CSMail SSL 7.0.1 Release Notes.
28 September 2009.

1 Changes in this release

1.1 Workaround for oddly configured Secure Mail Servers

Some secure mail servers (notably those of Yahoo/AT&T) request a client certificate from the CSMail Library during the SSL handshake phase. It is normal for such servers to provide a list of acceptable Certification Authorities (CAs) during the process; the affected servers do not, however, provide this list. Without such a list of acceptable CAs the library will attempt to provide an appropriate certificate from the Windows Certificate Store. If the user has only a self signed certificate, or a certificate issued by a private CA then this certificate will most probably not be accepted by the remote server and the SSL connection will fail.

This release provides two new options for the SSLInfo object that allow greater control of the selection of client certificates.

See sections 2.1 and 2.2 below for details of the SSLNoDefaultCredentials and SSLNoDefaultCredentialsHard options.

1.2 RFC 2047 (Message Header Extensions for Non-ASCII Text) Encoding of underscore

Following a review of the text of RFC 2047 Section 4.2 the handling of underscore characters (‘_’) in non-ASCII message headers has been modified to better reflect the requirements of that document.

2 New Features

2.1 SSLNoDefaultCredentials Option (SSLInfo Object)

By default the CSMail Library will allow the Windows Security Support Provider Interface (SSPI) to automatically supply a client certificate chain to a remote mail server. In some circumstances this behaviour is not desirable and the new **SSLNoDefaultCredentials** option for the SSLInfo Object provides a mechanism for disabling the default behaviour.

If the **SSLNoDefaultCredentials** option is **False** the library behaves as before and the SSPI is allowed to supply a client certificate chain.

If the **SSLNoDefaultCredentials** option is **True** the library provides it’s own algorithm for supplying a client certificate chain.

Example

```
' Prevent SSPI from providing client certificate chain
' The Library will attempt to provide a certificate chain instead
ssl.Option(SSLNoDefaultCredentials)=True
```

2.2 SSLNoDefaultCredentialsHard Option (SSLInfo Object)

In some cases it is desirable to prevent *any and all* selection of a client certificate chain when the mail server does not provide a list of acceptable CAs. The new **SSLNoDefaultCredentialsHard** option for the SSLInfo Object, in combination with the **SSLNoDefaultCredentials** option achieves this effect.

If the **SSLNoDefaultCredentialsHard** option is **False** the library behaves as before.

If the **SSLNoDefaultCredentials** option is **True** AND the SSLNoDefaultCredentials is also **True** the library will never provide a client certificate to a server that does not provide a CA list with the client certificate request.

Example

```
' SSLNoDefaultCredentialsHard has no effect unless SSLNoDefaultCredentials is True
ssl.Option(SSLNoDefaultCredentials)=True


' Prevent any certificate chain from being presented to the server
ssl.Option(SSLNoDefaultCredentialsHard)=True
```

2.3 Summary of SSLNoDefaultCredentials and SSLNoDefaultCredentialsHard

The table below summarises the behaviour of the SSLNoDefaultCredentials and SSLNoDefaultCredentialsHard options.

<table>
<tr><td colspan="2" rowspan="2"></td><th colspan="4">SSLNoDefaultCredentials</th></tr>
<tr><th colspan="2">False</th><th colspan="2">True</th></tr>
<tr><th rowspan="4">SSLNoDefaultCredentialsHard</th><th>False</th><td colspan="2">Use SSPI client certificate chain selection</td><td colspan="2">Use internal client certificate chain selection</td></tr>
<tr><th rowspan="3">True</th><th colspan="2">Server provides CA List</th><th colspan="2">Server provides CA List</th></tr>
<tr><th>False</th><th>True</th><th>False</th><th>True</th></tr>
<tr><td>Use SSPI client certificate chain selection</td><td>Use SSPI client certificate chain selection</td><td>Do not provide any client certificate chain</td><td>Use internal client certificate chain selection</td></tr>
</table>

2.4 LOG_F_DATA facility (LogHandler Object)

A new facility, LOG_F_DATA, has been added to the available facility codes for the LogHandler object. At present this facility, when used in combination with the LOG_F_SSL facility codes includes a hexadecimal dump of the SSL Protocol Handshake phase data exchange.