






Belgian eID Authentication Reverse Proxy User's guide

For
Fedict

From
CSC Computer Sciences



Table of Contents

1.	<i>Introduction.....</i>	3
2.	<i>Architecture.....</i>	4
2.1	<i>Infrastructure.....</i>	4
2.2	<i>Application access control.....</i>	5
3.	<i>Solution description</i>	6
4.	<i>Prerequisites and limitations</i>	7
4.1	<i>Notation.....</i>	7
4.2	<i>Wizard.....</i>	7
4.3	 <i>Windows</i>	7
4.4	 <i>Unix.....</i>	8
4.5	 <i>Known issues</i>	9
5.	<i>Installation</i>	11
5.1	 <i>Windows</i>	11
5.2	 <i>Unix.....</i>	13
5.3	<i>Customisation.....</i>	15
5.4	<i>Proxy and SSL Configuration.....</i>	16
5.5	<i>Install Government Certificates</i>	17
5.6	<i>Install Server Certificate</i>	18
5.7	<i>Configure security parameters</i>	20
5.8	<i>Server restart.....</i>	21
6.	<i>Usage</i>	22
6.1	<i>Retrieving citizens' certificate information</i>	22
6.2	<i>Restricting access to a path requiring SSL authentication</i>	22
6.3	<i>Logging OCSP answers</i>	23
6.4	<i>SSL Error Redirection</i>	23
6.5	<i>CRL</i>	25
6.6	<i>Certificates validation.....</i>	25
7.	<i>License issues</i>	26
7.1	<i>EID Authentication Reverse Proxy license agreement.....</i>	26
7.2	<i>Third-party licenses</i>	29
8.	<i>Software History.....</i>	36
9.	<i>Document History.....</i>	39

1. INTRODUCTION

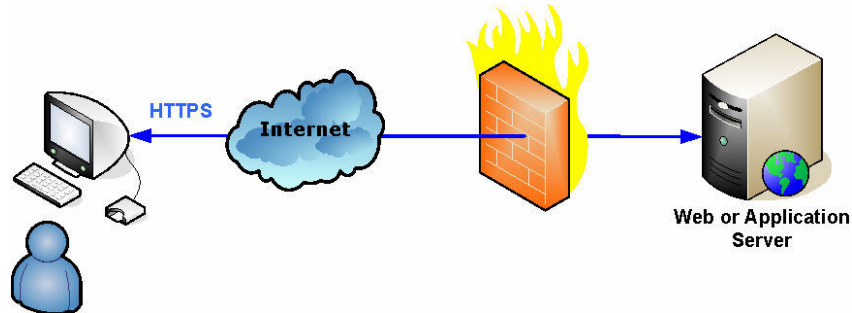
This document describes the usage of the “*Belgian EID Authentication Reverse Proxy*” – being referred here as “*the reverse proxy*”. This reverse proxy is a multi-platform solution for authenticating citizens with their eID card on a Web Server (like Microsoft IIS, or Apache), or an Application Server (like IBM Websphere, Weblogic, or Tomcat). We will refer this server as “*the Application Server*”, although it could be a simple Web Server.

The main goal of this guide is to explain the architecture, the installation, the usage, and the parameterisation of this reverse proxy.

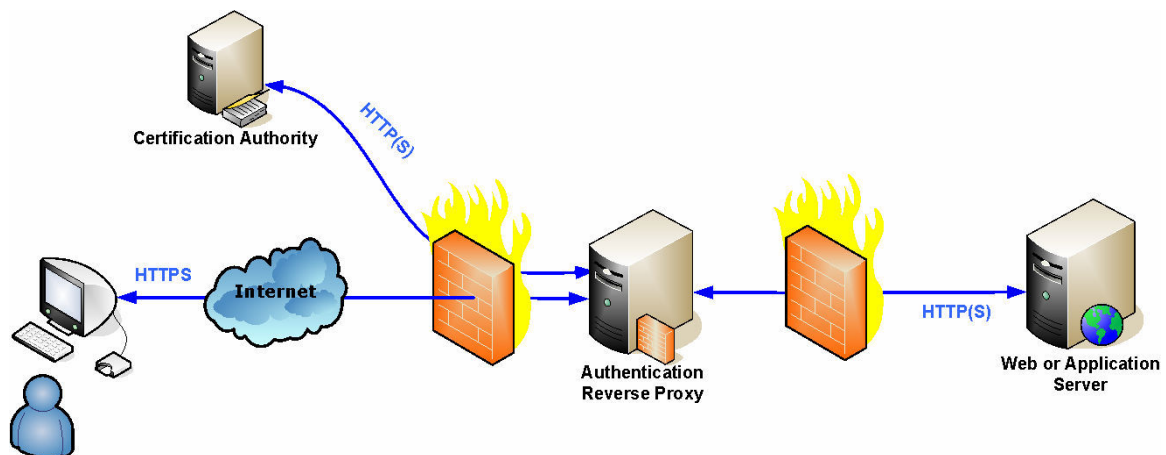
2. ARCHITECTURE

2.1 Infrastructure

In the most simple situation, the user's browser connects directly to the Application Server.



In order to add an authentication step, we will add the reverse proxy between the user's browser and the Application Server. The reverse proxy may (should) contact the **Certification Authority** to check the certificates validity – that is, that they have not been *revoked*.



Note that a “normal” reverse proxy is often installed for other technical and security reasons, like not having the users directly connected to it.

We represented here the most common architecture, with the reverse proxy between two firewalls – in a zone called DMZ, but the solution would also work with the reverse proxy installed on the same machine as the Application Server¹.

¹ In this case, the Application Server must run on other ports than the standard ones, as the standard ones will be used by the reverse proxy.

2.2 Application access control

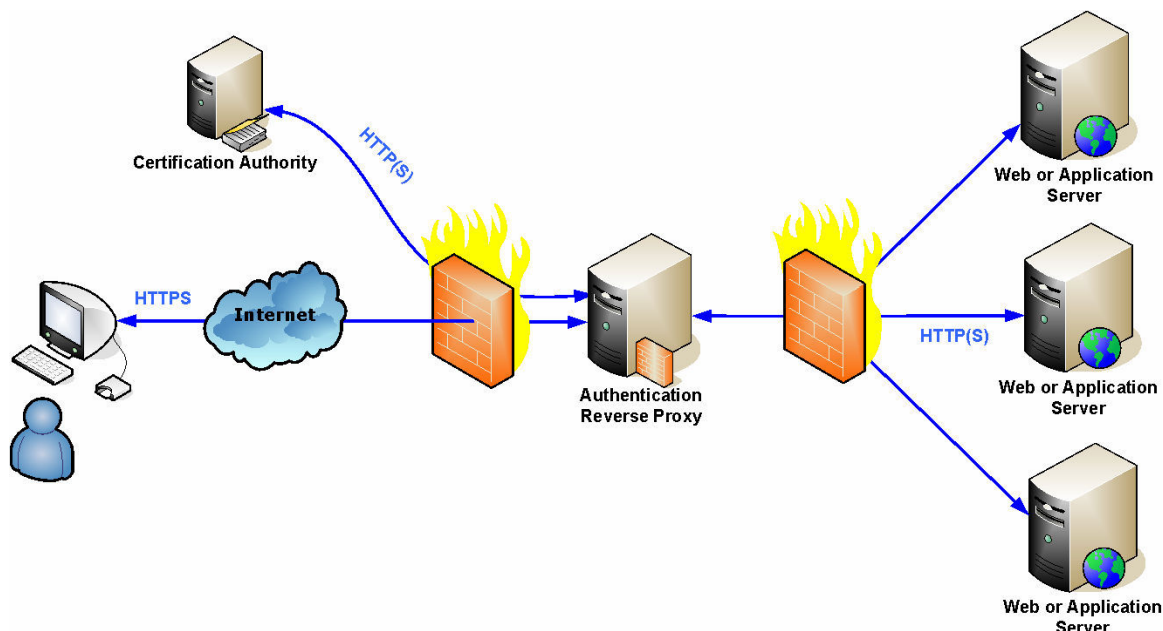
In order to integrate an access control mechanism in your Web application, you need to receive the citizen's information. This information is provided in HTTP headers, that are usually mapped by your Application Server to environment variables.

In case of a Web Server with static pages, the reverse proxy may also be used to limit the access to some parts of the site to specific people.

The detailed information is described in chapter 6.2.

3. SOLUTION DESCRIPTION

The reverse proxy is a customised version of the open source reverse proxy and Web Server *Apache* (<http://www.apache.org>). Apache itself allows a much more complex architecture than the one described above, like – for example – having one authentication reverse proxy for several applications.



All the usual *Apache* features will be available, although only the authentication part for simple architectures will be discussed in this document.

Customisations added to the default Apache package:



- Updated version of “mod_ssl” to support the OCSP protocol²
- External module to trap certificates validation errors and to redirect to a HTTP URL³
- Updated version of “mod_headers” to export SSL headers⁴
- Several bug fixes – see chapter 8
- Installation of the Belgian Government Root Certificate
- “Wizard” to automate the configuration of a simple architecture

² Submitted to the Apache group for inclusion in a next version (http://nagoya.apache.org/bugzilla/show_bug.cgi?id=31383).

³ This required a modification in “mod_ssl” – Submitted to the Apache group for inclusion in a next version (http://nagoya.apache.org/bugzilla/show_bug.cgi?id=35083).

⁴ To be included in future versions, see http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/metadata/mod_headers.c?r1=1.49&r2=1.50

4. PREREQUISITES AND LIMITATIONS

-  You must have administration privileges on the machine in order to install the software.
-  Port 80 and 443 must be free; any other service or application using them must be stopped (like a Web server)

For more information, see the Apache Documentation <http://httpd.apache.org/docs-2.0/>; this documentation will also be installed locally.

4.1 Notation

In the following chapters, the commands to be executed, or the parameters to adapt in the configuration files use the following syntax:

- All commands or parameters are written in a grey box

```
tar xvfz openssl-0.9.7f.tar.gz
```

- Everything that must be replaced by your own data is in italic bold green

```
ServerName myservername:80
```

- Comment may be added in small italic brown

```
ServerName myservername:80 you must use the full domain name
```

4.2 Wizard

The “wizard” configure Apache Web Server as a Reverse Proxy to a single remote server. Advanced features like Virtual servers, caching, Reverse Proxy to several remote servers, ... must be installed manually.

4.3 Windows

- Microsoft Windows 2000 server or upper (a workstation could be used for tests)
- Microsoft Windows Installer 2.0 must be installed.
- IIS, if installed, must be stopped

4.4 **Unix**

For all platforms, except Windows, Apache must be compiled on the target machine.

In order to compile Apache, the following programs must be available :

- gcc
- gawk
- flex ?
- gunzip

The following shared objects must be available in order to run Apache

- libiconv 1.8
- lzlib 1.1.4

4.4.1 **Linux**

- All needed programs and shared objects are usually installed with all Linux distributions

4.4.2 **Solaris**


- zlib is usually installed
- Warning: on some version the program *ar* (needed to create dynamic modules) is located in */usr/ccs/bin*, which is not included in the path !

4.5 Known issues

4.5.1 Apache bugs

 Do not use session caching parameter “*dbm*”, as this introduces memory leaks; the best parameter is usually “*shmcb*”

```
SSLSessionCache shmcb:...
```

 When a user tries to reconnect a page in SSL with an invalid certificate (revoked, suspended, ...), Apache does not validate the certificate again if it is still in its cache; it immediately rejects it. In this case, the SSL error handling module is notified about the error, but it does not receive the “*location*” context: it traps the error in the “*virtual host*” context. So, if redirected pages were defined in “*location*” contexts, they are ignored.

As only the “*virtual host*” context will be used in this case, be sure either to only define you SSL error pages at the “*virtual host*” level, or, at least, to add some pages at the “*virtual host*” level.

Example:

```
<VirtualHost _default_:443>
...
<Location /sub>
    SSL_Error_DefaultURL "/error/invalid.html"
    SSL_Error_URL      23  "/error/revoked.html"
    SSL_Error_URL      10  "/error/expired.html"
</Location>
...
</VirtualHost>
```


becomes:

```
<VirtualHost _default_:443>
...
    SSL_Error_DefaultURL "/error/invalid.html"
    SSL_Error_URL      23  "/error/revoked.html"
    SSL_Error_URL      10  "/error/expired.html"
...
</VirtualHost>
```


or:

```
<VirtualHost _default_:443>
...
    SSL_Error_DefaultURL "/error/invalid.html"
    SSL_Error_URL      23  "/error/revoked.html"
    SSL_Error_URL      10  "/error/expired.html"
    <Location /fr>
        SSL_Error_DefaultURL "/error/invalid_fr.html"
        SSL_Error_URL      23  "/error/revoked_fr.html"
        SSL_Error_URL      10  "/error/expired_fr.html"
    </Location>
...
</VirtualHost>
```

4.5.2 Microsoft Internet Explorer bugs


 Some versions of *Microsoft Internet Explorer* do not correctly support one specific encryption algorithm (RC4/RSA/64 bits); this should be disabled from the list of allowed algorithms:

```
SSLCipherSuite -ALL:SSLv3+HIGH:-aNULL: !EXPORT56:RC4+RSA
SSLProtocol -ALL +SSLv3 +TLSv1
```

 Some versions of *Microsoft Internet Explorer* do not correctly support the SSL protocol (see <http://support.microsoft.com/default.aspx?kbid=831167>). In order to be compatible with these versions, the following directive may be used:

```
SetEnvIf User-Agent ".*MSIE [456].*" ssl-unclean-shutdown
```



Some rare versions of *Microsoft Internet Explorer* 6.0 (after *Windows XP* Service Pack 2) do not work with this configuration. In this case, the browser needs to be updated (typically, with *Windows/Microsoft Update*).

 Some versions of *Microsoft Internet Explorer* do not work correctly if SSL connection reuse is not enabled on the server. To enable it, use the directive

```
SSLSessionCache shmcb:...
```

Remark: other mechanisms can be used than “*shmcb*”

4.5.3 Installation issues

  Under Solaris, the build does not find the library *libgcc_s.so.1* (see http://issues.apache.org/bugzilla/show_bug.cgi?id=33696). To solve it, set the environment variable *LD_LIBRARY_PATH* to the path in the GCC installation tree where *libgcc_s.so.1* resides.

5. INSTALLATION

Here is a high-level description of the installation steps:

1. Install (customised version of) Apache
2. Install OpenSSL
3. Configure Apache as a secured reverse proxy
4. Add Belgian Government Root certificate
5. Create a server certificate request
6. Ask a certificate to a certification authority
7. Install the server certificate

A wizard is provided to automate the steps. This wizard creates and installs a self-signed server certificate. Before going in production, you must ask a real one to a real Certification Authority.

The provided Unix distribution already contains the new modules in the source code.

Step 3 may be re-run to modify the configuration later.


5.1 Windows

 You must log in as **Local Administrator**.

This section describes all the steps to install and configure the software.

The steps can be automated with the provided script “*install.bat*”.

5.1.1 Delete previously installed Apache configuration files

 The Apache uninstall procedure keeps the previous settings. In case you previously installed Apache, and uninstall it, you must manually delete the whole Apache program folder and sub-folders; otherwise, the configuration of the old version will be re-used, which is usually not advisable.

5.1.2 Install Apache

The installation consists in a MSI package.

Execute the install file “**apache_2.0.54-win32-x86-no_ssl.msi**”

- Some information must be supplied :
 - *License agreement* : Select “I accept ...” and click on Next button
 - *Read this first* : Click on Next button
 - *Server Information* : Fill in all fields and click on Next button
 - **Network Domain**: your domain name, like “*mycompany.com*”
 - **Administrator’s Email Address**: ...
 - The checkbox “*for all users on port 80, as a service – recommended*” must be selected.
- ⓘ If you cannot select port 80 (only port 8080 for current user), you may not have Administrator’s privileges.
- *Setup type* : use **Typical** (default choice) and click on Next button
- *Destination Folder* : Keep default directory and click on Next button
- *Ready to install the program* : Click on Install button .
- *Installation Wizard completed* : Click on Finish button

5.1.3 Install mod_ssl and OpenSSL

All directories – except the ones located under **%SystemRoot%** are relative to the Apache installation directory (by default: “C:\Program Files\Apache Group\Apache2”)

- copy “**mod_ssl.so**” to directory “**modules**”
- copy “**mod_headers.so**” to directory “**modules**”
- Install **OpenSSL 0.97f** (higher versions are not compatible with this Apache version)
- Check that files “**libeay32.dll**” and “**ssleay32.dll**” were copied in system directory “**%SystemRoot%\system32**”
- Create the directory “**conf\ssl**”

5.1.4 Install additional module mod_ssl_error

- copy “**mod_ssl_error.so**” to directory “**modules**”

5.1.5 Configure Apache

See 5.3

5.1.6 Install the Belgian Government Root Certificate

See 5.5

5.1.7 Obtain and Install the Server Certificate

See 5.6

5.1.8 Create and start Apache2SSL Service

Delete Apache2 service (automatically created during Apache Installation)

```
bin\apache.exe -w -k stop -n "Apache2"  
bin\apache.exe -w -k uninstall -n "Apache2"
```

Create Apache2SSL service :

```
bin\apache.exe -w -k install -n "Apache2SSL" -D SSL
```

Start Apache2SSL service


```
bin\apache.exe -w -k start -n "Apache2SSL"
```

5.1.9 Starting and stopping the application

The service is started automatically by the installation procedure.

The Apache Monitor is also automatically started, an icon is available in the system tray to start/stop/restart the service.


5.2 Unix

 Execute all following commands as *root*.

This section describes all the steps to install and configure the software.

5.2.1 Automatic installation

The steps can be automated with the provided script “./install.sh”. This does not encompass the daemon installation.

 The default distribution of the files is a ZIP file. In this case, the shell scripts are not marked as executable. To mark them as executable, use the following command:

```
Chmod +x *.sh
```

5.2.2 Manual installation

5.2.2.1 Install OpenSSL

```
tar xvfz openssl-0.9.7f.tar.gz.tar  
cd openssl-0.9.7f  
./config  
make  
make test  
make install
```

5.2.2.2 Install Apache

The distributed TAR file contains the modified version of “mod_ssl” and “mod_headers”.

```
tar xvfz httpd-2.0.54_OCSP.tar.gz
cd httpd-2.0.54
make clean
./configure --prefix=/usr/local/apache2
             --enable-modules="ssl proxy headers"
             --with-ssl /usr/local/ssl
make
make install
```

5.2.2.3 Install additional module mod_ssl_error

The distributed TAR file contains the module “mod_ssl_error” (see 6.4).

```
cd modules/mod_ssl_error
apxs -cia /I../openssl/include mod_ssl_error.c
```

5.2.2.4 Configure Apache

See 5.3

5.2.2.5 Install the Belgian Government Root Certificate

See 5.5

5.2.2.6 Obtain and Install the Server Certificate

See 5.6

5.2.2.7 Starting and stopping the application


- Starting the application

```
./apachectl sslstart
```
- Stopping the application

```
./apachectl stop
```
- Restarting the application

```
./apachectl restart
```

5.2.3 Install Apache Daemon

 By default, only the HTTP daemon can be started automatically. In order to automatically start Apache with SSL support, you must add, in the file “**apachectl**”, “**-DSSL**” to the start directive (it does not hurt to add it for all the commands – stop/restart/graceful).

If you want to start Apache automatically when the system boots, you must install daemons. This installation depends on the Unix distribution you are using.

Here is an example to start Apache automatically on Red Hat Linux :

- Change the working directory to the Apache binaries

```
cd /usr/local/apache2/bin
```
- Create a link from the file called “**apachectl**” to the daemon initialization directory

```
ln -s /usr/local/apache2/bin/apachectl /etc/rc.d/init.d/httpd
```
- Register the daemon (replace sequence number 85 depending on other daemon installed)



```
cd /etc/rc3.d  
ln -s ../init.d/httpd S85httpd  
ln -s ../init.d/httpd K85httpd  
cd /etc/rc5.d  
ln -s ../init.d/httpd S85httpd  
ln -s ../init.d/httpd K85httpd
```

5.3 Customisation

Customisation of Apache can be executed as many times as you want. In this case, only **Proxy Remote server URL** is asked and the new value introduced replace the old one.

Execute the script “**customise_proxy.bat**” (Windows) or “**./customise_proxy.sh**” (Unix) and follow the instructions.

The scripts asks for the “**Proxy Remote server**”: Fill in the name of the remote Application Server. If “**http://**” omitted at the beginning of the string, it is automatically added.

  The default distribution of the files is a ZIP file. In this case, the Unix shell scripts are not marked as executable. To mark them as executable, use the following command:


```
Chmod +x *.sh
```

5.4 Proxy and SSL Configuration

Update configuration file “conf/httpd.conf”

- Port :

```
Listen 80
```

-  Windows only: mandatory modules. Check that following modules are loaded (remove # at the beginning)

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule ssl_module modules/mod_ssl.so
```

Remark : for Unix, those modules are statically installed.

- Do not use session caching parameter “*dbm*”, as this introduces memory leaks; the best parameter is usually “*shmcb*”

```
SSLSessionCache shmcb:...
```

- Add SSL :

```
<IfModule mod_ssl.c>
    Include conf/ssl.conf
</IfModule>
```

- Add Reverse Proxy :

```
<IfModule mod_proxy.c>
    ProxyRequests off
    ProxyPass / http://remote_server_name_or_address/
    ProxyPassReverse / http://remote.server.name/
</IfModule>
```

More info on http://httpd.apache.org/docs-2.0/mod/mod_proxy.html

- Adapt the number of concurrent requests handled by the server. In case more requests come, they are queued, and thus wait for another to complete before being treated. Note that the OCSP checking – if activated – may take several seconds, thus slowing waiting requests.

For a normal server, 25 concurrent requests should be enough. If you expect a big number of incoming requests, you may increase this number to enhance the response time, however this will require more memory and CPU resource.

```
ThreadsPerChild 25
```


5.5 Install Government Certificates

- Update configuration file “**conf\ssl.conf**”

SSLCACertificateFile	conf/ssl/client-trusted-list.pem
----------------------	----------------------------------

- Add the Belgian Government Root certificate (or any other trusted root if any) to “*client-trusted-list.pem*”. Just concatenate the file to the existing one. The certificate must be in PEM format, like below:

```
# This is the Government Root Certificate
-----BEGIN CERTIFICATE-----
MIID1DCCAnygAwIBAgIQWAsFbFMk2D7JvQxhf+ewmUDANBgkqhkiG9w0BAQUFADAN
MwswCQYDVQGEWJCRTEYMBYGA1UEAxMPQmVsz211bSBsb290IENBMB4XDTAZMDEY
NjIzMDAwMFoXDTE0MDEYNjIzMDAwMFowJZELMAkGA1UEBhMCQkxGDAWBgNVBAMT
D0J1bGdwdWogUm9vYvdCBQDTCASISWQYJzK0ZihvCNAQEgBBQAdgEAPDCAQoCg9Eg
AMihcekcRk35eHFNA6pqsokt03H10swkxvpl9eLS2zhmFfjCwK3HEcVAQGPaaXQS
J4fpnoVxtIis0RIYqjBeoiG52bv/9nTrMQHn035YD5EWtXaJqAFPrSJmcPpLHZXB
MFjyqvn112jq0i0tJR1Lf0lMvdssuXR1Jsw9q0P9vMIt7EU(CT9YvvzW7wCMgtVty
v/cY6pziF5ssofvsY9LKyn0FrMhtB20yvmi4BUCUvj3hwPmbxM0jvxkuXtgfem08S
dkpbNCNUwOpszv42kqgJF+qhLc9s44q03ocumws8d0IhUDiVLZg5cYx+dtA+mqh
pIqTm6cbBocdJ9Peoc1mSG8CAWEAAaObuzCBuDAObgNVHGBA8BAf8EBAMCAQYwDwYD
VR0TAQH/BAUwAwEB/ZBCBgNVHSAEOZAS5MDCGBWA4AQEBMCAwLAIYkWBbBQUHAgEW
IGh0dHA6Ly9yZXBvc210b3J3J5LmVpZC51ZWxnaxvtLmJ1MBOGA1UdDgQWBQ8Axw
m2Hqvz2ZnZdt925FI7b5jARBGlghkgBhvhGAgEABEAMCAAcwHwyDVROjBBGwFOAU
EPmVpht61c6tjyXbZ+/dURSO2+YwDQYJKoZIhvcNAQEFBQAdgEgAMHTI1LKgyfpg
17m7VILKb+Mbcx0YA2s1q52sq+11Ip0XjN9dzowbZV4yveex09ABPHMTjHud79ZC
wT+oq0VPN7p2k0k9Cz0/00RBSZ29wyn0Aiwi3EbV1jZKE4trfta57vJRUQDRSp/
M382StbtobqkCA5c/ciJv0J71/Fg8teH91cuen564Ad30QPXY49cTGXYNSecMqP
8JTHSHVugfmbRxc6CLKP240sj2tr6L/D2fvdw2RV6Gq9NoY2uiGmlxoh10ot06y6
7Kcdq765SpS1LxxCHVGnH1TtEpF/8m6HfubJdNbv6z19511uBPqE5KJYvhzgoaiJe
4r50EAREAQyo=
-----END CERTIFICATE-----
```

i Because of a bug in Internet explorer, you also need to add GlobalSign Root certificate, and restrict accepted certificates to the ones emitted by the Citizen CA – see “*SSLRequire*” directive in 5.7.

The wizard installs all needed certificates, including test ones, but only real ones will be accepted until you add their Distinguished Name in the accepted list – see “*SSLRequire*” directive in 5.7.

5.6 Install Server Certificate

This part heavily uses OpenSSL (<http://www.openssl.org/>). The program (*openssl.exe*) lies in the “*OpenSSL*” subfolder of the Apache program folder.

Either go into that folder to type the commands, or make sure the “PATH” environment variable points to this folder.

Obtain and Install certificates.

- Create a private key and a server certificate signing request

- Generate a Private Key

```
openssl genrsa -out server.key 1024
```

- Edit file “**config.txt**” (at least CN field with server name or IP address).

Example (minimal) :

```
[ req ]
default_bits          = 1024
default_md             = sha1
default_keyfile        = server.key
distinguished_name     = req_distinguished_name
prompt                = no
output_password        =

[ req_distinguished_name ]
C                     = BE
ST                    = Belgium
L                     = City
O                     = Company name
OU                    = Departement
CN                    = server_name
emailAddress          = name@company.com
```

- Generate a certificate signing request file

```
openssl req -config config.txt -out req.csr -new -key
server.key -sha1 -days 2000
```

- Send the file “**req.csr**” to a Certification Authority

- In order to immediately test the environment, you may want to create a self-signed certificate. This is done in the automated wizard.

```
openssl x509 -in req.csr -out server_cert.pem -req
-signkey server.key -days 2000
```

- The Certification Authority returns the certificate (let's call it "*certificates.xxx*"), together with the whole certificate chain. It may be one of the following formats:
 - a. PKCS#7 – usually with an extension **“.P7B”**
 - b. X.509 – usually with an extension **“.CER”** or **“.CRT”**
 - c. PKCS#12 – usually with an extension **“.PFX”** or **“.P12”**
This is only if the CA generated itself the secret key (not advised)

Furthermore, the file may be encoded in

- a. PEM : base-64 encoded
- b. DER : binary

To know the encoding, load the file in a text editor (like **“notepad”**): a PEM-encoded file has one or several line(s) of the form **“-----BEGIN CERTIFICATE-----”**, and **“-----END CERTIFICATE-----”**.

- If needed: convert the certificates *“certificates.xxx”* received from the CA to a list of certificates in PEM format (base-64 encoded)
 - a. If the certificates are a list of X.509 certificates PEM-encoded in a file *“certificates.cer”*, just rename the file to *“server_cert.pem”*
 - b. If the certificates are a list of X.509 certificates DER-encoded in a file *“certificates.cer”*

```
openssl x509 -in certificates.cer -inform DER -out server_cert.pem
```

- c. If the certificates *“certificates.p7b”* are in PKCS#7 format

- i. With OpenSSL

```
openssl pkcs7 -print_certs -in certificates.p7b -out server_cert.pem  
(add “-inform DER” if the file is DER-encoded)
```

- ii. With Windows

- Open *“certificates.p7b”*
- For each certificate
 - Open it
 - Click on the tab **“Details”**
 - Click on **“Copy to file...”**
 - Choose **“Base-64 encoded”**
 - Give a filename *“cert1.out”*, *“cert2.out”*, *“cert3.out”*,...
- Concatenate all certificates (*“*.out”*) to a file *“server_cert.pem”*

```
copy *.out server_cert.pem
```

- Copy Certificates to directory **“conf/ssl”**
 - Certificate *server_cert.pem* (received from CA)
 - Private Key *server.key*

- Update configuration file “**conf/ssl.conf**”

See <http://httpd.apache.org/docs-2.0/ssl/> for details.

- Define Certificates

```
SSLCertificateFile    conf/ssl/server_cert.pem    # from CA
SSLCertificateKeyFile conf/ssl/server.key          # see step 1
```

5.7 Configure security parameters

- Ensure that “SSLRequireSSL” always take the precedence over a “Satisfy any” directive

```
SSLOptions +StrictRequire
```

- Protect the site with client certificates

```
SSLVerifyClient require
SSLVerifyDepth 10
```

- Define the accepted cipher suites and protocols

```
SSLCipherSuite -ALL:SSLV3+HIGH:-aNULL
SSLProtocol    -ALL +SSLV3 +TLSv1
```

- Add OCSP parameters

```
SSLUseOCSP      on    # try to connect to OCSP responder
```

- Force certificates validation

```
# Refuse certificate if specified validation mechanism (OCSP responder, CRL)
# is not available
SSLForceValidation on
```

This directive is used to refuse the certificate in case all the specified validation mechanisms⁵ failed to answer (neither positively, nor negatively).

The following cases are never considered as an error:

- The certificate does not contain the path to the OCSP responder

The following cases are considered as a technical error:

- If OCSP has to be used
 - The OCSP responder is unavailable
 - The OCSP response is incorrect
- If CRL have to be used
 - No CRL is found
 - A CRL is found but is incorrect

In case of a technical error with all specified validation mechanisms, the certificate is accepted if the directive “SSLForceValidity” is set to “off”; it is refused if the directive “SSLForceValidation” is set to “on”


- Accept only SSL connections (refuse HTTP connections)

```
<Location />
SSLRequireSSL
</Location>
```

⁵ Specified with the directives, SSLUseOCSP, SSLCARevocationFile, etc.

- Accept only certificates emitted by Citizen CA

```
<Location />  
# Accept only certificates emitted by Citizen CA  
# If test certificates are also needed, add "SPECIMEN Citizen CA" in the list  
SSLRequire %{SSL_CLIENT_I_DN_C} eq "BE"  
and %{SSL_CLIENT_I_DN_CN} in {"Citizen CA"}  
</Location>
```

 Because of a bug in Internet explorer, you also need to add GlobalSign Root certificate, and restrict accepted certificates to the ones emitted by the Citizen CA.

If you want to accept government test certificates, you need to add them explicitly in the list.

5.8 Server restart

Although the server may run for months without interruption, it is always a good practice to restart it on a regular basis⁶. As the server can be restarted without interrupting the users – see <http://httpd.apache.org/docs-2.0/stopping.html> - we advise to restart it each day or each week.

This also ensures that new CRL are loaded – see 6.5.

⁶ It is always difficult to assure no memory leak will occur in any circumstance

6. USAGE

6.1 Retrieving citizens' certificate information

The Application Server can receive the citizen's distinguished name in a HTTP header; it can use this value to identify the user.

- Add the user's full distinguished name in HTTP header, for example in variable **HTTP_SSL_USERID**.

```
RequestHeader set SSL_USERID "%{SSL_CLIENT_S_DN}e"
```

- Add the user's national number in HTTP header, for example in variable **HTTP_SSL_USERID**.

```
RequestHeader set SSL_USERID \
    "%{SSL_CLIENT_S_DN_serial}Number}e"
```

- If Apache is not used as a proxy, but the Application Server is directly connected to it, the header **REMOTE_USER** can be used. To set it to the user's distinguished name:

```
SSLUserName SSL_CLIENT_S_DN
```

Or the user's national number:

```
SSLUserName SSL_CLIENT_S_DN_serialNumber
```

i Remark: In newer version of Apache (from 2.2), you must use "%{SSL_CLIENT_S_DN}s" to retrieve the certificate's distinguished name – and the same for any SSL-related variable ("%{SSL_...}s").

6.2 Restricting access to a path requiring SSL authentication

If you want to restrict the access to some resources (URL), you may add the following lines to “conf/ssl.conf”:

```
<Location /path>    ex: /admin, or /internal/users/
SSLVerifyClient require
SSLRequireSSL
SSLOptions          +FakeBasicAuth
AuthType Basic
AuthUserFile conf/group.auth
require valid-user
</Location>
```

Then, you must add the complete distinguished name of each user in the file “conf/group.auth”⁷, followed by a colon and the string “xxj31ZMTZzkVA” (without quotes):

```
/C=BE/CN=xxx/SN=xxx/serialNumber=xxx:xxj31ZMTZzkVA
/C=BE/CN=yyy/SN=yyy/serialNumber=yyy:xxj31ZMTZzkVA
```

Or, if you use the user's national number (**SSLUserName SSL_CLIENT_S_DN_serialNumber**), you must only add the national number of each user in the file:

```
xxx:xxj31ZMTZzkVA
yyy:xxj31ZMTZzkVA
```

For more information, see <http://httpd.apache.org/docs-2.0/howto/auth.html>

⁷ Actually, you may use any filename ; this allows to group users by logical functions, etc.

6.3 Logging OCSP answers

Answers coming from the OCSP server are logged in the `mod_ssl` error file. You need to specify the “*LogLevel*” to at least “*Info*”

```
LogLevel info
```

The logging contains the certificate serial number, the certificate’s subject name, and the OCSP answer. If you want to extract only the lines containing answers coming from the OCSP server, you may search for the string “OCSP response”.

6.4 SSL Error Redirection

In case of error during certificates validation, the SSL error may be trapped in order to establish the connection, and the browser may be redirected to an error page.

Note that, if no SSL connection can be established without client certificate (ex: no ciphersuite in common, etc.), no redirection is possible, and the server returns the normal SSL error code.

To enable this feature, the module “`mod_ssl_error`” must be loaded:

```
LoadModule ssl_error_module modules/mod_ssl_error.so
```

Error page customisation

1. If nothing is specified, the server sends an error 403 to the browser.
2. If a default URL is specified, the browser is redirected to that page

```
<IfModule mod_ssl_error.c>  
SSL_Error_DefaultURL "http://.../error/ssl\_valid.html"  
</IfModule>
```

The browser is redirected to

http://.../error/ssl_valid.html?errorNb=N&error=XXX&serial=YYY&dn=ZZZ,

where **N** is the error number returned by the OpenSSL library, **XXX** is the error message, **YYY** is the certificate serial number, **ZZZ** is the certificate distinguished name. A script on the server could thus get the exact error message from the variable/header “error”, and customize the page displayed to the user.

3. If a specific error is specified, the browser is redirected to that page

```
<IfModule mod_ssl_error.c>
SSL_Error_URL 10  "/error/expired.html"
SSL_Error_URL 12  "/error/crl_expired.html"
SSL_Error_URL 23  "/error/revoked.html"
</IfModule>
```

The certificate serial number and distinguished name are included as above.

Valid errors are:

- 2 unable to get issuer certificate
- 3 unable to get CRL
- 4 unable to decrypt certificate signature
- 5 unable to decrypt CRL signature
- 6 unable to decode issuer public key
- 7 certificate signature failure
- 8 CRL signature failure
- 9 certificate not yet valid
- 10 certificate has expired
- 11 CRL not yet valid
- 12 CRL has expired
- 13 error in certificate "not before" field
- 14 error in certificate "not after" field
- 15 error in CRL "last update" field
- 16 error in CRL "next update" field
- 17 out of memory
- 18 depth zero self signed certificate
- 19 self signed certificate in chain
- 20 unable to get issuer certificate locally
- 21 unable to verify leaf signature
- 22 certificate chain too long
- 23 certificate revoked
- 24 invalid certification authority
- 25 path length exceeded
- 26 invalid purpose
- 27 certificate not trusted
- 28 certificate rejected, or no certificate provided
- 29 subject issuer mismatch
- 30 "akid" skid mismatch
- 31 "akid" issuer serial mismatch
- 32 "keyusage" different from "certsign"
- 33 unable to get CRL issuer
- 34 unhandled critical extension
- 35 "keyusage" not for CRL signing
- 36 unhandled critical CRL extension

Important remarks:

- ❑ The URL provided for the redirection should normally use the **HTTP** protocol, not **HTTPS**, otherwise it may provoke another SSL error, resulting in a redirection, ... thus an infinite loop. The URL can be relative; in this case, a HTTP connection is used.
- ❑ Due to a bug, it is better to not use error redirections inside “*locations*”. If you really want to, read the problem description in 4.5.1.

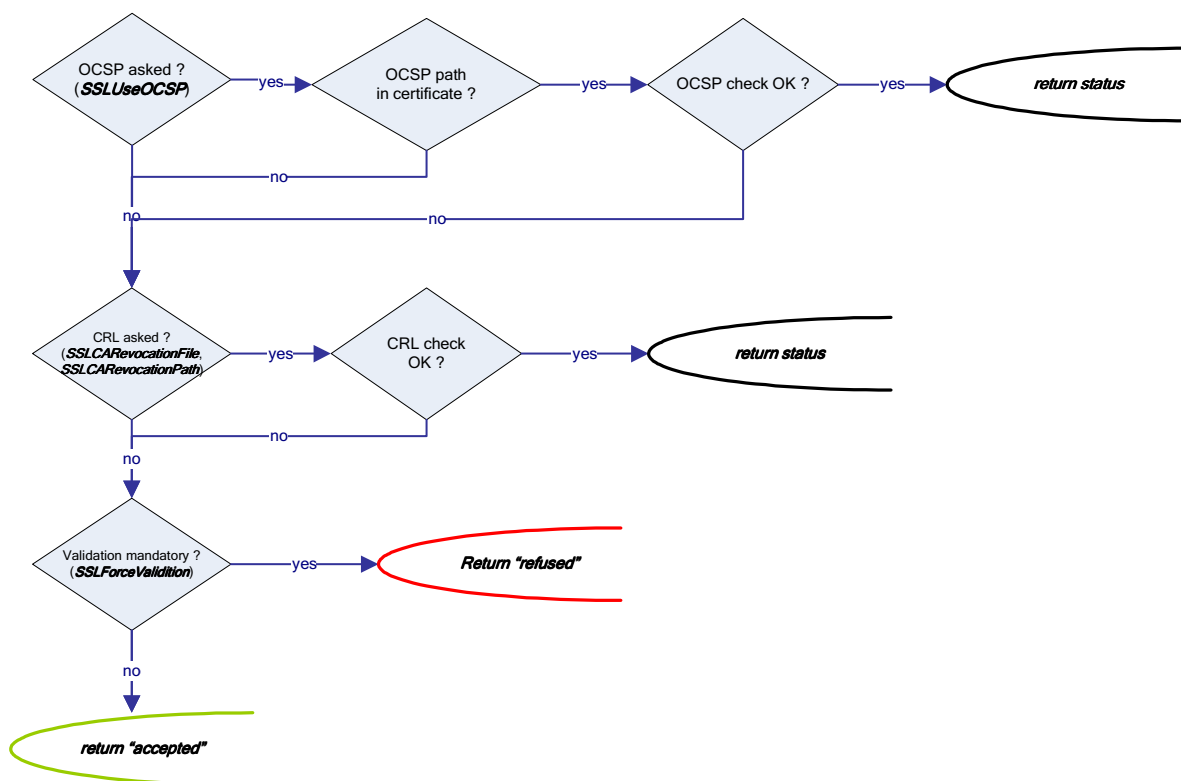
6.5 CRL

CRL can be used to validate certificates – see : http://httpd.apache.org/docs-2.0/mod/mod_ssl.html. New CRL have to be downloaded and installed in the corresponding directory.

CRL are loaded at start-up time. In order to take new CRL into account, the server has to be restarted. Note that the server can be restarted without interrupting the users – see <http://httpd.apache.org/docs-2.0/stopping.html>.

6.6 Certificates validation

Here is the description of the certificates validation mechanism.



Warning: in case no CRL is found (in the specified file or directory), the check is considered as successful.

7. LICENSE ISSUES

The eID Authentication Reverse Proxy use several third-party libraries or code.

Redistributions in any form of the eID Authentication Reverse Proxy– even embedded in a compiled application – must reproduce all the eID Authentication Reverse Proxy, and third-party's copyright notices, list of conditions, disclaimers, and any other materials provided with the distribution.

7.1 *EID Authentication Reverse Proxy license agreement*

IMPORTANT -- READ CAREFULLY BEFORE USING THIS SOFTWARE: Do not install, download or use the eID Authentication Reverse Proxy software until you have read and accepted this Agreement (including its Exhibit). By clicking on the "Accept" button, installing, downloading or otherwise using the eID Authentication Reverse Proxy you agree to be bound by the terms of this Agreement (including its Exhibit). If you do not agree to the terms of this Agreement (and/or its Exhibit), click on the "cancel" button and/or do not install the eID Authentication Reverse Proxy software.

eID Authentication Reverse Proxy Software License

Whereas this eID Authentication Reverse Proxy is being provided by Fedict for no fee and for wide use by any third party under the terms and conditions of this Agreement;

WHEREAS THIS AGREEMENT REFERS TO AN OPEN-SOURCE LIBRARY, BEING ITSELF BASED ON OPEN-SOURCE SOFTWARE, THE TERMS AND CONDITIONS OF WHICH ARE INCLUDED IN THE EXHIBIT, WHICH NEED TO BE COMPLIED WITH BY ANY PARTY USING, REPRODUCING, COPYING, MODIFYING, DISPLAYING AND DISTRIBUTING THE EID AUTHENTICATION REVERSE PROXY;

WHEREAS THIS AGREEMENT DOES NOT TAKE AWAY YOUR FREEDOM TO SHARE THE EID AUTHENTICATION REVERSE PROXY AND CHANGE IT IN ORDER TO ENABLE ITS WIDEST POSSIBLE ROLL-OUT TO OTHER POTENTIAL USERS, PROVIDED THAT SUCH USE IN RELATION TO THE EID AUTHENTICATION REVERSE PROXY COMPLIES WITH THE TERMS AND CONDITIONS SET OUT IN THIS AGREEMENT (INCLUDING ITS EXHIBIT).

Article 1: Grant of license

The terms of this License Agreement ("License Agreement") between you, the licensee, and the Belgian Federal Government ("Fedict"), the Licensor, allow you, subject to the terms and limits set forth in this License Agreement and its Exhibit (collectively "Agreement"), to receive from Fedict a world-wide, royalty-free, non-exclusive, perpetual and transferable right of using, reproducing, copying, modifying, displaying and distributing the software set out in the Exhibit ("eID Authentication Reverse Proxy").

Article 2: Warranties of Licensor and Disclaimers

2.1. Since the eID Authentication Reverse Proxy has not specifically been created and tailored to address, and which has not been based on, your specific needs, Fedict does not warrant that the eID Authentication Reverse Proxy will meet your specific requirements or that the operation of the eID Authentication Reverse Proxy will operate in the specific combinations which you may select for use. As no software is error-free, Fedict cannot guarantee that the eID Authentication Reverse Proxy will operate without interruption or be error free.

2.2. Without prejudice to the above paragraph, this eID Authentication Reverse Proxy is provided by Fedict "AS IS" and any expressed or implied warranties other than those laid down in provision 2.1, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed.

2.3 This Agreement does not entitle you to receive any maintenance, support (be it telephone, fax or e-mail) or any other assistance with respect to the eID Authentication Reverse Proxy or with respect to any alteration made on the eID Authentication Reverse Proxy in any form whatsoever, including, but not limited to additions, upgrades, improvements to the substance and structure of the software ("Modifications").

Article 3: Licensee obligations

3.1. Any use, including, but not limited to, reproduction, copy, modification, display and distribution, is subject to compliance with the terms of this Agreement. You warrant that you will comply with the terms of this Agreement including the licenses governing the libraries or codes developed (and protected by intellectual property rights as the case may be) by third parties, which have been used wholly or in part for the development of the eID Authentication Reverse Proxy, being embedded in the e-ID application, linked to, being integrated into or compiled with other libraries and codes to form the eID Authentication Reverse Proxy ("Third-Party Work").

3.2. You may not copy, modify, sublicense, or distribute the eID Authentication Reverse Proxy otherwise than as expressly provided under this Agreement. Any attempt otherwise to copy, modify, sublicense or distribute the Agreement is void, and will automatically terminate your rights under this Agreement.

3.3. Third parties who have received copies, or rights, from you under this Agreement will not have their licenses terminated if you infringe the terms of this Agreement according to paragraph 1, so long as such parties remain in full compliance with these terms.

Article 4: Liability

4.1. Under this Agreement, Fedict shall under no circumstances, except for fraud or wilful misconduct, be liable for any indirect, special, incidental or consequential damages, or for any loss of profits, loss of data, loss of savings or business opportunity, trading losses, staff costs or costs of staff turnover, computer failure or malfunction, IT system break-down, business interruption or other technical or operational damage of any dimension whatever, or other indirect, consequential or punitive damages arising from or in connection with the use of the eID Authentication Reverse Proxy or of any modified or derivative work, or for any other commercial damages or losses arising from the use of it.

4.2. Fedict shall not be liable to indemnify you for any claims of intellectual property right infringement, including contributory infringement or inducement to infringe, of any intellectual property claimed in the eID Authentication Reverse Proxy by the authors of the Third-Party Works as identified in the special notices in the Exhibit. You agree to indemnify, defend and hold harmless Fedict against any and all claims, demands, penalties, proceedings, losses, liabilities, damages of whatsoever nature, costs, fees and expenses of any kind relating to in any way directly or indirectly out of Modifications and/or the use of the eID Authentication Reverse Proxy alone or in combination with other devices, products, software, services and/or materials, provided that Fedict notifies you in writing of the claim and allows you to control and reasonably cooperates with you in the defence of the claim and any related settlement negotiations.

4.3. Fedict shall not be responsible for (i) the consequences of modifying the eID Authentication Reverse Proxy, integrating the eID Authentication Reverse Proxy in proprietary products, or using the eID Authentication Reverse Proxy in combination with other devices, products, software, services and/or materials or (ii) determining whether you require a license to or additional rights from any of the Third Party Works, obtaining any such license on its behalf, or paying any fees relating to any such licenses, to the extent that such Third Party Works are claimed to be open source products.

Article 5: Termination

5.1 The Agreement and all licenses granted by the Licensor hereunder shall automatically terminate by law if you breach this Agreement.

5.2 Upon termination of the Agreement, you shall cease all use of the eID Authentication Reverse Proxy and shall destroy all copies of the eID Authentication Reverse Proxy within your possession or control.

Article 6: General

6.1 If any term or provision of this Agreement is determined to be illegal or unenforceable, such term or provision shall be deemed stricken, and all other terms and provisions shall remain in full force and effect. Each such provision shall be modified by the parties to the extent necessary to make it valid, legal and enforceable whilst preserving the intent of and balance between the parties.

6.2 This Agreement constitutes the entire understanding and agreement with respect to the eID Authentication Reverse Proxy and supersedes all prior oral and written communications.

6.3 This Agreement shall be governed by the laws of Belgium. Any dispute that cannot be settled amicably shall be subject to the courts of Brussels.

Exhibit

The Belgian eID Authentication Reverse Proxy consists of

- The Apache software, with some extensions
- The OpenSSL software
- A procedure to configure the Apache software for the intended purpose
- Some scripts to automate the above Apache configuration

7.2 Third-party licenses

7.2.1 Apache

This Toolkit uses the Apache developed by the Apache Software Foundation (<http://www.apache.org/>).

Here is a copy of the license (from <http://www.apache.org/licenses/LICENSE-2.0.txt>):

Apache License
Version 2.0, January 2004
<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner

or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the

appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

7.2.2 OpenSSL

This Wizard uses the OpenSSL Toolkit developed by the OpenSSL Project (<http://www.openssl.org/>). Version available in this wizard is not complete.

Here is a copy of the license (from <http://www.openssl.org/source/license.html>):

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2003 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-). 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

7.2.3 GAWK

This Toolkit uses GAWK (GNU version of awk).

More information are available at <http://www.gnu.org/software/gawk/>

Here is a copy of the license

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that

you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we

want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free

program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the

Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the

notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1

above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt

otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed

through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

8. SOFTWARE HISTORY

Version 0.9 – 09-2004

Version based on Apache 2.0.49 and OpenSSL 0.9.7d.

Bug fixes

- #20462
- #25659
- http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_kernel.c?r1=1.105&r2=1.106
- http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/metadata/mod_headers.c?r1=1.49&r2=1.50

Enhancements

OCSP protocol: *mod_ssl* has been modified to support the OCSP protocol.

Version 1.0.0 – 12-09-2005

Version based on Apache 2.0.54 and OpenSSL 0.97f.

Bug fixes

- #20462
- #25659
- #25667
- #31418
- #31848
- #34452
- #35081
- #35154
- http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/metadata/mod_headers.c?r1=1.49&r2=1.50
- CAN-2005-2700: <http://people.apache.org/~jorton/CAN-2005-2700.diff>

OCSP answers logging: All OCSP answers are now logged – see 6.3.

SSL Error Redirection: In case of error during certificates validation, the SSL error is trapped, the connection is established, and the browser is redirected to an error page – see 6.4.

Other: Normally, in case CRL have to be used but cannot – for instance if the CRL is expired – Apache the certificate validation fails and the SSL connection is dropped. We changed this to only fail is the directive “SSLForceValidation” is set to “on”. This directive replace the old one “SSLForceOCSP” – see 6.6.

Version 1.0.1 – 27-09-2005

SSL Error Redirection: error number is returned – see 6.4.

Bug fixes

- #12355
- #12340
- Authorisation problem on error redirected pages

Version 1.0.2 – 07-10-2005

SSL Error Redirection: error message is no more returned

Bug fixes

- corrected access denied when certificate is invalid and SSL re-negotiation is needed

Version 1.0.3 – 14-11-2005

Bug fixes

- Trap errors when retrying a failed SSL connection
- #35279

Version 1.0.4 – 01-12-2005

Use OpenSSL 0.98a

Bug fixes

- CAN-2005-2970: <http://svn.apache.org/viewcvs.cgi?view=rev&rev=292949>

1.0.5 - 19-12-2005

Bug fixes

- With Firefox (and probably other SSL compliant browsers), the first access was trapped as an error; when doing a refresh, the situation was corrected.

1.0.6 – 24-01-2006

Bug fixes

- #37791

1.0.7 – 22-03-2006

Bug fixes

- Remove new lines from headers – see `unwrap_header()` in http://people.apache.org/~jorton/mod_headers-2.0-ssl.diff

1.0.8 – 01-08-2006

Bug fixes

- Connection was allowed when interrupting the SSL negotiation by hitting ESC in the PIN dialog (Firefox only)

1.0.9 – 18-09-2006

Bug fixes

- Using OpenSSL 0.9.8c
- Added, by default, *SSLRequireSSL* for the whole site

9. DOCUMENT HISTORY

Date	Version	Author(s)	Reason for change
21-05-04	1.0	Philippe Londo Marc Stern	First version
28-05-04	1.0.1	Marc Stern	Minor changes
03-06-04	1.0.2	Marc Stern	Minor changes
10-06-04	1.0.3	Marc Stern	Added authorisation explanation
19-10-04	1.0.4	Marc Stern	Detailed certificates installation
31-05-05	2.0	Marc Stern	Added sections <ul style="list-style-type: none"> • Software history • SSL error redirection • Certificates validation • Logging OCSP answers • Server restart • CRL • Known issues
01-06-05	2.0.1	Marc Stern	Added retrieval of national number
27-09-05	2.0.2	Marc Stern	Advised to use “ <i>SSLSessionCache shmcb</i> ” SSL Error Redirection: error number is returned Explained SSL compatibility issues with IE Removed known issue (#12355)
10-11-05	2.0.3	Marc Stern	Updated SSL compatibility issues with IE 6.0
14-11-05	2.0.4	Marc Stern	Added fix “CAN-2005-2970” Use OpenSSL 0.98a
24-01-06	2.0.5	Marc Stern	Added fix for bug #37791
01-02-06	2.0.6	Marc Stern	Added description of interaction between SSL cache and “ <i>locations</i> ” in case of certificate rejection (see 4.5.1).
22-03-06	2.0.7	Marc Stern	Added remark about syntax change to retrieve SSL-related info in future versions of Apache.

01-08-06	2.0.8	Marc Stern	Added GlobalSign Root certificate, and restrict accepted certificates to the ones emitted by the Citizen CA
08-09-06	2.0.9	Marc Stern	Removed reference to a beta version in the license agreement. Added that test certificates are in the trust store, but not accepted by default
18-09-06	2.0.10	Marc Stern	Using OpenSSL 0.9.8c Added, by default, SSLRequireSSL for the whole site