

optiPoint 410/420 family

SIEMENS

Global network of innovation

XML and/or IEEE 802.1x Certificate over secure link

**Administration Manual** 

# Contens

1 Introduction	1-1
1.1 PRINCIPLE	1-2
1.2 What is needed	1-5
2 SETTING UP	2-1
2.1 Installing the web server	<u>2-1</u>
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
3 Abbreviations	3-1

# Contens

# 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.

### Handshake Sequence for TLS

# 1. Client Hello 2. Server Hello 3. Server Certificate 4. Server Hello Done 5. Client Key Exchange 6. Change Cipher Spec 7. Finished 8. Change Cipher Spec 9. Finished

Phone (Web Client)

Download Web Server

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 followon 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.

	•		
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

### See compact line trace example:

### 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, Appli- cation 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  $\rightarrow$  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)

# 3. Installing a Certificate Authority

To be able to setup a secure web server, the web server needs a root- and server certificate witch 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 crate 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

# 2.1 Installing the web server

IIS is an additional package that can be installed Windows CD. Launch to the "**Control Pane**l" and select "**Add or Remove Programs**" and then select the option "**Add/Remove** <u>W</u>indows **Components**", from the list select "Internet Information Services".

	the location of the IIS can differ, either the IIS group" Application Group" (see below).
Vindows Components Wizard	×
Windows Components You can add or remove components of Windows.	
To add or remove a component, click the checkbox. A shaded part of the component will be installed. To see what's included i Details.	
Components:	
🗹 📻 Accessories and Utilities	4.9 MB 🔺
🗹 🥞 Application Server	33.4 MB 📥
🗹 📴 Certificate Se 🔤 ces	1.4 MB
🗆 🛄 E-mail Services	1.1 MB
Eax Services	7.9 MB
Description: Includes ASP.NET, Internet Information Services ( Application Server Console.	IIS), and the
Total disk space required: 5.1 MB Space available on disk: 9838.2 MB	(etails)
< <u>B</u> ack <u>N</u> ext >	Cancel Help

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

Application Server	×
To add or remove a component, click the check box. A shaded box me- of the component will be installed. To see what's included in a compone	
Sub <u>c</u> omponents of Application Server:	
🗆 🗖 🏠 Application Server Console	0.0 MB 📐
🗆 🔁 🍓 ASP.NET	0.0 MB
Enable network COM+ access	0.0 MB
🗆 🗇 🚯 Enable network DTC access	0.0 MB
🗹 💱 Internet Information Services (IIS)	26.9 MB
🗆 🚅 Message Queuing	6.5 MB
Description: IIS Includes Web, FTP, SMTP, and NNTP support, along for FrontPage Server Extensions and Active Server Page	
Total disk space required: 5.1 MB	Details
Space available on disk: 9839.2 MB	
ОК	Cancel

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

Internet Information Services (IIS)		X
To add or remove a component, click the check box. A shaded box means of the component will be installed. To see what's included in a component,		
Sub <u>c</u> omponents of Internet Information Services (IIS):		
Background Intelligent Transfer Service (BITS) Server Extensions	0.2 MB	
🗹 🔷 Common Files	1.0 MB	
🗹 📮 File Transfer Protocol (FTP) Service	0.1 MB	
🗆 🅎 FrontPage 2002 Server Extensions	14.1 MB	
🗹 📸 Internet Information Services kanager	1.3 MB	
🗆 🎯 Internet Printing	0.0 MB	
🗆 💩 NNTP Service	1.0 MB	•
Description: Provides support to create FTP sites used to upload and do	wnload file:	s.
Total disk space required: 5.1 MB	Details	1
Space available on disk: 9839.2 MB	<u>P</u> _000110	
ОК	Cancel	

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 Pane**l" and select "**Add or Remove Programs**" and then select the option "**Add/Remove** <u>**W**</u>indows 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.
Windows Components Wizard
Windows Components         You can add or remove components of Windows.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Accessories and Utilities 4.9 MB
Application Server 33.4 MB
✓ Securificate Services
🗆 🛄 E-mail Services 1.1 MB
T 9MB
Description: Installs a certification authority (CA) to issue certificates for use with public key security programs.
Total disk space required: 5.1 MB Details
Space available on disk: 9839.2 MB
< <u>B</u> ack <u>N</u> ext > Cancel Help

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

Installing a Certificate Authority

Windows Components Wizard	×
Select the type of CA you want to set up.	Q
C Enterprise root CA	
O Enterprise subordinate CA	
Stand-alone root CA	
C Stand-alone subordinate CA	
Description of CA type The most trusted CA in a CA hierarchy.	
To install an enterprise CA, Active Directory is required; you must also be a member of the Enterprise Admins group.	1
☑ Use custom settings to generate the key pair and CA certificate	
< <u>B</u> ack <u>N</u> ext > Cancel He	lp

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.

Windows Components Wizard		×
Public and Private Key Pair Select a cryptographic service provider (CSP), hash alg key pair.	gorithm, and settings for the	Ē
CSP: Microsoft Base DSS Cryptographic Provider Microsoft Enhanced Cryptographic Provider v1.0 Microsoft Strong Cryptographic Provider Schlumberger Cryptographic Service Provider Allow this CSP to interact with the desktop	Hash algorithm: MD4 MD5 SHA-1 Key length:	
🗖 Use an <u>e</u> xisting key:	2048	
Microsoft Internet Information Server MS IIS DCOM Server	I <u>m</u> port ⊻iew Certificate	
< <u>B</u> ack <u>N</u> ext >	Cancel	Help

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

Windows Components Wizard	×
<b>CA Identifying Information</b> Enter information to identify this CA.	t
Common name for this CA:	
PhoneXML	
Distinguished name suffix:	
Preview of distinguished name:	
CN=PhoneXML	
, ⊻alidity period:	Expiration date:
5 Years 💌	29.05.2011 01:32
< <u>B</u> ack	Cancel Help

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

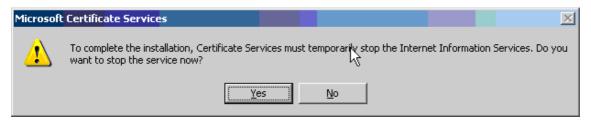
Windows Components Wizard	×
Certificate Database Settings Enter locations for the certificate database, database log, and configura information.	ation
Certificate database:	
C:\WINDOWS\system32\CertLog	Browse
Certificate <u>d</u> atabase log:	
C:\WINDOWS\system32\CertLog	Bro <u>w</u> se
<ul> <li>Store configuration information in a shared folder</li> <li>Shared folder:</li> <li>C:\CAConfig</li> <li>Preserve existing certificate database</li> </ul>	B <u>r</u> owse
< <u>B</u> ack <u>N</u> ext > Cance	I Help

### 10. November 2006

XML and/or IEEE 802.1x certificate over secure link, Administration Manual

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

Windows Components Wizard	×
<b>Configuring Components</b> Setup is making the configuration changes you requested.	Ć
Please wait while Setup configures the components. This may take several minutes, depending on the components selected.	
Status: Copying files	_
N	
h2	
< <u>B</u> ack <u>N</u> ext > Cancel	Help

### All needed files will be installed

Microsoft	Certificate Services				X
1	Active Server Pages (ASPs) must be enab Services to provide web enrollment service evaluated. You can enable ASPs later if yo enable this functionality. Do you want to enable Active Server Page	es. Enabling ou choose n	) ASPs is a potential secu	rity risk and mu	st be carefully
	<u> </u>	əs [	No		

Select "Yes" to activate the Active Server Pages.

Windows Components Wizard			×
	Completing the Windows Components Wizard		
	< Back Finish	Help	

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.

Installing a Certificate Authority

🐌 Internet Information Service	Default Web Site Properties
Section       View       Window         ←       →       E       III       X       E       III         Internet Information Services       Internet Information Services       IIII       IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Documents         Directory Security         HTTP Headers         Custom Errors           Web Site         Performance         ISAPI Filters         Home Directory           Web site identification         Description:         Default Web Site
⊕ - → Application Pools ⊖ → → Web Sites ⊡ - → Default Web Site ⊕ - → CertSrv ⊕ - → CertControl	IP address:     (All Unassigned)     Image: Advanced       ICP port:     80     SSL port:     443
E-     GertEnroll     Web Service Extension     FTP Sites	Connections Connection timeout: 120 seconds  Connection timeout: 120 seconds  Connection timeout: 120 seconds
	Enable logging         Active log format:         W3C Extended Log File Format
<b>↓</b>	OK Cancel Apply Help

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"

internet Information Service	efault Web Site Properties
Section     View     Window       ←     →     €     ●     ×     ●     ●	Web Site         Performance         ISAPI Filters         Home Directory         I           Documents         Directory Security         HTTP Headers         Custom Errors         I
Internet Information Services Multi XML-WEBSERVER (local cor Application Pools Web Sites Default Web Site	Authentication and access control  Enable anonymous access and edit the authentication methods for this resource.  Edit
CertSrv     DertControl     DertEnrol     DertEnrol     Web Service Extension	IP address and domain name restrictions Grant or deny access to this resource using IP addresses or Internet domain names.
⊕- 🍎 FTP Sites	Ed <u>i</u> t
	Secure communications
	Require secure communications and enable client certificates when this Server Certificate
	resource is accessed.
	E <u>d</u> it
	OK Cancel Apply Help

In the "Web Site" tab of the properties page click on the "Server Certificate" button.

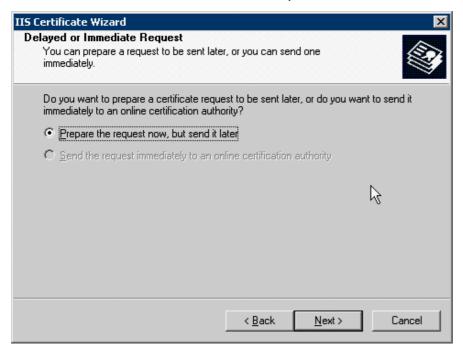
Welcome to the Web Server	Certificate Wizard.	×	
	Welcome to the Web Server Certificate Wizard This wizard helps you create and administer server certificates used in secure Web communications between your server and a client.		
	Status of your Web Server:		
	You have a certificate installed for the selected server. Certificate Wizard will help you to manage this certificate.		
	To continue, click Next.		
		<u></u>	
	< Back Cancel		

# Click "Next" to start the Certificate Wizard

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 Ce	ertificate Wizard 🛛 🛛 🛛 🛛 🛛
	ne 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.
	Na <u>m</u> e:
	Default Web Site
	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 lengt <u>h</u> : 1024
	Select cryptographic service provider (CSP) for this certificate
	< <u>B</u> ack <u>N</u> ext > Cancel

Define the mane 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:
Siemens
Organizational <u>u</u> nit:
GVS
< <u>B</u> ack <u>N</u> ext > Cancel

Administrate the "Organization" and "Organization unit". => Click Next.

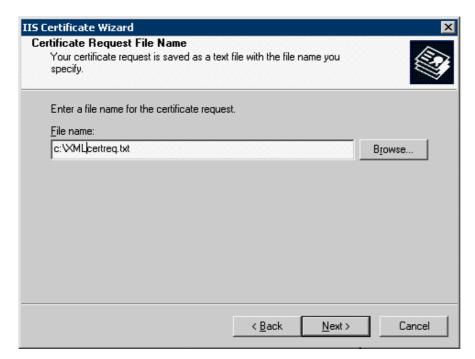
# **SETTING UP** *Installing a Certificate Authority*

Type the common name for your site. If the name. If the server is on the intranet, you m name.		
If the common name changes, you will nee	to obtain a new certificate.	
<u>C</u> ommon name:		
Webserver-XML		
	< <u>B</u> ack <u>N</u> ext>	Cancel

Administrate the "Common name" => Click Next.

IIS Certificate Wizard	×
Geographical Information The certification authority requires the followin	ng geographical information.
<u>C</u> ountry/Region: BE (Belgium)	
<u>State/province:</u>	
Brussels	•
City/locality:	
Huizingen	<b>•</b>
State/province and City/locality must be comp abbreviations.	plete, official names and may not contain
	< 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.

IIS Certificate Wizard			×
Request File Summary You have chosen to generate	a request file.		
To generate the following requ	iest, click Next.		
File name: c:\xmlcertreq.txt			
Your request contains the follo	wing information:		
Issued To Friendly Name Country/Region State / Province City Organization Organizational Unit	Webserver-XML Default Web Site BE Brussels Huizingen Siemens GVS		
	< <u>B</u> ack	<u>N</u> ext >	Cancel

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

Installing a Certificate Authority



Press "Finnish"

The result of this action is that you got a Certificate which needs to be signed by a trusted authority (CA).

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

----BEGIN NEW CERTIFICATE REQUEST----

```
MIIDRzCCArACAQAwbDELMAkGA1UEBhMCQkUxETAPBgNVBAgTCEJydXNzZWxzMRIw
EAYDVOOHEwlldWl6aW5nZW4xEDAOBqNVBAoTB1NpZW11bnMxDDAKBqNVBAsTA0dW
UzEWMBQGA1UEAxMNV2Vic2VydmVyLVhNTDCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAt9K2TpVPSWrO822BiYOiNtuoMijlEPIjGxsPpfhc32SfEQ4YVnM2qxtN
u1w0kzE0Y0ss1ipyKeABqxrtqoJVdi5Dki3aEZi11UvTssh05Mqwvdckhe9j0CCA
hvbGpCb8+VJJqjxwRIcP7w6jNFXfBMMcasD3w75S+dfWAnjsnkECAwEAAaCCAZkw
GqYKKwYBBAGCNw0CAzEMFqo1LjIuMzc5MC4vMHsGCisGAQOBqjcCAQ4xbTBrMA4G
A1UdDwEB/wQEAwIE8DBEBgkqhkiG9w0BCQ8ENzA1MA4GCCqGSIb3DQMCAgIAgDA0
BqqqhkiG9w0DBAICAIAwBwYFKw4DAqcwCqYIKoZIhvcNAwcwEwYDVR01BAwwCqYI
KwYBBQUHAwEwgf0GCisGAQQBgjcNAgIxge4wgesCAQEeWgBNAGkAYwByAG8AcwBv
AGYAdAAgAFIAUwBBACAAUwBDAGgAYQBuAG4AZQBsACAAQwByAHkAcAB0AG8AZwBy
AGEAcABoAGkAYwAqAFAAcqBvAHYAaQBkAGUAcqOBiQAAAAAAAAAAAAAAAAAAAAAAAAA
HkFvk5F4gDQvFDTE3G/3T1i9G6yP4FdxDe4eMWIuz5DFI6RDit9Q2d4xTIDVSZFV
WbCR0sqyzyTpOz2QNhkxhoQa48jSOOYCfWB9HcQyN3Z5gMJIAEsO+NDVKzVkR3lr
vFvpROJPG+92f6YNU0aUUGSEoHYi3yStU6w+
```

-----END NEW CERTIFICATE REQUEST-----

# 2.2.2 Signing the server certificate by the CA

# Launch to the CA

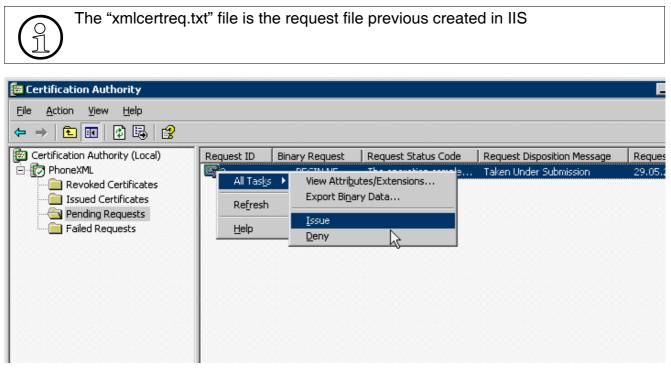
📴 Certification Authority					_		
<u>File Action View Help</u>							
Certification Authority (Local)  PhoneXML  Revoked Certificates  Pending Requests  Failed Requests	Name	All Tasks ► Refresh Properties Help	Description         Start Service         Stop Service         Submit new request         Back up CA         Restore CA         Renew CA Certificate	Y			

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

Open Request Fi	le				? ×
Look jn:	See Local Disk (C:	:)	- ÷	) 💣 🎟 -	
My Recent Documents Desktop My Documents My Computer	CAConfig Documents and Program Files WINDOWS Certreq.txt Certreq.txt				
My Network	File <u>n</u> ame:	xmlcertreq.txt		•	<u>O</u> pen
Places	Files of <u>type</u> :	Request Files (*.req; *.txt;	*.cmc; *.der)	•	Cancel

Installing a Certificate Authority

Launch to the CA request file and press "open"



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**"

📴 Certification Authority		_
Eile Action View Help		
⇔ ⇒ 🗈 📧 🚯 😫		
Certification Authority (Local)	Reque 🛆 Requester Name 🛛 Binary Certificate	Certificate Template
	2 XML-WEBSERVEBEGIN CERTIFICATE MIIE	
	Open     RVEBEGIN CERTIFICATE MIIE	
Pending Requests	All Tasks 🕨 View Attributes/Extensions	
End Requests	Refresh Export Binary Data	
	Help Revoke Certificate	

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**"

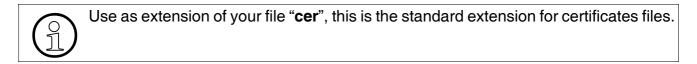
Export Binary Data 🙎 🎗
You can export only the binary data for the columns displayed in the details pane. To add a column to the details pane, on the View menu, click Add/Remove Columns.
Columns that contain binary data:
Binary Certificate
Export options: C View formatted text version of data C Save binary data to a file
DK Cancel

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".

S	ave Binary Data					? ×
	Savejn:	🗇 Local Disk (C:)		-	🗢 🗈 💣 🎫	•
	My Recent Documents Desktop My Documents My Computer	CAConfig Documents and Program Files WINDOWS Certreq.txt Courcert.cer Curcert.txt	Settings			
	My Network Places	File <u>n</u> ame: Save as <u>t</u> ype:	xmlcertreq.cef All Files (*.*)		•	Save Cancel

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



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.

Default Web Si	te Properties		? ×		
Web Site Documents	Performance Directory Security	ISAPI Filters	Home Directory		
Authenticat	ion and access control				
	Enable anonymous access a authentication methods for t		<u>E</u> dit		
□ IP address	and domain name restrictions				
8	Grant or deny access to this IP addresses or Internet dor				
			Edit		
Secure com	Secure communications				
Require secure communications and enable client certificates when this resource is accessed.					
			E <u>d</u> it		
	ОК	Cancel App	Help		

Select the "Directory Security" tab and press the "Server Certificate" button

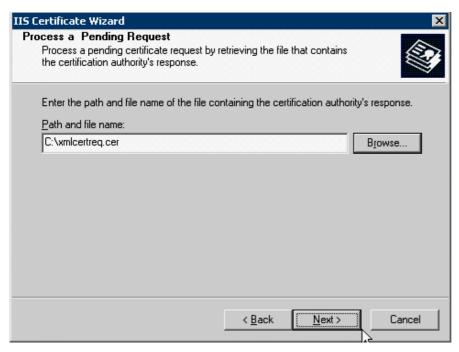
Welcome to the Web Server Certificate Wizard.		
	Welcome to the Web Server Certificate Wizard	
This wizard helps you create and administer server certificates used in secure Web communications between your server and a client.		
	Status of your Web Server:	
	You have a pending certificate request. Certificate Wizard will help you to process the response from a Certification Authority or to remove this pending request.	
	To continue, click Next.	
	< Back Next > Cancel	

# On Wizard screen press "Next"

IIS Certificate Wizard	×
Pending Certificate Request A pending certificate request is a request to which the certification authority has not yet responded.	
A certificate request is pending. What would you like to do?	
Process the pending request and install the certificate	
O Delete the pending request	
N	
k∕	
< <u>B</u> ack <u>N</u> ext >	Cancel

Select the option to "Process the pending request and install the certificate"

Installing a Certificate Authority



Launch to the location of your certificate file, and press "Next".

IIS Certificate Wizard			×
SSL Port Specify the SSL port for this web site.			
SSL port this web site should use:			
	< <u>B</u> ack	Next >	Cancel

Administrate the "SSL port" your will use and press "Next

Certificate Wizard Tertificate Summary You have chosen to	install a certificate from a response file.	×
To install the followin	g certificate, click Next.	
File name:	C:\xmlcertreq.cer	
Certificate details: Issued To Issued By Expiration Date Intended Purpose Friendly Name Country/Region State / Province City Organization Organizational Unit	Webserver-XML PhoneXML 5/31/2007 Server Authentication Default Web Site BE Brussels Huizingen Siemens GVS	
	< <u>B</u> ack <u>Next</u> > Cance	el

# Verify the certificate and press "Next

IIS Certificate Wizard	×
	Completing the Web Server Certificate Wizard
	You have successfully completed the Web Server Certificate wizard.
	A certificate is now installed on this server.
	If you need to renew, replace, or delete the certificate in the future, you can use the wizard again.
	To close this wizard, click Finish.
	< Back Finish Cancel

# Press "Finish

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.

•	Config	uration management
	0	Settings
	0	Check for updates

o Error Log

In the administrator main menu select "Settings" of the configuration management.

/ 🚺 admi	discovery has selected HTTPS as the download mechanism; nistration changes to fields marked with an asterisk (*) have been d out.
eployment se	ervice (DLS) (Not in use)
	IP address or DNS name: 0.0.0.0 *
	Port: 20 *
ecure config	uration download (HTTPS) (In use)
	IP address or DNS name: 10.23.13.252 *
	Port: 443 *
	File path for URL: /

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:	op420adv_conf
Configuration file type:	xml
After registration, check for updates every:	600 seconds (0 = don't check)
If registration fails, check for updates every:	360 seconds
Authentication enabled:	
Submit	Reset

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 activateed if your SIP provider support this function.



Setup the phone for HTTPS connection

# 2.3.1 Check and test the HTTPS connection

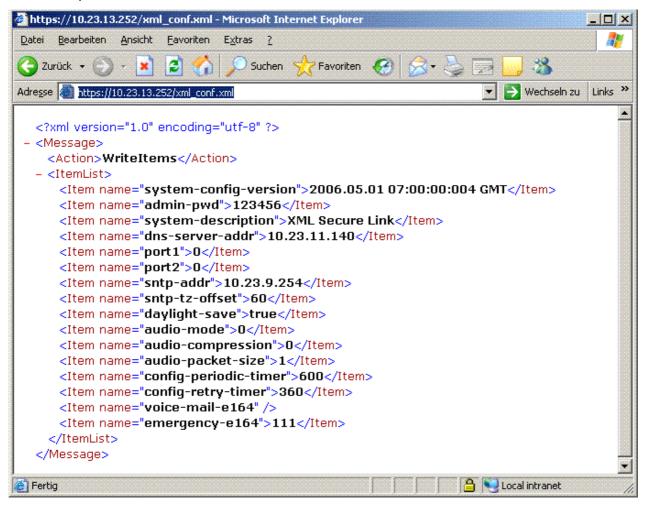
To Test the XML webserver you need to open a browser, and launch to the IP address as administrated in the "administrator" page, when typing the correct file names you must be able to see the contents of the XML files.

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 sent 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-cal">----BEGIN CERTIFICATE----

MIICrDCCAhWgAwIBAgIJANv25GBRph+iMA0GCSqGSIb3DQEBBAUAMIGKMQswCQYD

VQQGEwJERTEPMA0GA1UECBMGQmF5ZXJuMQ8wDQYDVQQHEwZNdW5pY2gxEDA0BgNV

BAOTB1NpZW11bnMxEzARBgNVBAsTC1N5c3R1bXR1c3QxDzANBgNVBAMTBkx1ZHdp

ZzEhMB8GCSqGSIb3DQEJARYSTHVkd2lnLnNpZW1lbnMuY29tMB4XDTA1MDYwODA5

MTk0MFoXDTA2MDYwODA5MTk0MFowgYsxCzAJBgNVBAYTAkRFMQ8wDQYDVQQIEwZC

YXllcm4xDzANBgNVBAcTBk11bmljaDEQMA4GA1UEChMHc2llbWVtczEUMBIGA1UE CxMLZW5naW51ZXJpbmcxDzANBgNVBAMTBnNlcnZlcjEhMB8GCSqGSIb3DQEJARYS c2VydmVyQHNpZW11bnMuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCa jFqWTqGOuwzb39NDjFnkomTFA6+8I1xKmbyTq+U6aW3RX88aWn1JbOcMH7sOz0kk NkxBQO/ErnvMlwPEk11Lx4oexz+gpk63hlbi6jUs/ovraYyCl/sDqihXR6ldyHya hiAfkZRzpdclrPzFtdX3ENE52j8KTdqdY0oWZabbUwIDAQABoxcwFTATBgNVHSUE DDAKBggrBgEFBQcDATANBgkqhkiG9w0BAQQFAAOBgQAhbrtPB40v6xGrdfYDyy2s nUBjsHhyB5yRIcZb2LX5aK9DmFPSF93Xj20XVOrQKIq5QjmnAidkPXQyNNNcYv4I N06Ujy2YdnNdkJFX+ihQfnA5KzGYeVN2FMTh3RFvPF94HwNt1ry1jdza2ywj/h/g keRyV/blKtcJeexS6kZO1g==

-----END CERTIFICATE----

### This is an example of the client certificate in B64 format

<Item name="802.1x-certifi-

cate">MIIGqQIBAzCCBm8GCSqGSIb3DQEHAaCCBmAEggZcMIIGWDCCA1cGCSqGSIb3DQEH BqCCA0gwggNEAgEAMIIDPQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQI2IDu BBdjnd4CAggAgIIDEEG9w263Sd2V1MYUHeU11JTJ6BoMVk1B3q6+rix0MCfnR70a aj9n1dP2ZJPXL1nRZJQ9QKvZrxoqrpR/v7NV+TSiOwRVqQH6NYo/AmKQlertFbde ZYkBIkszjt2S9C9DhD/ACuZHw3cmHb3N3yqk06qjPwXFylfeYYuoasoxadn36Dr7 gu6cPEoG1B/EIemW67I7OB9B1buWYGd/9aLX+G0mgoDDH2sx5gAU9nLR7XNw32A4 +HHFGzP/if0LCfIa47fK9QAwjDqsPesINE+cCBOqpG8kHH4VyvluvDl2xhs/Jomz Rvc5S3d2qq//tc3nSS3TB0Dovdu8TDLTDk3J16b0ZEKJ1F8Y+N2sk6VbCV0exOIP iMsqYLKQzSXYxdhY5mzeIwKkQvMzQMSz+LUlNjYk3R1KCpifZ1brtzXV6yPv9m68 HCUUlOSUSfCvKGlxjUH+UTXtsgkbpGvGQSNJI1mYhjB+WJ5ZAeHac0bJI9dYS2yt OH0XiaRxeAX6OqcjSj1IeGmSCyMy8JuGH4LzJqhvYz3p2AKYnIryYxM4OQ1aoQ1x w7lE2q9+PHspogtp2sU0jVsUFgkeSHo6pcSEwZutYElvekWo3PElnjBaSrt+Obxu VEqC7Ez1mBCcpVudPJdbCjbHZP0xtucisdBJG6QnUnendZqXn1ShOCM2XYZjEj6m pcZNkzCSRu98XB7KzoGFOotq5en8Jo+91UEe1EeL7dkCg1fzajGzwcmJFYpUMth0 Mw8g2WIjuAe3BiMnhTIrNBflKpJrL5e8R70Jtz3b95YHKRCDntKAycJClzD00fCi coAX4WDN/37H1+pWoO6iHu1+Z7VgjNBBfa44tltLxlZc/+sohBVettKDF+0/o5ws f3MB0b8kqyHouQQMOYq5wYvTeQKW90eJ5E1szIZYfc7K0MSr1p06wkt+Rgqu256Q 9lbOacoBBE96jRYZY8aYzuXbYcIuR+phDV3tgdAOsjLWIa40ZNge155hzf7aT3Wh

xcVrpywes80CdBHodq6IMLP6jPy4UfXHcicKSx0wqgL5BqkqhkiG9w0BBwGqqgLq BIIC5jCCAuIwggLeBgsqhkiG9w0BDAoBAqCCAqYwggKiMBwGCiqGSIb3DQEMAQMw DgQIcRC43gulfRoCAggABIICgCsL2VkVatmTyQx0732cstmsWTOHStSI57Zo9smD kqtQrJ611n35+dK/FBUnqsvKuHCPScP4nLSZ4a5QNt40cuzfnlPJvdqqPq4S0tMU 5ysg9dvH4xxvGi9/SzxvksrfOHroap4gZ5CAjt1nMFmu1w+GHhneEdOZZOzmOCOl 0rt98pJ5g08LIIfm0bpHBrsrEqHAeSCavjd1qPJWBmbb+5Q1EPQBqZDK764zJxka 9ibYabgng+Ecq/6UODbUN6K8gQN5Ma6xAkS+/S1KCNwjkQzp07jy7bwSdL6rlewM HzGFaDB1hRrcCnNH/sBfyE128R8ixuBCv2GeUAQotipUq7CY/tDEA3mIfn8537MG i5Ctt8vK+3i4LJJzmmqkk0juYaN2Bapad1aDZroVsxxkNtFjrDBMhIXDgB0PZTrf XoyWeX/5zHIb5FNapW/VOJgbGq9Ch4irK/VqfismMNYfksy+VM+sDS5fUnsM0BEq weraQPcwtzMwbCmaHJuS7YAKWDgk7QbeHC6YnUNUPQPSctGXL2GhTYugSztH/Znp BkiX3jSh8XV35X2fg5QHGt0Ee36y1SzDeM+UZHzh8ML1RX7RMVe6eusVEN5uBcLu hnIHuJq8hyp6LK8MF5JAAHkz0mZ0NisOdnj808dr+q/E1OAt5fLWXFMrZBkYQDPt zz9qGSGkh0a8s6mCuyNevnw2eoMkayszrmTNaiF0ptekdf3iWThjx6XtVOr1ouq0 ob8SfiMqKEZL6HW5m+KVeeA2PdGEvb9UJIiWnpdhbTTjTXEpKARNy+NuFKqE4XiR T5Ttxw3QP1BePjG06aoUP6z3m2aQiJX2RQ0AtxvyIMIkjegxJTAjBgkqhkiG9w0B CRUxFqOUoTCMpc4uJFdVNVO/ENUBxDCvVYswMTAhMAkGBSsOAwIaBOAEFOz/10MI /CW+QKABtIZvuo5TD2j8BAgB6Z/fqKb2egICCAA=</ltem>

802.1X certificates in the XML configuration files

# 3 Abbreviations

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

# Abbreviations

# 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.

CE

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.

# 

© Siemens AG 2006 • Siemens Communications • Hofmannstraße 51 • D-81359 München, Germany Reference No.: A31003-J4260-M102-1-76A9 Subject to availability. Right of modification reserved.