



User's guide

APACHE 2.0 + SSL – Linux

Using non-qualified certificates with
APACHE 2.0 + SSL – Linux

version 1.3

Table of contents

1. PREFACE	3
2. GENERATING CERTIFICATE	3
2.1. GENERATING REQUEST FOR CERTIFICATE (CSR)	3
2.2. GENERATING CERTIFICATE ON THE BASIS OF REQUESTED CSR.....	5
2.3. IMPORT OF CERTIFICATES	7
3. INSTALLING KEYS AND CERTIFICATES	9
3.1. INSTALLING CERTUM CERTIFICATES	9
3.2. INSTALLING PRIVATE KEY	9
3.3. INSTALLING CERTIFICATE OF SERVER.....	10
4. AUTHENTICATE TO SERVER USING CERTIFICATE.....	11
5. VIRTUAL HOSTS FOR AMBIGUOUS ADDRESSES.....	12
6. THE SSL AND TLS PROTOCOLS FOR VIRTUALHOSTS	13
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/>

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 server's CSR certificate, which will be saved in *server.csr* file. You should remember to point to 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 pop3.test.net
- **Email (Email)** – enter administrator's e-mail address of the server, i.e. cunizetowski@certum.eu

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

- for unequivocal address – i.e. www.mysite.com, 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, *.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-----  
MIIDMCCApkCAQAwZoxGzAZBgNVBAMTEmRsdWJhY3oudW5pemV0by5wbDEhMB8G  
A1UECxMYRHppYWwgT2Nocm9ueSBJbmZvcmlhY2ppMRswGQYDVQQKEkJVbml6ZXRv  
IFNwLiB6IG8uby4xETAPBgNVBACTCFN6Y3plY2luMRswGQYDVQQIEiExJaYWNob2Ru  
aW9wb21vcnNraWUxZCZAJBgNVBAYTA1BMMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB  
iQKBgQC8JvRqRPbltoZyvMjfxCef5PIcyLMQv6Z2A10j2GMoeKBCCyZF1kHoDsWW  
0ZF54FrTZhyKwYqfgiHO5duLfJSBqb/PTzovZH9qXUtxl+zQIhcJnA4Z/jKyWHG1  
X7LUlC9u2bas/vWwQZWYvxeqNMW4RZ+LU9Qqm9b/YD2qtOZ2qwIDAQABoIIBUzAa  
BgorBgEEAYI3DQIDMQwWCjUuMC4yMTk1LjIwNQYKKwYBBAGCNwIBDjEnMCUwDgYD  
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, fill request form out and paste CSR at the CERTUM website (www.certum.eu -> Offer -> Choose the certificate you would like to buy and click on the Buy button).

Your certificate request

Enter your certificate request (CSR) compliant with PKCS#10 in the following field:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDMDCCApkCAQAwZ0xGzAZBgNVBAMTEmRsdWJhY3oudW5pemV0by5wbDEhMB8G
A1UECkMYRHp p YW w g T 2 N o c m 9 u e S B J b m Z v c m 1 h Y 2 p p M R s w G Q Y D V Q Q K E x J V b m I 6 Z X R v
IFNwLiB6IG8ub y 4 x E T A P B g N V B A c T C F N 6 Y 3 p I Y 2 l u M R s w G Q Y D V Q Q I E x J a Y W N o b 2 R u
a W 9 w b 2 1 v c n N r a W U x C z A J B g N V B A Y T A I B M M I G f M A 0 G C S q G S I b 3 D Q E B A Q U A A 4 G N A D C B
i Q K B g Q C 8 J v r q R P b l t o Z y v M j f X C e f 5 P I c y L M Q v 6 Z 2 A l O j 2 G M o e K B C C y Z F 1 k H o D s W W
O Z F 5 4 F i T Z h y K w Y q f i H O 5 d u L f J S B q b / P T z o v Z H 9 q X U t k I + z Q I h c J n A 4 Z / j K y W H G I
X 7 L U I C 9 u 2 b a s / v W w Q Z W Y v x e q N M W 4 R Z + L U 9 Q q m 9 b / Y D 2 q t O Z 2 q w I D A Q A B o I I B U z A a
B g o r B g E E A Y I 3 D Q I D M Q w W C j U u M C 4 y M T k 1 L j I w N Q Y K K w Y B B A G C N w I B D j E n M C U w D g Y D
V R O P A Q H / B A Q D A g T w M B M G A 1 U d J Q Q M M A o G C C s G A Q U F B w M B M I H 9 B g o r B g E E A Y I 3 D Q I C
M Y H u M I H r A g E B H l o A T Q B p A G M A c g B v A H M A b w B m A H Q A I A B S A F M A Q Q A g A F M A Q w B o A G E A
-----
```

Attention! Cryptographic keys in CSR must have at least 2048 bit length (for RSA or DSA algorithms) and 571 bit length (for EC algorithms: NIST K-571 and NIST B-571). CSR with shorter key length will not be processed.

E-mail address

Enter your e-mail address to receive further instructions.

E-mail:

Invoice details

I would like to receive an invoice of my purchase.

Cash Payment

I will pay 369.00EUR by Credit Card [PayPal](#)
 The payment was made with activation card

Statement

PLEASE READ THE FOLLOWING NOTICE BEFORE YOU REQUEST OR CONFIRM A CERTIFICATE OR USE IT FOR YOUR FIRST SIGNATURE. DO NOT REQUEST, CONFIRM OR USE THE CERTIFICATE UNLESS YOU AGREE TO THE TERMS AND CONDITIONS OF THE FOLLOWING DECLARATION.

The following declaration will come into effect once you send your request for issuing a certificate to CERTUM - Powszechne Centrum Certyfikacji. By requesting the issue of a certificate, you ask the issuer to review the request and issue the certificate. At the same time, you acknowledge the terms and conditions of the certificate.

I agree

Next

Note!
The certificate should be copy and paste from line „--BEGIN CERTIFICATE - „ to „--END CERTIFCATE--” 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 correct value is in the subject field (if you are buying certificate for domain www.mydomain.com please, make sure that this name is in the subject field.

If all details are correct, click on Next:

Buy Wildcard Domain

Data validation

i The following information is included in your certificate request. If you need to modify the data, cancel this form and prepare a new PKCS#10 request

Country:	PL
State:	Zachodniopomorskie
City:	Szczecin
Company:	Unizeto Technologies S.A.
Branch/Office/Organisational Unit:	Dzial Wdrozen
Common name:	www.unizeto.eu
E-mail:	cunizetowski@unizeto.pl
Key Length:	RSA 2048bit

New window shows the information of all documents needed to complete the process of buying certificate.

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 and paste ID number to activate certificate:

Installation ID of certificate : b7b1610e652ec1bddbd7e247508dca82a8a5e6a9

Please, paste this number at:

<https://www.certum.eu/>

--

Unizeto CA

info@certum.eu

Go to website address, paste ID number and click Next.

Installation

Enter Certificate's number given in e-mail message from CERTUM:

New window will appear with the details of the certificate:

Installation

Private WEB Server	valid to : 13.06.2007
Podmiot: 10.100.10.122	
Email: mproszkiewicz@certum.pl	
Numer: 0x37CCC	
<input type="button" value="Install"/>	

Copy number of the certificate, go to <http://www.certum.eu/services/search.html> and paste certificate's number in the Serial Number field.

Start > Manage certificate > Search for certificates

Search for certificates

Search for certificates

 Enter the e-mail address or common name (first and last names or the WWW server address) or serial number to find the certificate.

E-mail:

Common name:

Serial no.:

New website will appear with two options of saving the certificate:

- in binary form,
- in text form.

Searching non-qualified certificate

Private WEB Server	Valid to : 13-06-2007	
Subject: 10.100.10.122		
Number : 0x37CCC		
Status: Valid		
<input type="button" value="Save"/>	<input type="button" value="Save as text"/>	<input type="button" value="Save as binary"/>

3. Installing keys and certificates

3.1. Installing CERTUM certificates

Besides the server's certificate that has been installed, there also should 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)
```

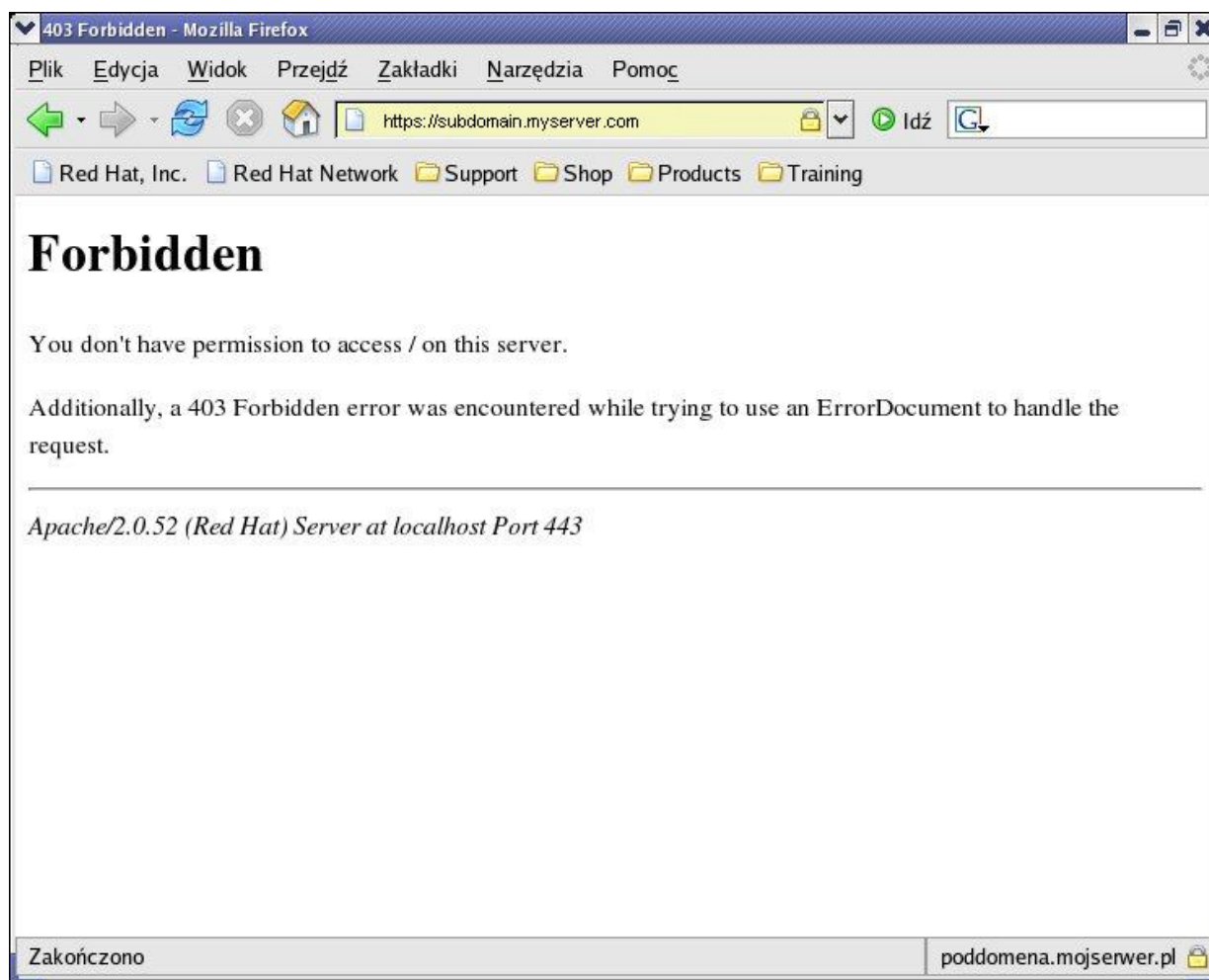
To restrict access to websites only for some clients, i.e. clients having certificate Certum Level III with serial number 02F110 you should add in *ssl.conf* file (in section Location) the following lines:

```
<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 to 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.

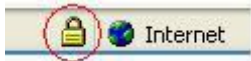
Start Apache server to check if VirtualHosts are working as expected:

```
#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 point of view of client 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 this 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.