

SSL Plus

Version 4.5.1

Release Update

PUB- 0300-0213
December 4, 2003

© Certicom Corp. 2000-2003. All rights reserved.

Certicom, the Certicom logo, SSL Plus and Security Builder are trademarks or registered trademarks of Certicom Corp. All other trademarks or registered trademarks are property of their respective owners. This product is covered by one or more of the following U.S. Patents: US 6,195,433, 6,178,507, 6,141,420, 6,134,325, 6,122,736, 6,097,813, 6,078,667, 6,049,815, 5,999,626, 5,955,717, 5,933,504, 5,896,455, 5,889,865, 5,787,028, 5,761,305, 5,600,725, 4,745,568.

Other applications and corresponding foreign protection pending.

Certicom Corp.
5520 Explorer Drive,
4th Floor,
Mississauga, Ontario,
Canada, L4W 5L1
905.507.4220



This document describes the changes between this release and v4.0 of SSL Plus.

Other documentation provided with SSL Plus includes the *Programmer's Reference* and *User's Guide*. The *Programmer's Reference Manual* is a comprehensive document detailing all of the function calls within the API along with the data structures. The User's Guide describes how to use the API and explains the security concepts and technologies contained in SSL Plus.

Copyright Notice

© Certicom Corp. 2000, 2001, 2002,2003. All rights reserved. This documentation contains Certicom's proprietary information and any use and distribution are limited to authorized licensees of Certicom. Any unauthorized use, reproduction, and distribution of this documentation is strictly prohibited by law.

You can reach Certicom 's technical support department by telephone at 1-800-511-8011, by fax at 1-800-474-3877, or by email at support@certicom.com.

What's new for SSL Plus 4.5.1 ?

We have addressed four candidates in this release: CAN-2003-0543, CAN-2003-0544, CAN-2003-0545 and CAN-2003-0851. See <http://cve.mitre.org/> for more information.

We have also addressed CERT advisory CA-2003-26. See <http://www.cert.org/advisories/CA-2003-26.html> for more information.

Components

The **components** library (libshared.a) has been moved to **components/lib/<platform>**.

What's new for SSL Plus 4.4 ?

Security issue

We have reviewed the security issue described in <http://www.imc.org/ietf-tls/mail-archive/msg03859.html>.

Please be advised that SSL Plus and OpenSSL do not share any source code.

Additional OS support

Support for Symbian and Solaris v2.9 (gcc and Sun Workshop compiler releases) has been added.

Interoperability with non-standard sites

SSL Plus now provides functions that allow you to change the standard behaviour of an SSL protocol. You may need to do this if you are attempting to connect to a site which is using a non-standard implementation of the protocol. See the the **SSL Plus User's Guide** and the **SSL Plus Programmer's Reference** for more information.

Changes to function names

The following function names have changed.

- **ssl_setPolicy()** to **ssl_setPkiPolicy()**
- **SSL_PROTOCOL_SSLV3_V2_SERVERSIDE()** to **SSL_PROTOCOL_SSLV3_SSLV2_SERVERSIDE()**
- **SSL_PROTOCOL_SSLV3_V2_CLIENTSIDE()** to **SSL_PROTOCOL_SSLV3_SSLV2_CLIENTSIDE()**
- **SSL_PROTOCOL_TLSV1_SSLV3_V2_SERVERSIDE()** to **SSL_PROTOCOL_TLSV1_SSLV3_SSLV2_SERVERSIDE()**
- **SSL_PROTOCOL_TLSV1_SSLV3_V2_CLIENTSIDE()** to **SSL_PROTOCOL_TLSV1_SSLV3_SSLV2_CLIENTSIDE()**

The old function names are still supported in this release. However, we recommend that you use the new function names in your application.

What's new for SSL Plus 4.3 ?

Support for WAP 2.0

You can now develop a WAP 2.0-compliant application using SSL Plus. See the WAP appendix in the **SSL Plus User's Guide** for more information.

Support for MIDP 2.0

You can now develop a MIDP 2.0-compliant application using SSL Plus. This support is useful for Java KVM manufacturers. See the MIDP appendix in the **SSL Plus User's Guide** for more information.

CERT Advisory

On July 30, 2002 the CERT Coordination Center issued CERT Advisory CA-2002-23 (Multiple Vulnerabilities on OpenSSL). This release of SSL Plus addresses the subset of issues that affect this product.

What's new for SSL Plus 4.2 ?

This section describes the differences between version 4.2 and 4.0 of **SSL Plus**. Please note that version 4.1 of the product is not available.

Support for EAP

SSL Plus supports a number of extensions to the Extensible Authentication Protocol (EAP). The EAP is an extension of the PPP (Point to Point Protocol) that provides support for additional authentication methods within PPP.

SSL Plus supports the following extensions to EAP:

- EAP-TLS
- EAP-TTLS (EAP-Tunnel TLS)
- PEAP (Protected EAP)
- SCTP (Stream Control Transmission Protocol)

See the **SSL Plus User's Guide** for more information.

Cryptoswift RSA Hardware Accelerator

SSL Plus 4.2 now supports the Cryptoswift RSA hardware accelerator on the Win32, Linux x86 and Solaris platforms. New cipher suite and client authentication objects have been added to the SSL Plus API to support this device. See the **SSL Plus Programmer's Reference** and the **User's Guide** for more information.

PKCS #12 support

SSL Plus 4.2 provides support for parsing a PKCS #12 PFX.

New functions have been added to the API which allow you to both export certificates and a private key to a PFX, and to read the certificates and private key

from an existing PFX and store them in an array. Decryption suite objects have been added to the API to allow you to decrypt different types of PFXs. See the **SSL Plus Programmer's Reference** for a description of these functions.

Cache Memory Manager

SSL Plus 4.2 now includes a Cache Memory Manager (CMM). The CMM can improve the performance of your application if it makes a large number of connections. See the **SSL Plus User's Guide** for more information.

Cipher Suites

SSL Plus 4.2 now supports the following Diffie-Hellman cipher suites:

```
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DHE_DSS_EXPORT_WITH_3DES_EDE_CBC_SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
SSL_DH_anon_WITH_RC4_128_MD5
SSL_DH_anon_WITH_DES_CBC_SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
SSL_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA
SSL_DHE_DSS_EXPORT1024_WITH_RC4_56_SHA
SSL_DHE_DSS_WITH_RC4_128_SHA
```