr7
gu6cPEoG1B/EIemW67I7OB9BlbuWYGd/9aLX+G0mqoDDH2sx5gAU9nLR7XNw32A4
+HHFGzP/if0LCfIa47fK9QAwjDqsPesINE+cCBOqpG8kHH4VyvluvDl2xhs/Jomz
Rvc5S3d2qq//tc3nSS3TB0Dovdu8TDLTDk3J16bOZEKJlF8Y+N2sk6VbCV0exOIP
iMsqYLKQzSXYxdhY5mzeIwKkQvMzQMSz+LUlNjYk3R1KCpifZ1brtzXV6yPv9m68
HCUU1OSUSfCvKGlXjUH+UTXtsgkbpGvGQSNJI1mYhJB+WJ5ZAeHac0bJI9dYS2yt
OH0XiaRxeAX6QgcjSj1IeGmSCyMy8JuGH4LzJghvYz3p2AKYnIryYxM4QQ1aoQlx
w71E2q9+PHspogtp2sU0jVsUFgkeSHo6pcSEwZutYElvekWo3PElnjBaSrt+Obxu
VEqC7EzlmBCcpVudPJdbCjbHZP0xtucisdBJG6QnUnendZqXnlShOCM2XYZjEj6m
pcZNkzCSRu98XB7KzoGF0otq5en8Jo+9lUEe1EeL7dkCg1fzajGzwcmJFYpUMth0
Mw8g2WIjuAe3BiMnhTirNBflKpJrL5e8R70Jtz3b95YHKRCDntKAycJClzD0OfCi
coAX4WDN/37Hl+pWo06iHu1+Z7VgjNBBfa44tltLxlZc/+sohBVettKDF+0/o5ws
f3MB0b8kqyHouQQMOYq5wYvTeQKW9OeJ5E1szIZYfc7K0MSr1p06wkt+Rgqu256Q
91bOacoBBE96jRZY8aYzuXbYcIuR+phDV3tgdA0sjLWIa4OZNge155hzf7aT3Wh
```

```

xcVrpywes80CdBHodg6IMLP6jPy4UfXHcicKSx0wggL5BgkqhkiG9w0BBwGgggLq
BIIC5jCCAUIwggLeBgsqhkiG9w0BDAoBAqCCAqYwggKiMBwGCIqGSIB3DQEMAQMw
DgQIcRC43gulfRoCAggABIICgCsL2VkVatmTyQx0732cstmsWTOHStSI57Zo9smD
kqtQrJ611n35+dK/FBUnqsvKuHCPScP4nLSZ4a5QNT4OcuzfnlPJvdqqPg4S0tMU
5ysq9dvH4xxvGi9/SzxyksrfQHroap4qZ5CAjtlMFmulw+GHhneEd0ZZOzmOCQl
0rt98pJ5gO8LIIIfm0bPHBrsrEqHAeSCavjd1qPJWBmbb+5Q1EPQBqZDK764zJxka
9ibYabgng+Ecq/6UODbUN6K8gQN5Ma6xAkS+/S1KCNWjkQzp07jy7bwSdL6rlwM
HzGFaDB1hRrcCnNH/sBfyEl28R8ixuBCv2GeUAQotipUq7CY/tDEA3mIfn8537MG
i5Ctt8vK+3i4LJJzmmqkk0juYaN2Bapad1aDZroVsxxkNtFjrDBMhIXDgB0PZTrf
XoyWeX/5zHIb5FNapW/VOJgbGg9Ch4irK/VqfismMNYfksy+VM+sDS5fUnsM0BEq
weraQPcwtzMwbCmaHJuS7YAKWDgk7QbeHC6YnUNUPQPSctGXL2GhTYugSztH/Znp
BkiX3jSh8XV35X2fg5QHGT0Ee36ylSzDeM+UZHzh8ML1RX7RMVe6eusVEN5uBcLu
hnIHuJg8hyp6LK8MF5JAAHkz0mZ0NisOdnj808dr+g/E10At5fLWXFMrZBkYQDPt
zz9gGSGkh0a8s6mCuyNevnw2eoMkayszrmTNaiF0ptekdf3iWThjx6XtVOrlouqO
ob8SfiMqKEZL6HW5m+KVeeA2PdGEvb9UJIiWnpdhhbTTjTXEpKARNy+NuFKqE4XiR
T5Ttxw3QP1BePjG06aoUP6z3m2aQiJX2RQ0AtxvyIMIkjegxJTAjBgkqhkiG9w0B
CRUxFgQUoTCMpc4uJFdVNVO/ENUBxDCvVYswMTAhMAkGBSsOAwIaBQAEFOz/10MI
/CW+QKABtIZvuo5TD2j8BAGB6Z/fqKb2egICCAA=</Item>

```

## **SETTING UP**

*802.1X certificates in the XML configuration files*

### 3 Abbreviations

| <b>Abbreviation</b> | <b>Definition</b>                                                                                                 |
|---------------------|-------------------------------------------------------------------------------------------------------------------|
| DHCP                | Dynamic Host Configuration Protocol.                                                                              |
| DLS                 | Deployment and Licensing Service                                                                                  |
| DNS                 | Domain name server                                                                                                |
| <b>EAP</b>          | <b>Extensible Authentication Protocol</b>                                                                         |
| <b>EAPOL</b>        | <b>Extensible Authentication Protocol Over LAN</b>                                                                |
| <b>FTP</b>          | <b>File Transfer Protocol</b> “.                                                                                  |
| IAS                 | Internet Authentication Service                                                                                   |
| IIS                 | Internet Information Server                                                                                       |
| IP                  | Internet Protocoll                                                                                                |
| <b>PEAP</b>         | <b>Protected Extensible Authentication Protocol</b>                                                               |
| RFC                 | Request For Comments; A IETF Protocol Specification                                                               |
| <b>TAP</b>          | <b>Techniker ArbeitsPlatz</b> (Meist ein speziell mit Soft- und Hardware ausgestattetes Notebook des Technikers.) |
| <b>TLS</b>          | <b>Transport Layer Security</b>                                                                                   |
| <b>TTLS</b>         | <b>Tunneled Transport Layer Security</b>                                                                          |
| VID                 | Virtual LAN ID                                                                                                    |
| VLAN                | Virtual LAN                                                                                                       |

## Abbreviations



[www.siemens.com/hipath](http://www.siemens.com/hipath)

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products.

An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract.

The trademarks used are owned by Siemens AG or their respective owners.



The device conforms to the EU directive 1999/5/EG, as attested by the CE mark.



This device has been manufactured in accordance with our certified environmental management system (ISO 14001). This process ensures that energy consumption and the use of primary raw materials are kept to a minimum, thus reducing waste production.

