



## User's guide

# APACHE 2.0 + SSL – Linux

Using non-qualified certificates with

APACHE 2.0 + SSL – Linux

version 1.5

# Table of contents

|                                                                 |           |
|-----------------------------------------------------------------|-----------|
| <b>1. PREFACE</b> .....                                         | <b>3</b>  |
| <b>2. GENERATING CERTIFICATE</b> .....                          | <b>3</b>  |
| 2.1. GENERATING REQUEST FOR CERTIFICATE (CSR).....              | 3         |
| 2.2. GENERATING CERTIFICATE ON THE BASIS OF REQUESTED CSR ..... | 5         |
| 2.3. IMPORT OF CERTIFICATES.....                                | 8         |
| <b>3. INSTALLING KEYS AND CERTIFICATES</b> .....                | <b>9</b>  |
| 3.1. INSTALLING CERTUM CERTIFICATES.....                        | 9         |
| 3.2. INSTALLING PRIVATE KEY .....                               | 9         |
| 3.3. INSTALLING CERTIFICATE OF SERVER .....                     | 10        |
| <b>4. AUTHENTICATE TO SERVER USING CERTIFICATE</b> .....        | <b>11</b> |
| <b>5. VIRTUAL HOSTS FOR AMBIGUOUS ADDRESSES</b> .....           | <b>12</b> |
| <b>6. THE SSL AND TLS PROTOCOLS FOR VIRTUALHOSTS</b> .....      | <b>13</b> |
| 6.1. CONFIGURING VIRTUALHOSTS WITHOUT SSL PROTOCOL.....         | 13        |
| 6.2. CONFIGURING VIRTUALHOSTS WITH SSL PROTOCOL.....            | 14        |

## 1. Preface

Apache is one of the most popular and advanced HTTP server. The Apache is open-source HTTP server, so it is possible to download it (even as a source code) and install for free (see Apache's license at <http://www.apache.org/licenses/>). Apache can be installed on Unix/Linux and Windows operating systems. This HTTP server altogether with module *modssl* can be used for strong cryptography.

To configure Apache using SSL following components should to be installed:

1. Apache – <http://httpd.apache.org>
2. OpenSSL - <http://www.openssl.org/>
3. mod\_ssl - <http://www.modssl.org/>

<http://www.modssl.org/>

If your Linux distribution does not include necessary components, you will have to download and install them on your server.

### Note!

**Module mod\_ssl is not included in Apache 1.3. This option is available in newer Apache 2.0 version.**

## 2. Generating certificate

### 2.1. Generating request for certificate (CSR)

In order to generate keys for Apache, download Openssl (at <http://openssl.org> you can find latest release of Openssl) and install it. After installation follow the steps:

1. After instalation of Openssl on the server, execute the following:

```
openssl genrsa -des3 -out server.key 2048
```

This will generate private key named *server.key*. The private key will be 2048bit and encrypted by 3DES algorithm. During the process of generating private key you will be asked for password. Access to the private key will not be possible without giving the proper password.

```
OpenSSL> genrsa -des3 -out server.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....++++++
++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
```

The CSR file with the private key (*server.key*) should be backed up, i.e. on the floppy disk, pendrive or any other device.

2. After the private key has been successfully generated, execute the following:

```
openssl req -new -key server.key -out server.csr
```

This command requests for CSR certificate server, which will be saved in *server.csr* file. You should remember to point at server's private key (in this case *server.key*) and give the correct password when needed. You will be asked for the following information:

**Country (C)** – symbol of your Country. You should use ISO code, i.e. correct code for Poland is PL (in capital letters).

**State / Province (ST)** – name of the State/Province, i.e. Zachodniopomorskie. You should not use any abbreviations of the name.

**Locality (L)** – name of the city or village, i.e. Szczecin, Berlin, Warsaw.

- **Organization Name(O)** – full name of organization, i.e. My Company;
- **Organizational Unit (OU)** – if there is a need you can enter here department/branch;
- **Common Name (CN)** – very important field. You must enter the full name (fqdn) of DNS server, i.e. [www.test.com](http://www.test.com) [pop3.test.net](http://pop3.test.net)
- **Email (Email)** – enter administrator's e-mail address of the server, i.e. [cunizetowski@certum.eu](mailto:cunizetowski@certum.eu)

In the **Common Name** field you must enter website address of your site.

- for unequivocal address – i.e. [www.mysite.com](http://www.mysite.com), [mysite.com](http://mysite.com):

```
OpenSSL> req -new -key server.key -out server.csr
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:Zachodniop
Locality Name (eg, city) []:Szczecin
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Moja firma
Organizational Unit Name (eg, section) []:Oddzial w Moja firma
Common Name (eg, YOUR name) []:www.mysite.com
Email Address []:cunizetowski.pl_
```

- for ambiguous address – i.e. [\\*.myserver.com](http://*.myserver.com), [\\*.mydomain.com](http://*.mydomain.com):

```
OpenSSL> req -new -key server.key -out server.csr
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:Zachodniopomorskie
Locality Name (eg, city) []:Szczecin
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Moja firma
Organizational Unit Name (eg, section) []:Oddzial w Moja firma
Common Name (eg, YOUR name) []:\*.myserver.com
Email Address []:cunizetowski@certum.pl
```

#### Note!


You should not use any diacritics or special keys such as % ^ \$ \_ when filling the fields during process of generate the CSR certificate.

## 2.2. Generating certificate on the basis of requested CSR

The generated request should be similar to:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDMCCApkCAQAwGzAZBgNVBAMTEmRsdWJhY3oudW5pemV0by5wbDEhMB8G
A1UECXMpYRHpYWwgT2Nocm9ueSBJamZvcmlhY2ppMRswGQYDVQQKEXJVbml6ZXRv
IFNwLiB6IG8uby4xETAPBgNVBACTCFN6Y3plY2luMRswGQYDVQQIEXJaYWNob2Ru
aW9wb21vcnNraWUxZzA5bG9uZS50b3R5b250b3R5b250b3R5b250b3R5b250b3R5
b250b3R5b250b3R5b250b3R5b250b3R5b250b3R5b250b3R5b250b3R5b250b3R5
iQKBgQC8JvRqRPbltoZyvMjfxCef5PIcyLMQv6Z2A10j2GMoeKBCCyZF1kHoDsWW
0ZF54FrTZhyKwYqfgiHO5duLfJSBqb/PTzovZH9qXUtxl+zQIhcJnA4Z/jKyWHG1
X7LUlC9u2bas/vWwQZwYvxeqNMW4RZ+LU9Qqm9b/YD2qtOZ2qwIDAQABoIIBUzAa
BgorBgEEAYI3DQIDMwWCjUuMC4yMTk1LjIwNjYyYzYyYzYyYzYyYzYyYzYyYzYy
VR0PAQH/BAQDAgTwMBMGA1UdJQQMMAoGCCsGAQUFBwMBMIH9BgorBgEEAYI3DQIC
MYHuMIHrAgEBHloATQBpAGMAcGbvAHMAbwBmAHQAIABSAFMAQQAgAFMAQwBoAGEA
bgBuAGUAbAAgAEMAcgB5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkA
ZABLAHIDgYkAXxNuAz6gcBaZUdef8WQ2PAroKMW8sprcKv7QD2encz6/Wct9DZ5C
kGynLgy0f+Lff7ViSDJqxYwAJ68ddqgXyAqIilF63kivPTiC6yxLaNX65v3cnKFx
4UrUrGXZtub7M7/NuxSipOW0Vv7yCHganypxDyRzp6IhulEnL4APEH4AAAAAAAAA
ADANBgkqhkiG9w0BAQUFAAOBgQAsTG3Hu00fFzNTekFo/fb3tKsmuS/1rCCB5sQK
iNpWGZ8Z8+TmqBB0Tuz4FPTkeSqLpWv1ORfmxMKPIu10dC3QwRP2E//oMPnaU807
IJIDwn2VZ7qQ/h0KcWoWSPmvt7J0KKshdGgAF7P6AYc7W4yA9B9nPeyEzQRW0t4D
YBApPQ==
-----END NEW CERTIFICATE REQUEST-----
```

After the request has been generated, order a certificate on Certum Shop, fill request form out and paste CSR at the CERTUM website. Choose **Activate Certificates** option, and find proper certification type (SSL). Then choose **Activate** option.

| Order detail                       |                                                                                              | Activation status        |              |
|------------------------------------|----------------------------------------------------------------------------------------------|--------------------------|--------------|
| Order Number                       | ZoZE/026008/MS/20/07/2011                                                                    | Certificate profile      | Wildcard SSL |
| Order date                         | 20 lipca 2011                                                                                | Activation date          | ---          |
| Payment state                      |  Awaiting | Activation state         | ---          |
| <a href="#">View order details</a> |                                                                                              | <a href="#">Activate</a> |              |

Choose **CSR** type delivery method and click **Next**.

- Electronic codes
- Activate Certificates
- Certificates' management
- Orders history
- Address details
- Tools
- Newsletter
- Group activation

### Activation

1.Orders 2.Method Choice 3.Keys 4.Data 5.Confirmation

Service name **Wildcard SSL, 1 year**  
Issue

---

Select delivery method of key pair for certificate


Key pair generation

CSR

Additional info about CSR can be found in Help section or can be obtained from infoline consultants.

[Next >>](#)

Paste CSR request and click **Next**.



Sklep

801 540 340 Czat Email

Your account: [Łukasz WERKOWSKI](#) Logout

Cart (empty)

PRODUCTS HELP ABOUT US

Search in the shop

Main page » My account » Edit activation details

- Electronic codes
- Activate Certificates
- Certificates' management
- Orders history
- Address details
- Tools
- Newsletter
- Group activation

### Activation

1.Orders 2.Method Choice 3.Keys 4.Data 5.Confirmation

Service name **Wildcard SSL, 1 year**  
Issue

---

CSR \*

```
-----BEGIN CERTIFICATE REQUEST-----
MIICnQCCAYUCQAwTElMAAGAIUEBhMCUeWwDeANBgNVBAoTBNFULRVTTEZMBcG
A1UEAxQK1S8d3cudW5pemV0by5wbDEeMBwGCSpG8Tb3DQEJARVFaW5mb0B1bm16
ZXRvLnBzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2NyasFcgV03e
MPFeSbdw1uA1T+2019v2ktmFaIocINV3yVfVvqGa7cs+iTR1aj165Xz/IV6+CSK
dGUhGTT6Hg/5NvGe5G5saw1ITf2MR0Dg1D52jwfcvLpMpdVMS0Fems42ia2kP
38HTQ6k07bJ1sF8K1kOLAPFfn/LEOYePdsHDLARPwaMikc002kUQoF88VcAN7MK
bmQ+qK6Pa6VjseJHEP7os0T0GvqP6JLwda4EG1h6N9RovPhwn6J1Yy8PQ2QmonBFI
DskAtuy65licTROeEW71AwTR0ktztCOEYK5aPScGFP9e+0dDNDaEBT0hSvsHaLx3M
c3p6UhjE3wIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAgcWQCoPExB/CnPEB1
DefcPK4JEBp9SJs9Q10yQLdI4F7oKFF34B8QyRMV1Jldf07JF64qjzFF+82K
rgwXf0yze0NCE/TRB8Epxu0CR++RMXLTUV6f8B0cIXFAS7qCU1hnaTeGeQ0K7YSA
4EwXKSU7ivsm2RrFYHQjH7nQTCgocVhvtvhw2hNoC4RamaFXLp9cb2efiThnQ14h
X1AmXg1V1DNUbG83U8BciFmSg7WGWwEMKcoiD4LYS+2uPR6ga11f82PPhEgN2Q0
8518H1g7BcD0Mx0Y9Gp84U0NGag28dvenW06rq97f8J121ocK104MftdddmfUF
Acg=
-----END CERTIFICATE REQUEST-----
```

[<< Previous](#)   [Next >>](#)

**Note!**

The certificate should be copied and pasted from line „--BEGIN CERTIFICATE - „ to „-END CERTIFICATE--” with these lines.

Please, check again if the e-mail address is correct. Next instructions will be sent to this address.

New site will appear with given details. Please, make sure that the details are correct.

**Note!**

Please, make sure that, value given in the subject field is correct (if you are buying certificate for domain [www.mydomain.com](http://www.mydomain.com) please, make sure that this name is in the subject field.)

If all details are correct, click on Next:

**Electronic codes**

**Activate Certificates**

**Certificates' management**

**Orders history**

**Address details**

**Tools**

**Newsletter**

**Group activation**

### Activation

1.Orders 2.Method Choice 3.Keys 4.Data 5.Confirmation

Service name **Wildcard SSL, 1 year Issue**

---

**Certificate Data:**

Start of validity

End of validity

DNS Domain \*

Organization

Organizational unit

Country \*

Email

<< Previous Next >>

Confirm certification request data and click **Activate**.


## Activation

1.Orders 2.Method Choice 3.Keys 4.Data 5.Confirmation 

Service name **Wildcard SSL, 1 year**  
Issue

### Certificate Data:

Start of validity 20 lipca 2011  
End of validity 19 lipca 2012  
Organization CERTUM  
Organizational unit  
Country Poland  
Email info@unizeto.pl  
DNS Domain \*.www.unizeto.pl

 Please check Your data. After activation correction is not possible.

### Certificate Structure:

Subject E=info@unizeto.pl, CN=\*.www.unizeto.pl,  
O=CERTUM, C=PL  
Subject Alt. Name dNSName=\*.www.unizeto.pl,  
dNSName=www.unizeto.pl

#### Statement

BEFORE SENDING REQUEST TO ISSUE CERTIFICATES, CONFIRMATION OR USE FOR THE FIRST SIGNATURE - YOU MUST READ THE TEXT OF THIS STATEMENT. IF YOU DO NOT AGREE WITH THIS STATEMENT, DO NOT SEND THE ORDER TO ISSUE CERTIFICATES, DO NOT CONFIRM AND DO NOT USE.

This statement is required from the time of application for issue of certificate CERTUM - Open Certification Authority. Sending the application to issue a certificate means that you want to issuing authority reviewed the application and issued the certificate, at the same time acknowledge that you accept, certain in her condition.

Certification services are provided according to the rules defined in the Rules of Certification procedures (KPC), which, through reference to it ceases integral part of this statement. Rules of certification procedures is available via the Internet from a repository CERTUM - Open Certification Authority at <http://www.certum.pl/repozytorium/> or by e-mail request sent

Confirm certification   
request data \*

<< Previous Activate

Request has been sent to Certum Certification center. Check your e-mail in order to obtain further information.

## 2.3. Import of certificates

To import certificate you need to follow instructions from e-mail. Open the website given in an e-mail message. Then you can choose certificate type (\*.cer or \*.pem).

Save binary

Save plain

## 3. Installing keys and certificates

### 3.1. Installing CERTUM certificates

Besides the server's certificate that has been installed, there should also be CERTUM's certificates installed on the server (you can find them at <http://www.certum.pl/keys/ca-bundle.crt>). In the bundle you can find all CERTUM's certificates: from Level I to Level IV and the root CA at the end.

To install all CERTUM's certificates (from Level I to Level IV and the root CA) copy (using Midnight Commander or Command Line) bundle *ca-bundle.crt* to directory where it will be kept, i.e.:

```
/usr/share/ssl/certs/ca-bundle.crt
```

The *ssl.conf* file looks like the following:

```
SSLCACertificateFile /usr/share/ssl/certs/ca-bundle.crt
```

After this the http server should be restarted:

```
#httpd restart
```

Installing of root CA and all certificates from Level I to Level IV is now successfully completed.

For your convenience you can put at the beginning in *ca-bundle.crt* file, certificate of your server (copy contents of *No\_certificate.pem* and paste it at the beginning in *ca-bundle.crt*).

### 3.2. Installing private key

To install private key on the server, you should copy (using Midnight Commander or Command Line) file with private key - *server.key* - to directory where it will be kept, i.e.:

```
/etc/httpd/conf/ssl.key/server.key
```

The *ssl.conf* file looks like the following:

```
SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key
```

To take off the password of private key (Apache server won't ask for password every time it's restarted), execute the following:

```
openssl rsa -in server.key -out server.key
```

```
OpenSSL> rsa -in server.key -out server.key
Enter pass phrase for server.key:
writing RSA key
OpenSSL>
```

Secure private key from being read by executing the following:

```
#chmod 400 /etc/httpd/conf/ssl.key/server.key
```

Apache server should now be restarted, as follows:

```
#httpd restart.
```

Installation of private key is successfully completed.

### 3.3. Installing certificate of server

After pasting ID at CERTUM's website, you will receive an e-mail message with the certificate of your server. You should copy and paste it to any text editor (i.e. Notepad) and save it as, i.e. *server.crt*.

#### Note!

The certificate should be copied and pasted from line „--BEGIN CERTIFICATE - „ to „-END CERTIFICATE--” with these lines.

Please, do not use Word or any other text processor.

In case the certificate file has been lost, you should remember, that it can be found at the beginning of *ca-bundle.crt* file (to have it back you can just copy and paste it from there). Second possibility is to search for it in repositories at CERTUM's websites.

To install server's certificate copy (using Midnight Commander or Command Line) file with the certificate to directory where it will be kept, i.e.:

```
/etc/httpd/conf/ssl.crt/server.crt
```

The *ssl.conf* file will look like the following:

```
SSLCertificateFile /etc/httpd/conf/ssl.crt/server.crt
```

Restart the server and execute the following:

```
#httpd restart
```

Installation of private key is now successfully completed.

After the DNS server has been configured to operate with your domain (or subdomains), HTTP server will be able to handle unequivocal and ambiguous addresses (if any virtual hosts have been added, see chapter 5).

If you do not have your own DNS server, please contact with your ISP (Internet Service Provider).

#### Note!

Keys and certificates can be kept in one file. In this case you should append to *ca-bundle.crt* file private key and change configuration in *ssl.conf* file accordingly.

```
SSLCertificateFile /path_to_file/ca-bundle.crt
```

```
SSLCACertificateFile /path_to_file/ca-bundle.crt
```

```
SSLCertificateKeyFile /path_to_file/ca-bundle.crt
```

## 4. Authenticate to server using certificate

To enforce client to store certificate in SSL.conf file, add and execute the following lines:

```
SSLVerifyClient require (enforces client's certificate)
```

```
SSLVerifyDepth 10 (max depth of certificate's path)
```

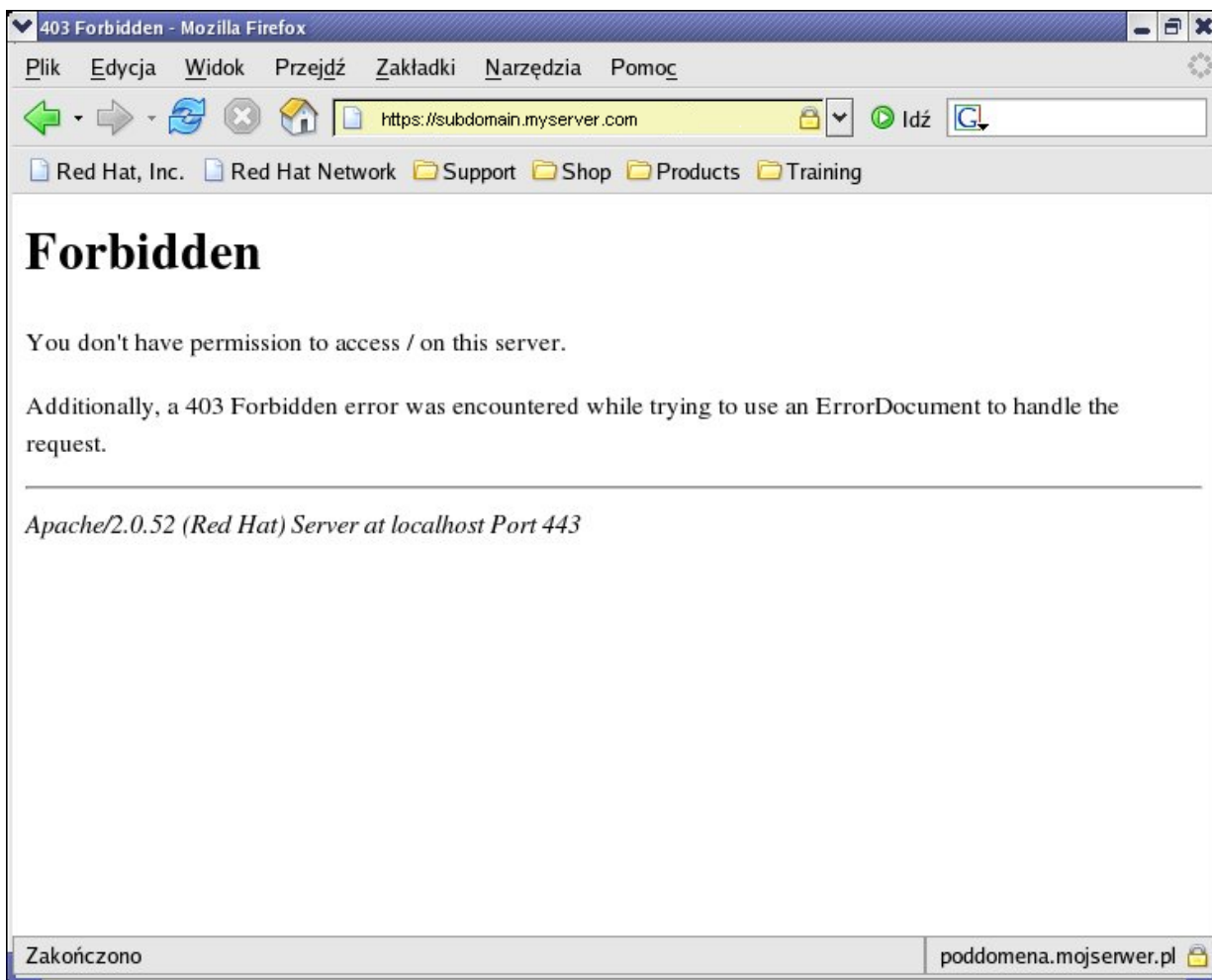
To restrict access to websites only for some clients, i.e. clients having certificate Certum Level III with serial number 02F110 you should add in *ssl.conf* file (in section Location) the following lines:

```
<Location />
```

```
SSLRequire ( %{SSL_CLIENT_I_DN_CN} eq "Certum Level III" and  
%{SSL_CLIENT_M_SERIAL} eq "02F128")
```

```
</Location>
```

When client does not have permissions to access the website, error message will be displayed:



Save the `ssl.conf` file and restart the server:

```
#httpd restart
```

You can find more information at <http://httpd.apache.org/>

## 5. Virtual hosts for ambiguous addresses

In order to allow many virtual subdomains (with Wildcard certificates) to work on one server you need to change the `ssl.conf` file, add lines as follows:

```
NameVirtualHost ip_address_of_server:443
```

- First VirtualHost section:

```
<VirtualHost ip_address_of_server:443>
```

Location of the `www` files:

```
DocumentRoot /var/www/html1
```

DNS name of virtual host:

```
ServerName subdomain1.myserver.pl
```

To enable `ssl` sessions:

```
SSLEnable
```

No changes for further lines:

```
...  
</VirtualHost>
```

- Second VirtualHost section:

```
<VirtualHost ip_address_of_server:443>
```

```
DocumentRoot /var/www/html2
```

```
ServerName subdomain2.myserver.pl
```

```
SSLEnable
```

```
...  
</VirtualHost>
```

Save changes and restart server:

```
#httpd restart
```

When DNS server is configured to operate with your domains (if you do not have your own DNS server, please contact with your ISP), Apache server is ready to handle certificates for ambiguous addresses.

Start Apache server to check if VirtualHosts are working as expected:

```
#httpd start
```

Open web browser and go to:

- <https://subdomain1.myserver.pl>
- <https://subdomain2.myserver.pl>

When session is encrypted, padlock icon appears on the bottom of the browser.



In case of any problems, tools like nmap, ps, netstat, openssl or s\_client might help to resolve the problem.

## 6. The SSL and TLS protocols for VirtualHosts

### 6.1. Configuring VirtualHosts without SSL protocol

Apache server allows to configure more than one website on one physical server. On the basis of HTTP headers or addresses in IP packets server can find requested website. There are two types of VirtualHosts:

- based on names,
- based on IP addresses.

First method allows to run more than one website on one physical server, which has only one public IP address assigned. In this case request for the website is handled on the basis of HTTP headers.

Method based on IP addresses allows to run more than one website on one physical server, which has more than one public IP address assigned. This means, that Apache server has as many IP addresses as VirtualHosts. From the client's point of view there are many hosts handling many websites but actually there is only one physical server with many Virtualhosts handling many websites. When client requests for a website, DNS server is resolving the website (fqdn) to IP address and passes IP address back to the client.

In order to configure VirtualHosts you need to edit httpd.conf and VirtualHosts configuration files. Usually there are located in /etc/apache2 and /etc/apache2/sites-enabled directory (on Linux).

#### Note!

**Depends on operating systems and versions of servers paths to configuration files can vary. Check the documentations of operating systems or version of servers for proper paths.**

In main configuration file (httpd.conf) find following line:

```
#Include conf/extra/httpd-vhosts.conf
```

And uncomment the line (delete the “#” key).

Now, edit configuration files of VirtualHosts. The content of files should be similar to:

```
<VirtualHost 11.100.10.109:80>
    ServerAdmin admin@certum.eu
    DocumentRoot /var/www/html1
    ServerName site1.local
    ServerAlias site1.local
    ErrorLog "logs/site1.local.log"
    CustomLog "logs/site1.local-access.log" common
</VirtualHost>
```

```
<VirtualHost 11.100.10.110:80>
    ServerAdmin jmila@certum.eu
    DocumentRoot /var/www/html2
    ServerName site2.local
    ServerAlias site2.local
    ErrorLog "logs/site2.local.log"
    CustomLog "logs/site1-access.log" common
</VirtualHost>
```

Line `<VirtualHost 11.100.10.109:80>` shows that server will listen on network interface with IP address 11.100.10.109 and port 80. Next lines describe name of the server, paths to files and log files.

This configuration shows how VirtualHosts using method based on IP addresses should be configured. Each VirtualHost has different IP addresses assign. If two or more VirtualHosts have the same IP address assign it will be method based on names.

## 6.2. Configuring VirtualHosts with SSL protocol

### Note!

**In order to configure SSL/TLS protocol for more than one website, each website should have its own VirtualHost using based on IP addresses method.**

This document assumes that server's administrator owns proper amount of valid certificates with private keys. All of the certificates and keys are saved in `/etc/apache2/ssl` directory. Private keys should not

have passwords. If they are secured by passwords, starting SSL/TLS protocols without entering correct passwords will not be possible. To remove password from the private key, execute the following:

```
openssl rsa -in protected.key -out clear.key
```

First step to configure VirtualHosts is editing the main configuration file, look for the following line:

```
#LoadModule ssl_module modules/mod_ssl.so
```

And uncomment (delete the “#” key) the line. Next, look for the following line:

```
#Include conf/extra/httpd-ssl.conf
```

And uncomment this line. Save changes to the file and edit *httpd-ssl.conf*.

Switch on SSL protocol on 443 port, changing:

```
Listen 443
```

,to:

```
Listen 443 https
```

Most important to configure are VirtualHosts. To configure VirtualHosts with SSL/TLS protocols use configuration files from VirtualHosts without SSL/TLS protocols and make following changes:

```
<VirtualHost 10.100.10.109:443>
DocumentRoot "/etc/apache2/sites-enabled/site1.local"
ServerName site1.local
ServerAdmin admin@certum.eu
ErrorLog "/var/log/apache2/error.log"
TransferLog "/var/log/apache2/access.log"
SSLEngine on
SSLCipherSuite
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
SSLCertificateFile "/etc/apache2/SSL/site1.local/site1.local.pem"
SSLCertificateKeyFile "/etc/apache2/SSL/site1.local/site1.local.key"
SSLCACertificateFile "/etc/apache2/SSL/ca-bundle.cer"
</VirtualHost>
```

The most important changes:

SSLEngine on – switches on SSL/TLS protocols in this VirtualHost

SSLCipherSuite  
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL – shows what algorithms are used during transfer encrypted data.

SSLCertificateFile – defines path to file with server's certificate.

SSLCertificateKeyFile – defines path to file with private key matching server's certificate given in SSLCertificateFile directive.

SSLCACertificateFile – defines path to file with Unizeto's (from Level I to Level IV) certificates.

For next VirtualHosts you need to change the IP address and paths to files, as following:

```
<VirtualHost 10.100.10.110:443>
DocumentRoot "/etc/apache2/sites-enabled/site2.local"
ServerName site2.local
ServerAdmin admin@certum.eu
ErrorLog "/var/log/apache2/error.log"
TransferLog "/var/log/apache2/access.log"
SSLEngine on
SSLCipherSuite
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
SSLCertificateFile "/etc/apache2/SSL/site2.local/site2.local.pem"
SSLCertificateKeyFile "/etc/apache2/SSL/site2.local/site2.local.key"
SSLCACertificateFile "/etc/apache2/SSL/ca-bundle.cer"
</VirtualHost>
```

Please note that, IP addresses of VirtualHosts has changed. This means that all of the VirtualHosts should have different IP addresses as well as different certificates with private keys.