



MatrixSSL 3.8 APIs

Electronic versions are uncontrolled unless directly accessed from the QA Document Control system.

Printed version are uncontrolled except when stamped with 'VALID COPY' in red.

External release of this document may require a NDA.

© INSIDE Secure - 2016 - All rights reserved



TABLE OF CONTENTS

1	OVERVIEW.....	4
1.1	Source Code Package	4
1.1.1	Package Structure	4
1.1.2	Integer Size	4
1.1.3	Compile-Time Features	4
1.1.4	Cipher Suites.....	5
1.1.5	Matrix Deterministic Memory	5
2	MATRIXSSL API	6
2.1	matrixSslOpen.....	6
2.2	matrixSslNewKeys	6
2.3	matrixSslLoadRsaKeys	7
2.4	matrixSslLoadRsaKeysMem	9
2.5	matrixSslLoadEcKeys	10
2.6	matrixSslLoadEcKeysMem	12
2.7	matrixSslLoadPkcs12.....	13
2.8	matrixSslLoadSessionTicketKeys	14
2.9	matrixSslSetSessionTicketCallback.....	16
2.10	matrixSslNewSessionId	16
2.11	matrixSslClearSessionId	17
2.12	matrixSslDeleteSessionId	17
2.13	matrixSslNewClientSession	18
2.14	matrixSslNewServerSession	20
2.15	matrixSslGetReadbuf	21
2.16	matrixSslReceivedData	22
2.17	matrixSslGetOutdata	24
2.18	matrixSslProcessedData	25
2.19	matrixSslSentData	26
2.20	matrixSslGetWritebuf	27
2.21	matrixSslEncodeWritebuf	28
2.22	matrixSslEncodeToOutdata	28
2.23	matrixSslEncodeClosureAlert.....	29
2.24	matrixSslGetAnonStatus	30
2.25	matrixSslEncodeRehandshake	30
2.26	matrixSslDisableRehandshakes.....	32
2.27	matrixSslReEnableRehandshakes.....	32
2.28	matrixSslSetCipherSuiteEnabledStatus	33
2.29	matrixSslDeleteSession	33
2.30	matrixSslDeleteSessionTicketKey.....	34
2.31	matrixSslDeleteKeys	34
2.32	matrixSslClose	34
2.33	matrixSslNewHelloExtension	35

2.34	matrixSslLoadHelloExtension.....	35
2.35	matrixSslDeleteHelloExtension	36
2.36	matrixSslsSessionCompressionOn	37
2.37	matrixSslRegisterSNICallback	37
2.38	matrixSslCreateSNlnext	38
2.39	matrixSslRegisterALPNCallback	38
2.40	matrixSslCreateALPNNext.....	39
2.41	matrixSslLoadOCSPResponse	40
2.42	matrixSslWriteOCSPRequest.....	41
3	MATRIXDTLS API.....	42
3.1	Debug Configuration	42
3.2	Integration Notes.....	42
3.3	matrixDtlsGetOutdata.....	42
3.4	matrixDtlsSentData	43
3.5	matrixDtlsSetPmtu	44
3.6	matrixDtlsGetPmtu	44
4	MATRIXSSL X.509 API	46
5	SESSION OPTIONS	47
5.1	TLS version	47
5.2	Stateless Session Ticket Resumption	47
5.3	Extended Master Secret.....	48
5.4	Maximum Fragment Length	49
5.5	Truncated HMAC	49
5.6	Elliptic Curve Specification	49
5.7	Trusted CA Indication.....	50
5.8	OCSP Revocation	50
5.9	User Defined Opaque TLS Session Pointer	51
5.10	User Defined Opaque Memory Allocation Pointer.....	51
5.11	User Defined TLS Buffer Memory Pool	51
5.12	Session Options Summary Table.....	52
6	THE CERTIFICATE VALIDATION CALLBACK FUNCTION.....	54
6.1	Application Layer Certificate Acceptance	54
6.2	psX509Cert_t Structure.....	57
7	QUICK REFERENCE	61
	APPENDIX A - LIST OF TABLES.....	62

1 OVERVIEW

This document is the technical reference for the MatrixSSL and MatrixDTLS C code library APIs. The functions documented here can be used to add server or client SSL/TLS security to any new or existing application on any hardware platform using any data transport mechanism.

This document is primarily intended for the software developer performing MatrixSSL integration into their custom application but is also a useful reference for anybody wishing to learn more about MatrixSSL or the SSL/TLS protocol in general.

For additional information on how to implement these APIs in an application, see the MatrixSSL Developer's Guide included in this package.

1.1 Source Code Package

MatrixSSL is distributed as a C source code package with compile environments for the most popular development platforms.

1.1.1 Package Structure

MatrixSSL's public interface function prototypes are defined in the *matrixsslApi.h* file. Applications compiling with MatrixSSL APIs only have to include this single header file.

```
#include "matrixsslApi.h"
```

The *matrixsslApi.h* file includes other package-specific header files using relative paths based on the default directory structure. Optional product features are enabled and disabled by toggling documented `#defines`. There is no need to restructure the include logic within the header files or to move the header files from the default directory locations when configuring features.

The C data types used by functions in *matrixsslApi.h* come from a variety of module headers in the package directories. MatrixSSL API custom data types with publicly accessible members are documented where applicable.

1.1.2 Integer Size

MatrixSSL was designed without dependency on platform specific integer sizes. MatrixSSL uses the `int32_t` and `uint32_t` type definitions throughout the code to ensure compatibility. These typedefs are contained in the *core/osdep.h* header file. This layer enables global redefinitions for platforms that do not support 32-bit integer types as the native `int` type.

1.1.3 Compile-Time Features

MatrixSSL contains a set of optional features that are configurable at compile time. These, and how to use the example configurations provided, are described in the *MatrixSSL Developer's Guide*. Please consult that document for further information.

1.1.4 Cipher Suites

The user can enable or disable any of the supported cipher suites at compile-time from the *matrixsslConfig.h* header file. Simply comment out the cipher suites that are not needed. If run-time disabling of cipher suites is required, *matrixSslSetCipherSuiteEnabledStatus* can be used to disable (and re-enable) ciphers that have been compiled into the library.

The individual cryptographic algorithms may be enabled and disabled through the *cryptoConfig.h* header file for fine-tuning of library size. Below is a representative list of cipher suites along with their cryptographic requirements. The comprehensive list of which cipher suites are supported in the specific MatrixSSL package can be found in the *matrixsslConfig.h* file.

Sample Cipher Suites in matrixsslConfig.h	cryptoConfig.h Dependencies
USE_TLS_RSA_WITH_AES_256_CBC_SHA	USE_RSA USE_AES
USE_SSL_RSA_WITH_3DES_EDE_CBC_SHA	USE_RSA USE_3DES
USE_SSL_RSA_WITH_RC4_128_SHA	USE_RSA USE_ARC4
USE_TLS_DHE_RSA_WITH_AES_256_CBC_SHA	USE_DH USE_RSA USE_AES
USE_TLS_DH_anon_WITH_AES_256_CBC_SHA	USE_DH USE_AES
USE_TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	USE_DH USE_RSA USE_AES USE_SHA256
USE_TLS_RSA_WITH_AES_256_CBC_SHA256	USE_RSA USE_AES USE_SHA256
USE_TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	USE_ECC USE_AES
USE_TLS_DHE_PSK_WITH_AES_256_CBC_SHA	USE_DH USE_AES
USE_TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	USE_ECC USE_RSA USE_AES
USE_TLS_PSK_WITH_AES_256_CBC_SHA	USE_AES
USE_TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	USE_ECC USE_AES_GCM USE_SHA384

1.1.5 Matrix Deterministic Memory

In commercial versions of MatrixSSL enabling *USE_MATRIX_MEMORY_MANAGEMENT* in *coreConfig.h* will activate the deterministic memory feature of the library. Every memory allocation in the library will be confined to a specific memory pool that has a regulated lifecycle. The feature enables tight control over memory usage.

Any APIs in this document that refer to "memory pools" or references to *psPool_t* structures or *poolUserPtr* parameters are related to this memory feature and may be ignored by customers using the open source version of the software and commercial users that do not enable *USE_MATRIX_MEMORY_MANAGEMENT*.

The [Matrix Deterministic Memory](#) document contains the details.

2 MATRIXSSL API

2.1 matrixSslOpen

```
int32 matrixSslOpen();
```

Return Value	Description
PS_SUCCESS	Successful initialization
PS_FAILURE	Failed core module initialization. Can't continue

Servers and Clients

This is the initialization function for the MatrixSSL library. Applications must call this function as part of their own initialization process before any other MatrixSSL functions are called.

Memory Profile

This function internally allocates memory that is freed during `matrixSslClose`

2.2 matrixSslNewKeys

```
int32 matrixSslNewKeys(sslKeys_t **keys, void *memAllocUserPtr);
```

Parameter	Input/Output	Description
keys	input/output	Internally allocated structure to use when loading key material
poolUserPtr	input	Optional user context for the creation of the memory pool that will hold the key material. Only relevant to commercial versions when USE_MATRIX_MEMORY_MANAGEMENT is enabled. NULL otherwise.

Return Value	Description
PS_SUCCESS	Successful key storage initialization
PS_MEM_FAIL	Failure. Unable to allocate memory for the structure

Servers and Clients

This is a necessary function that all implementations must call before loading in the specific key material that will be used in the SSL handshake.

After allocating the key structure, the user will load custom key material from files (or memory) using `matrixSslLoadRsaKeys`, `matrixSslLoadEcKeys`, `matrixSslLoadPkcs12`, `matrixSslLoadDhParams`, and/or `matrixSslLoadPsk`. Loading RSA/ECC keys or DH parameters may be done once for each `keys` context. Multiple calls can be made to load pre-shared keys for a single `keys` context.

Once loaded with the key material, the `keys` structure will be passed to `matrixSslNewClientSession` or `matrixSslNewServerSession` to associate those keys with the SSL session.

Memory Profile

This function internally allocates memory that is freed during `matrixSslDeleteKeys`. The caller does not need to free the `keys` parameter if this function does not return `PS_SUCCESS`.

The `poolUserPtr` value will be passed as the `userPtr` to `psOpenPool` when creating the dedicated memory pool for this key material.

2.3 matrixSslLoadRsaKeys

```
int32 matrixSslLoadRsaKeys(sslKeys_t *keys, const char *certFile,
                           const char *privFile, const char *privPass,
                           const char *trustedCAFiles);
```

Parameter	Input/Output	Description
keys	input/output	Allocated key structure returned from a previous call to <code>matrixSslNewKeys</code> . Will become input to <code>matrixSslNewClientSession</code> or <code>matrixSslNewServerSession</code> to associate key material with a SSL session.
certFile	input	The fully qualified filename(s) of the PEM formatted X.509 RSA identity certificate for this SSL peer. For in-memory support, see <code>matrixSslLoadRsaKeysMem</code> . This parameter is always relevant to servers. Clients will want to supply an identity certificate and private key if supporting client authentication. <code>NULL</code> otherwise.
privFile	input	The fully qualified filename of the PEM formatted PKCS#1 or PKCS#8 private RSA key that was used to sign the <code>certFile</code> . This parameter is always relevant to servers. Clients will want to supply an identity certificate and private key if supporting client authentication. <code>NULL</code> otherwise.
privPass	input	The plaintext password used to encrypt the private key file. <code>NULL</code> if private key file is not password protected or unused. MatrixSSL supports the MD5 PKCS#5 2.0 PBKDF1 password standard.
trustedCAFiles	input	The fully qualified filename(s) of the trusted root certificates (Certificate Authorities) for this SSL peer. This parameter is always relevant to clients. Servers will want to supply a CA if requesting client authentication. <code>NULL</code> otherwise.

Return Value	Test	Description
PS_SUCCESS	0	Success. All input files parsed and the keys parameter is available for use in session creation
PS_CERT_AUTH_FAIL	< 0	Failure. Certificate or chain did not self-authenticate or private key could not authenticate certificate
PS_PLATFORM_FAIL	< 0	Failure. Error locating or opening an input file
PS_ARG_FAIL	< 0	Failure. Bad input function parameter
PS_MEM_FAIL	< 0	Failure. Internal memory allocation failure
PS_PARSE_FAIL	< 0	Failure. Error parsing certificate or private key buffer
PS_FAILURE	< 0	Failure. Password protected decoding failed. Likely incorrect password provided
PS_UNSUPPORTED_FAIL	< 0	Failure. Unsupported key algorithm in certificate material

Servers and Clients

This function is called to load the RSA certificates and private key files from disk that are needed for SSL client-server authentication. The key material is loaded into the `keys` parameter for input into the subsequent session creation APIs `matrixSslNewClientSession` or `matrixSslNewServerSession`. This API can be called at most once for a given `sslKeys_t` parameter.

A standard SSL connection performs one-way authentication (client authenticates server) so the parameters to this function are specific to the client/server role of the application. The `certFile`, `privFile`, and `privPass` parameters are server specific and should identify the certificate and private key file for that server. The `certFile` and `privFile` parameters represent the two halves of the public key so they must both be non-NULL values if either is used.

The `trustedCAFiles` parameter is client specific and should identify the trusted root certificates that will be used to validate the certificates received from a server. Note that version 1 root certificates can only be loaded when `ALLOW_VERSION_1_ROOT_CERT_PARSE` is defined in `cryptoConfig.h`.

Calling this function is a resource intensive operation because of the file access, parsing, and internal public key authentications required. For this reason, it is advised that this function be called once per set of key files for a given application. All new sessions associated with the certificate material can reuse the

existing key pointer. At application shutdown the user must free the key structure using `matrixSslDeleteKeys`.

Client Authentication

If client authentication functionality is desired, all parameters to this function become relevant to both clients and servers. The `certFile` and `privFile` parameters are used to specify the identity certificate of the local peer. Likewise, each entity will need to supply a `trustedCAcertFile` parameter that lists the trusted CAs so that the connecting certificates may be authenticated. It is easiest to think of client authentication as a mirror image of the normal server authentication when considering how certificate and CA files are deployed.

It is possible to configure a server to engage in a client authentication handshake without loading CA files. Enable the `SERVER_CAN_SEND_EMPTY_CERT_REQUEST` define in `matrixsslConfig.h` to allow the server to send an empty `CertificateRequest` message. The server can then use the certificate callback function to perform a custom authentication on the certificate returned from the client.

The MatrixSSL library must be compiled with `USE_CLIENT_AUTH` defined in `matrixsslConfig.h` to enable client authentication support.

Multiple CA Certificates and Certificate Chaining

It is not uncommon for a server to work from a certificate chain in which a series of certificates form a child-to-parent hierarchy. It is even more common for a client to load multiple trusted CA certificates if numerous servers are being supported.

There are two ways to pass multiple certificates to the `matrixSslLoadRsaKeys` API. The first is to pass a semi-colon delimited list of files to the `certFile` or `trustedCAcertFiles` parameters. The second way is to append several PEM certificates into a single file and pass that file to either of the two parameters. Regardless of which way is chosen, the `certFile` parameter MUST be passed in a child-to-parent order. The first certificate parsed in the chain MUST be the child-most certificate and each subsequent certificate must be the parent (issuer) of the former. There must only ever be one private key file passed to this routine and it must correspond with the child-most certificate.

Encrypted Private Keys

It is strongly recommended that private keys be password protected when stored in files. The `privPass` parameter of this API is the plaintext password that will be used if the private key is encrypted. MatrixSSL supports the MD5 based PKCS#5 2.0 PBKDF1 standard for password encryption. The most common way a password is retrieved is through user input during the initialization of an application.

RSA-PSS Signed Certificates

The stronger RSASSA-PSS signature standard is staring to appear in X.509 certificates as an upgrade to the standard PKCS#1 v1.5 scheme. To include support for RSA-PSS signatures in certificates, enable `USE_PKCS1_PSS` in `crypto/cryptoConfig.h`

Memory Profile

The keys parameter must be freed with `matrixSslDeleteKeys` after its useful life.

Define Dependencies

<code>MATRIX_USE_FILE_SYSTEM</code>	Must be enabled in platform compile options
<code>USE_SERVER_SIDE_SSL</code>	Optionally enable in <code>matrixsslConfig.h</code> for SSL server support
<code>USE_CLIENT_SIDE_SSL</code>	Optionally enable in <code>matrixsslConfig.h</code> for SSL client support
<code>USE_PKCS5</code>	Optionally enable in <code>cryptoConfig.h</code> to support password encrypted private keys
<code>USE_PKCS8</code>	Optionally enable in <code>cryptoConfig.h</code> to support PKCS#8 formatted private keys

USE_CLIENT_AUTH	Optionally enable in <i>matrixssl/Config.h</i> to support client authentication
-----------------	---

2.4 matrixSslLoadRsaKeysMem

```
int32 matrixSslLoadRsaKeysMem(sslKeys_t *keys,
                             const unsigned char *certBuf, int32 certLen,
                             const unsigned char *privBuf, int32 privLen,
                             const unsigned char *trustedCABuf, int32 trustedCALen);
```

Parameter	Input/Output	Description
keys	input/output	Allocated key structure returned from a previous call to <code>matrixSslNewKeys</code> . Will become input to <code>matrixSslNewClientSession</code> or <code>matrixSslNewServerSession</code> to associate key material with a SSL session.
certBuf	input	The X.509 ASN.1 identity certificate for this SSL peer. For file-based support, see <code>matrixSslLoadRsaKeys</code> . This parameter is always relevant to servers. Clients will want to supply an identity certificate and private key if supporting mutual authentication. <code>NULL</code> otherwise.
certLen	input	Byte length of <code>certBuf</code>
privBuf	input	The PKCS#1 or PKCS#8 private RSA key that was used to sign the <code>certBuf</code> . This parameter is always relevant to servers. Clients will want to supply an identity certificate and private key if supporting mutual authentication. <code>NULL</code> otherwise.
privLen	input	Byte length of <code>privBuf</code>
trustedCABuf	input	The X.509 ASN.1 stream of the trusted root certificates (Certificate Authorities) for this SSL peer. This parameter is always relevant to clients. Servers will want to supply a CA if requesting mutual authentication. <code>NULL</code> otherwise.
trustedCALen	input	Byte length of <code>trustedCABuf</code>

Return Value	Test	Description
PS_SUCCESS	0	Success. All input buffers parsed successfully and the keys parameter is available for use in session creation
PS_CERT_AUTH_FAIL	< 0	Failure. Certificate or chain did not self-authenticate or private key could not authenticate certificate
PS_PLATFORM_FAIL	< 0	Failure. Error locating or opening an input file
PS_ARG_FAIL	< 0	Failure. Bad input function parameter
PS_MEM_FAIL	< 0	Failure. Internal memory allocation failure
PS_PARSE_FAIL	< 0	Failure. Error parsing certificate or private key buffer
PS_UNSUPPORTED_FAIL	< 0	Failure. Unsupported key algorithm in certificate material

Servers and Clients

This function is the in-memory equivalent of the `matrixSslLoadRsaKeys` API to support environments where the certificate material is not stored as files on disk. Please consult the information above about `matrixSslLoadRsaKeys` for detailed information on how clients and servers should manage the certificate and private key parameters. This API can be called at most once for a given `sslKeys_t` parameter.

The buffers for the certificates and private key must be in the native ASN.1 format of the X.509 v3 and PKCS#1/PKCS#8 standards, respectively. Typically, the ".der" file extension is used for certificate material in this binary format.

There is no password protection support for private key buffers. It is recommended that the user implement secure storage for the private key material.

Multiple CA Certificates and Certificate Chaining

This in-memory version of the key parser also supports multiple CAs and/or certificate chains. Simply append the ASN.1 certificate streams together for either the `certBuf` or `trustedCABuf` parameters. If

using a certificate chain in the `certBuf` parameter the order of the certificates still MUST be in child-to-parent order with the `privBuf` being the key associated with the child-most certificate.

Memory Profile

The keys parameter must be freed with `matrixSslDeleteKeys` after its useful life.

Define Dependencies

USE_SERVER_SIDE_SSL	Optionally enable in <i>matrixsslConfig.h</i> for SSL server support
USE_CLIENT_SIDE_SSL	Optionally enable in <i>matrixsslConfig.h</i> for SSL client support
USE_PKCS8	Optionally enable in <i>cryptoConfig.h</i> to support PKCS#8 formatted private keys
USE_CLIENT_AUTH	Optionally enable in <i>matrixsslConfig.h</i> to support client authentication

2.5 matrixSslLoadEcKeys

```
int32 matrixSslLoadEcKeys(sslKeys_t *keys, const char *certFile,
const char *privFile, const char *privPass,
const char *trustedCAFiles);
```

Parameter	Input/Output	Description
keys	input/output	Allocated key structure returned from a previous call to <code>matrixSslNewKeys</code> . Will become input to <code>matrixSslNewClientSession</code> or <code>matrixSslNewServerSession</code> to associate key material with a SSL session.
certFile	input	The fully qualified filename(s) of the PEM formatted X.509 identity certificate for this SSL peer. For in-memory support, see <code>matrixSslLoadEcKeysMem</code> . This parameter is always relevant to servers. Clients will want to supply an identity certificate and private key if supporting client authentication. <code>NULL</code> otherwise.
privFile	input	The fully qualified filename of the PEM formatted private EC key that was used to sign <code>certFile</code> . Supported formats are PKCS# 8 or "SEC1: Elliptical Curve Cryptography" at www.secg.org . This parameter is always relevant to servers. Clients will want to supply an identity certificate and private key if supporting client authentication. <code>NULL</code> otherwise.
privPass	input	The plaintext password used to encrypt the private key file. <code>NULL</code> if private key file is not password protected or unused. MatrixSSL supports the MD5 PKCS#5 2.0 PBKDF1 password standard.
trustedCAFiles	input	The fully qualified filename(s) of the trusted root certificates (Certificate Authorities) for this SSL peer. This parameter is always relevant to clients. Servers will want to supply a CA if requesting client authentication. <code>NULL</code> otherwise.

Return Value	Test	Description
PS_SUCCESS	0	Success. All input files parsed and the keys parameter is available for use in session creation
PS_CERT_AUTH_FAIL	< 0	Failure. Certificate or chain did not self-authenticate or private key could not authenticate certificate
PS_PLATFORM_FAIL	< 0	Failure. Error locating or opening an input file
PS_ARG_FAIL	< 0	Failure. Bad input function parameter
PS_MEM_FAIL	< 0	Failure. Internal memory allocation failure
PS_PARSE_FAIL	< 0	Failure. Error parsing certificate or private key buffer
PS_FAILURE	< 0	Failure. Password protected decoding failed. Likey incorrect password provided
PS_UNSUPPORTED_FAIL	< 0	Failure. Unsupported key algorithm in certificate material

Servers and Clients

This function is called to load the ECC certificates and private key files from disk that are needed for SSL client-server authentication. The key material is loaded into the `keys` parameter for input into the subsequent session creation APIs `matrixSslNewClientSession` or `matrixSslNewServerSession`. This API can be called at most once for a given `sslKeys_t` parameter.

A standard SSL connection performs one-way authentication (client authenticates server) so the parameters to this function are specific to the client/server role of the application. The `certFile`, `privFile`, and `privPass` parameters are server specific and should identify the certificate and private key file for that server. The `certFile` and `privFile` parameters represent the two halves of the public key so they must both be non-NULL values if either is used.

The `trustedCAFiles` parameter is client specific and should identify the trusted root certificates that will be used to validate the certificates received from a server. Note that version 1 root certificates can only be loaded when `ALLOW_VERSION_1_ROOT_CERT_PARSE` is defined in `cryptoConfig.h`.

Calling this function is a resource intensive operation because of the file access, parsing, and internal public key authentications required. For this reason, it is advised that this function be called once per set of key files for a given application. All new sessions associated with the certificate material can reuse the existing key pointer. At application shutdown the user must free the key structure using `matrixSslDeleteKeys`.

Client Authentication

If client authentication functionality is desired, all parameters to this function become relevant to both clients and servers. The `certFile` and `privFile` parameters are used to specify the identity certificate of the local peer. Likewise, each entity will need to supply a `trustedCAcertFile` parameter that lists the trusted CAs so that the certificates may be authenticated. It is easiest to think of client authentication as a mirror image of the normal server authentication when considering how certificate and CA files are deployed.

It is possible to configure a server to engage in a client authentication handshake without loading CA files. Enable the `SERVER_CAN_SEND_EMPTY_CERT_REQUEST` define in `matrixsslConfig.h` to allow the server to send an empty CertificateRequest message. The server can then use the certificate callback function to perform a custom authentication on the certificate returned from the client.

The MatrixSSL library must be compiled with `USE_CLIENT_AUTH` defined in `matrixsslConfig.h` to enable client authentication support.

Multiple CA Certificates and Certificate Chaining

It is not uncommon for a server to work from a certificate chain in which a series of certificates form a child-to-parent hierarchy. It is even more common for a client to load multiple trusted CA certificates if numerous servers are being supported.

There are two ways to pass multiple certificates to the `matrixSslLoadRsaKeys` API. The first is to pass a semi-colon delimited list of files to the `certFile` or `trustedCAcertFiles` parameters. The second way is to append several PEM certificates into a single file and pass that file to either of the two parameters. Regardless of which way is chosen, the `certFile` parameter MUST be passed in a child-to-parent order. The first certificate parsed in the chain MUST be the child-most certificate and each subsequent certificate must be the parent (issuer) of the former. There must only ever be one private key file passed to this routine and it must correspond with the child-most certificate.

Encrypted Private Keys

It is strongly recommended that private keys be password protected when stored in files. The `privPass` parameter of this API is the plaintext password that will be used if the private key is encrypted. MatrixSSL supports an MD5 based PKCS#5 2.0 PBKDF1 standard for password encryption. The most common way a password is retrieved is through user input during the initialization of an application.

Memory Profile

The keys parameter must be freed with `matrixSslDeleteKeys` after its useful life.

2.6 matrixSslLoadEcKeysMem

```
int32 matrixSslLoadEcKeysMem(sslKeys_t *keys, unsigned char *certBuf,
int32 certLen, unsigned char *privBuf, int32 privLen,
unsigned char *trustedCABuf, int32 trustedCALen);
```

Parameter	Input/Output	Description
keys	input/output	Allocated key structure returned from a previous call to <code>matrixSslNewKeys</code> . Will become input to <code>matrixSslNewClientSession</code> or <code>matrixSslNewServerSession</code> to associate key material with a SSL session.
certBuf	input	The X.509 ASN.1 identity certificate for this SSL peer. For file-based support, see <code>matrixSslLoadEcKeys</code> This parameter is always relevant to servers. Clients will want to supply an identity certificate and private key if supporting mutual authentication. NULL otherwise.
certLen	input	Byte length of <code>certBuf</code>
privBuf	input	The PKCS#8 or "SEC1: Elliptical Curve Cryptography" private EC key that was used to sign the <code>certBuf</code> . This parameter is always relevant to servers. Clients will want to supply an identity certificate and private key if supporting mutual authentication. NULL otherwise.
privLen	input	Byte length of <code>privBuf</code>
trustedCABuf	input	The X.509 ASN.1 stream of the trusted root certificates (Certificate Authorities) for this SSL peer. This parameter is always relevant to clients. Servers will want to supply a CA if requesting mutual authentication. NULL otherwise.
trustedCALen	input	Byte length of <code>trustedCABuf</code>

Return Value	Test	Description
PS_SUCCESS	0	Success. All input buffers parsed successfully and the keys parameter is available for use in session creation
PS_CERT_AUTH_FAIL	< 0	Failure. Certificate or chain did not self-authenticate or private key could not authenticate certificate
PS_PLATFORM_FAIL	< 0	Failure. Error locating or opening an input file
PS_ARG_FAIL	< 0	Failure. Bad input function parameter
PS_MEM_FAIL	< 0	Failure. Internal memory allocation failure
PS_PARSE_FAIL	< 0	Failure. Error parsing certificate or private key buffer
PS_UNSUPPORTED_FAIL	< 0	Failure. Unsupported key algorithm in certificate material

Servers and Clients

This function is the in-memory equivalent of the `matrixSslLoadEcKeys` API to support environments where the certificate material is not stored as files on disk. Please consult the documentation for `matrixSslLoadEcKeys` for detailed information on how clients and servers should manage the certificate and private key parameters. This API can be called at most once for a given `sslKeys_t` parameter.

There is no password protection support for private key buffers. It is recommended that the user implement secure storage for the private key material.

Multiple CA Certificates and Certificate Chaining

This in-memory version of the key parser also supports multiple CAs and/or certificate chains. Simply append the ASN.1 certificate streams together for either the `certBuf` or `trustedCABuf` parameters. If

using a certificate chain in the `certBuf` parameter the order of the certificates still MUST be in child-to-parent order with the `privBuf` being the key associated with the child-most certificate.

Memory Profile

The keys parameter must be freed with `matrixSslDeleteKeys` after its useful life.

2.7 matrixSslLoadPkcs12

```
int32 matrixSslLoadPkcs12(sslKeys_t *keys,
                          const unsigned char *p12File,
                          const unsigned char *importPass, int32 ipasslen,
                          const unsigned char *macPass, int32 mpasslen,
                          int32 flags);
```

Parameter	Input/Output	Description
keys	input/output	Allocated key structure returned from a previous call to <code>matrixSslNewKeys</code> . Will become input to <code>matrixSslNewClientSession</code> or <code>matrixSslNewServerSession</code> to associate key material with a SSL session.
p12File	input	The fully qualified filename(s) of the PKCS#12 file.
importPass	input	The plaintext import password used to decrypt <code>p12File</code>
ipassLen	input	Byte length of the <code>importPass</code> parameter
macPass	input	Optional plaintext password used to verify the MAC of the PKCS#12 file. In most cases, the MAC password is identical to the import password and if set to <code>NULL</code> the import password will be used by default.
mpassLen	input	The byte length of the <code>macPass</code> parameter
flags	input	Reserved. Pass a 0

Return Value	Test	Description
PS_SUCCESS	0	Success. File parsed and the <code>keys</code> parameter is available for use
PS_CERT_AUTH_FAIL	< 0	Failure. Certificate or chain did not self-authenticate or private key could not authenticate certificate
PS_PLATFORM_FAIL	< 0	Failure. Error locating or opening input file
PS_ARG_FAIL	< 0	Failure. Bad input function parameter
PS_MEM_FAIL	< 0	Failure. Internal memory allocation failure
PS_PARSE_FAIL	< 0	Failure. Error parsing certificate or private key buffer
PS_UNSUPPORTED_FAIL	< 0	Failure. Unsupported algorithm in file material

Servers

This function is called to load certificate and key material from a PKCS#12 file. The PKCS#12 standard enables certificates and private keys to be stored together in a single file. This function requires that only a single private key is present in the PKCS#12 file and includes the accompanying certificate (or certificate chain).

The `sslKeys_t` output is loaded into the `keys` parameter for input into the subsequent session creation API `matrixSslNewServerSession`. This API can be called at most once for a given `sslKeys_t` parameter.

Calling this function is a resource intensive operation because of the file access, parsing, and internal public key authentications required. For this reason, it is advised that this function be called once per set of key files for a given application. All new sessions associated with the certificate material can reuse the existing key pointer. At application shutdown the user must free the key structure using `matrixSslDeleteKeys`.

Client Authentication

Clients may use this function to load certificates and the private key if engaging in a client authentication handshake.

However, for both server and client cases the counterpart Certificate Authority files must be loaded separately using the `matrixSslLoadRsaKeys` function because this PKCS#12 API does not support CA files. In this case, the same `sslKeys_t` parameter should be used in both APIs.

The MatrixSSL library must be compiled with `USE_CLIENT_AUTH` defined in *matrixsslConfig.h* to enable client authentication support.

Certificate Chaining

It is not uncommon for a server to work from a certificate chain in which a series of certificates form a child-to-parent hierarchy. The PKCS#12 file must have the certificate chain in a child-to-parent order and the private key must be for the child-most certificate.

Supported Integrity and Encryption Algorithms

The parser supports PKCS#12 files that are encoded in the standard “password integrity” and “password privacy” modes. If you require public-key modes please contact Inside Secure.

Each certificate and private key will be wrapped within a “password privacy” algorithm. The supported algorithms are:

- `pbeWithSHAAnd3-KeyTripleDES-CBC`
- `pbewithSHAAnd40BitRC2-CBC`

The use of these algorithms is historical and certificates are generally encrypted with RC2 and private keys are generally encrypted with 3DES. Please contact INSIDE if you require additional “password privacy” algorithms.

Memory Profile

The keys parameter must be freed with `matrixSslDeleteKeys` after its useful life.

Define Dependencies

<code>USE_SERVER_SIDE_SSL</code>	Optionally enable in <i>matrixsslConfig.h</i> for SSL server support
<code>USE_CLIENT_SIDE_SSL</code>	Optionally enable in <i>matrixsslConfig.h</i> for SSL client support
<code>USE_PKCS12</code>	Must enable in <i>cryptoConfig.h</i> to support PKCS#12
<code>USE_CLIENT_AUTH</code>	Optionally enable in <i>matrixsslConfig.h</i> to support client authentication
<code>MATRIX_USE_FILE_SYSTEM</code>	Must define in platform build environment for file access
<code>USE_RC2</code>	Optionally enable in <i>cryptoConfig.h</i> if RC2 encryption is needed

2.8 matrixSslLoadSessionTicketKeys

```
int32 matrixSslLoadSessionTicketKeys(sslKeys_t *keys,
```

```
const unsigned char name[16],
const unsigned char *symkey, short symkeyLen,
const unsigned char *hashkey, short hashkeyLen);
```

Parameter	Input/Output	Description
keys	input/output	Allocated key structure returned from a previous call to <code>matrixSslNewKeys</code> . Will become input to <code>matrixSslNewServerSession</code> to associate key material with a SSL session.
name	input	The 16 byte name assigned to the key pair. It should be a randomly generated string to help avoid collisions between servers
symkey	input	The AES key for ticket encryption/decryption.
symkeyLen	input	MUST be 16 or 32 for AES-128 or AES-256, respectively
hashkey	input	The HMAC-SHA256 key for ticket authentication
hashkeyLen	input	MUST be 32 bytes for SHA-256

Return Value	Test	Description
PS_SUCCESS	0	Success. Keys loaded and available for use
PS_LIMIT_FAIL	< 0	Failure. List full or one of the length parameters was not an accepted value
PS_MEM_FAIL	< 0	Failure. Internal memory allocation failure

Servers

This function is called to load an AES and HMAC-SHA key pair for use in stateless session resumption as specified in RFC 4507. The keys are used to encode a session resumption ticket that is given to a connected client and used to decode the ticket when a client later attempts a resumed session.

Calling this function effectively enables the stateless session ticket feature for any server session that uses the `sslKeys_t` context with `matrixSslNewServerSession`.

This function can be called many times for a given `sslKeys_t` context and each call will add a key to the end of a single-linked list. The first key in the list will always be the key used to encrypt newly issued session tickets. When decrypting a session ticket, the entire list will be searched to locate the encrypting key.

Keys can be deleted using `matrixSslDeleteSessionTicketKey`.

The `SSL_SESSION_TICKET_LIST_LEN` define in `matrixsslConfig.h` limits the length of the internal cache. If the limit is hit this function will return `PS_LIMIT_FAIL` and the caller can use `matrixSslDeleteSessionTicketKey` to make room if desired.

A user callback can be optionally registered to notify each time a session ticket is received to allow user intervention. The callback is registered using `matrixSslSetSessionTicketCallback` and is documented below.

Ticket Notes

The value of `SSL_SESSION_ENTRY_LIFE` in `matrixsslConfig.h` is used as the lifetime when generating a ticket.

The platform MUST implement the `psGetTime` function as documented in the [Porting Guide](#) so that the `int32` return value is the elapsed seconds from some epoch. This API is used to store the timestamp in the encrypted ticket and to retrieve the current time when decrypting the ticket to determine expiration

The cryptographic primitives used for ticket encoding is AES-128/256-CBC and HMAC-SHA256.

Interaction with cached session ID mechanism

If the stateless session ticket mechanism is used during the SSL handshake the server WILL NOT cache the session using the standard session ID mechanism.

Clients

Clients that wish to use the stateless session resumption mechanism must set the `ticketResumption` member of the `sslSessOpts_t` structure to 1 when calling `matrixSslNewClientSession`.

Define Dependencies

USE_SERVER_SIDE_SSL	Enable in <i>matrixsslConfig.h</i> for SSL server support
USE_MULTITHREADING	Optionally enable in <i>coreConfig.h</i> if multiple server threads will be accessing key list
USE_STATELESS_SESSION_TICKETS	Enable in <i>matrixsslConfig.h</i>
SSL_SESSION_ENTRY_LIFE	Configure in <i>matrixsslConfig.h</i>
USE_AES	Enable in <i>cryptoConfig.h</i>
USE_HMAC	Enable in <i>cryptoConfig.h</i>
USE_SHA256	Enable in <i>cryptoConfig.h</i>

2.9 matrixSslSetSessionTicketCallback

```
void matrixSslSetSessionTicketCallback(sslKeys_t *keys,
                                       int32 (*ticket_cb)(void* keys,
                                       unsigned char name[16], short found));
```

Parameter	Input/Output	Description
keys	input/output	Allocated key structure returned from a previous call to <code>matrixSslNewKeys</code> . Will become input to <code>matrixSslNewServerSession</code> to associate key material with a SSL session.
ticket_cb	input	The function to invoke when the server can't find the ticket decryption key for a session ticket.

Servers

Servers should register a callback for use with the stateless session ticket resumption mechanism. This callback will be invoked each time a client sends a session ticket and can be used as an opportunity for the application to locate and load the correct key or to void the ticket and revert to a full handshake.

Ticket Callback Function

The callback is invoked with a void pointer representing the `sslKeys_t*` context, the 16-byte key `name`, and the `found` indication of whether the correct key is already available in the server's cached list. The `void*` input is an `sslKeys_t*` type that should be typecast locally.

If the `found` parameter is 0 then the server does not currently have the session ticket key and the callback should be used as an opportunity to find and load the keys. If the named session ticket is located, the callback will call `matrixSslLoadSessionTicketKeys` using the typecast `keys` pointer as the first parameter.

If the `found` parameter is 1 then the server holds the correct key and the callback can be used to allow the resumption

Regardless of the value of the incoming `found` parameter, the return value of the callback will indicate to MatrixSSL whether to progress with a resumed session or to use a full handshake path and issue a new ticket. **A return value of ≥ 0 indicates the named key should be used to resume the handshake and a return value of < 0 means the key could not be found or the ticket should be discarded.**

2.10 matrixSslNewSessionId

```
int32 matrixSslNewSessionId(sslSessionId_t **sid, void *poolUserPtr);
```


Parameter	Input/Output	Description
sid	input/output	Storage for an SSL session ID used for future session resumption
poolUserPtr	input	Optional user context for the creation of the memory pool that will hold the session material. Only relevant to commercial versions when USE_MATRIX_MEMORY_MANAGEMENT is enabled. NULL otherwise.

Return Value	Test	Description
PS_SUCCESS	0	Success. Session ID storage ready to be passed to <code>matrixSslNewClientSession</code>
PS_MEM_FAIL	< 0	Failure. Internal memory allocation failed

Clients

This function is only meaningful to a client wishing to perform future SSL session resumptions with a particular server. After allocating a session ID with this call, the structure is passed to the `sid` parameter of `matrixSslNewClientSession` where it will be populated with valid resumption credentials during the handshake process. Subsequent calls to `matrixSslNewClientSession` to reconnect with the same server should pass this same session ID to initiate the much faster session resumption handshake.

See the **Session Resumption** chapter in the [MatrixSSL Developer's Guide](#) document accompanying this release for more information.

Memory Profile

The `sid` parameter must be freed with `matrixSslDeleteSessionId` after its useful life.

The `poolUserPtr` value will be passed as the `userPtr` to `psOpenPool` when creating the dedicated memory pool for the session material.

Define Dependencies

USE_CLIENT_SIDE_SSL	Must be defined in <i>matrixsslConfig.h</i>
---------------------	---

2.11 matrixSslClearSessionId

```
void matrixSslClearSessionId(sslSessionId_t *sid);
```

Parameter	Input/Output	Description
sid	input/output	Previously allocated SSL session ID to be cleared

Clients

This function is only meaningful to clients using the SSL session resumption feature. This function will empty the session ID contents of the `sid` parameter that were previously stored during an earlier handshake. The `sid` parameter will have been allocated by a previous call to `matrixSslNewSessionId`. This function is simply for convenience if wishing to initiate a new session with a full handshake without having to call `matrixSslDeleteSessionId` and `matrixSslNewSessionId`.

Define Dependencies

USE_CLIENT_SIDE_SSL	Must be defined in <i>matrixsslConfig.h</i>
---------------------	---

2.12 matrixSslDeleteSessionId

```
void matrixSslDeleteSessionId(sslSessionId_t *sid);
```

Parameter	Input/Output	Description
sid	input	Previously allocated SSL session ID to be cleared and freed

Clients

This function is only meaningful to clients using the SSL session resumption feature. This function will free the session ID that was previously allocated by `matrixSslNewSessionId`. It will also delete the dedicated memory pool for commercial versions that have enabled `USE_MATRIX_MEMORY_MANAGEMENT`.

Define Dependencies

<code>USE_CLIENT_SIDE_SSL</code>	Must be defined in <i>matrixsslConfig.h</i>
----------------------------------	---

2.13 matrixSslNewClientSession

```
int32 matrixSslNewClientSession(ssl_t **ssl,
                                const sslKeys_t *keys,
                                sslSessionId_t *sessionId,
                                uint32 cipherSuites[], uint16 cipherCount,
                                int32 (*certValidator)(ssl_t *, psX509Cert_t *, int32),
                                const char *expectedName,
                                tlsExtension_t *extensions,
                                int32 (*extensionCback)(ssl_t *ssl,
                                                         unsigned short type, unsigned short len,
                                                         void *data),
                                sslSessOpts_t *options);
```

Parameter	Input/Output	Description
ssl	input/output	New context for this SSL session
keys	input	Key pointer that has been populated with the necessary certificate and key material (see <code>matrixSslNewKeys</code>)
sessionId	input/output	SSL session id storage previously allocated by <code>matrixSslNewSessionId</code>
cipherSuites	input	Pass a value of NULL to allow the client and server to negotiate the cipher suite automatically OR pass the integer identifiers of the specific cipher suites that the client wants to use. See the full cipher suite list in the source code file <i>matrixssl/lib.h</i> for possible values.
cipherCount	input	If one or more cipher suites are specified in the <code>cipherSuites</code> array, this is the count of those. 0 if automatic negotiation should occur.
certValidator	input	The function that will be invoked during the SSL handshake to see the internal authentication status of the server certificate chain. This callback is also the opportunity for the application to perform custom validation tests as needed
expectedName	input	The name of the server that the client will be connecting to. This string is used during the x.509 certificate validation portion of the handshake. The <code>expectedName</code> is often a DNS. Set to NULL to exclude this name test.
extensions	input	Custom CLIENT_HELLO extensions. See <code>matrixSslNewHelloExtension</code> for details.
extensionCback	input	The function that will be invoked as a callback during the SSL handshake to see any SERVER_HELLO extensions that have been received
options	input	Run time SSL options for SSL protocol version, maximum fragment length, truncated HMAC, resumption method, elliptic curve selection, and custom user pointers. See the Session Options section for more information

Return Value	Test	Description
MATRIXSSL_REQUEST_SEND	> 0	Success. The <code>ssl_t</code> context is initialized and the CLIENT_HELLO message has been encoded and is ready to be sent to the server to begin the SSL handshake
PS_ARG_FAIL	< 0	Failure. Bad input function parameter
PS_MEM_FAIL	< 0	Failure. Memory allocation failure
PS_PROTOCOL_FAIL	< 0	Failure. SSL context is not in the correct state for creating a CLIENT_HELLO message or there was an error encrypting the message
PS_UNSUPPORTED_FAIL	< 0	Failure. The requested cipher suite was not found or library was not compiled with client support
PS_PLATFORM_FAIL	< 0	Failure. Internal call to <code>psGetEntropy</code> failed while encoding CLIENT_HELLO message

Clients

Clients call this function to start a new SSL session or to resume a previous one. The session context is returned in the output parameter `ssl`. The CLIENT_HELLO handshake message is internally generated when this function is called and the typical action to take after this function returns is to retrieve that message with `matrixSslGetOutdata` and send that data to the server.

This function requires a pointer to an `sslKeys_t` structure that was returned from a previous call to `matrixSslNewKeys` and loaded with the relevant certificate and key material using `matrixSslLoadRsaKey` or equivalent.

If the client wishes to resume a session with a server the `sessionId` parameter can be used. For the initial handshake with a new server this parameter should point to a `matrixSslNewSessionId` allocated `sslSessionId_t` location in which the library will store the session ID information during the handshake process. For this reason, it is essential that the `sessionId` location be scoped for the lifetime of the SSL session it is passed into. On subsequent handshakes with the same server, the client can simply pass through this same `sessionId` memory location and `matrixSslNewClientSession` will extract the session ID and encode a CLIENT_HELLO message that will initiate a resumed handshake with the server. The `sessionId` parameter may be `NULL` if session resumption is not desired.

If the user wants to ensure the `sessionId` parameter is initialized or cleared of any previous session ID information, `matrixSslClearSessionId` should be used to guarantee a full handshake.

The `cipherSuites` parameter can be used to force the client to send a specific set of cipher suites to the server rather than the entire set of supported ciphers. Set this value to `NULL` (or `cipherSuites[0]` to 0) to send the entire cipher suite list that is enabled in *matrixsslConfig.h*. Otherwise the values in the array are the decimal integer value of the cipher suite specified in the standards. The supported values can be found in *matrixsslLib.h*. If `cipherSuites` is used to select a set of cipher suites the `cipherCount` parameter must reflect the number of cipher suites that are set in the array.

An explicit cipher suite will take precedence over the cipher suite in `sessionId` if they do not match. So if both `sessionId` and `cipherSuites` are passed in and the `cipherSuites` does not match the cipher that is contained in the `sessionId` parameter, the `sessionId` will be cleared and the client will encode a new CLIENT_HELLO with the `cipherSuites` value. If the `cipherSuites` value is 0 or if it identically matches the cipher suite in the `sessionId` parameter, session resumption will be attempted.

The `certValidator` parameter is used to register a callback routine that will be invoked during the certificate validation portion of the SSL handshake. This optional (but highly recommended) registration will enable the application to see the internal authentication results of the server certificate, perform custom validation checks, and pass certificate information on to end users wishing to manually validate certificates. Additional tests a callback may want to perform on the certificate information might include date validation and host name (common name) verification. If a certificate callback is not registered the internal public-key authentication against the nominated Certificate Authorities will determine whether or not to continue the handshake.

Detailed information on the certificate callback routine is found in the section [The Certificate Validation Callback Function](#) towards the end of this document.

The `expectedName` should be set to confirm the name of the server is contained in the x.509 certificate for that server. The `commonName` and `subjectAltName` entries of the certificate are checked. Pass `NULL` if this name test is not needed.

The `extensions` parameter enables the user to pass custom `CLIENT_HELLO` extensions to the server. See `matrixSslNewHelloExtension` for more information.

The `extensionCb` parameter enables the user to register a function callback that will be invoked during the parsing of `SERVER_HELLO` if the server has provided extensions. The callback should return `< 0` if the handshake should be terminated.

The `options` parameter is required and allows the client application to specify the TLS protocol version, maximum fragment length, truncated HMAC, resumption method, and the elliptic curves it wishes to support for the session being created. All member values must be set to 0 or `NULL` (if pointer type) if the default behaviour is desired. See the **Session Options** section in this document for more details.

UPGRADE NOTE: Versions of `matrixSslNewClientSession` prior to 3.7 used a single `int32 flags` parameter as the final argument and it was used to specify the TLS protocol version. The protocol version must now be assigned to the `versionFlag` member of the `sslSessOpts_t` structure.

Memory Profile

The user must free the `ssl_t` structure using `matrixSslDeleteSession` after the useful life of the session. The caller does not need to free the `ssl` parameter if this function does not return `MATRIXSSL_REQUEST_SEND`.

The `keys` pointer is referenced in the `ssl_t` context without duplication so it is essential the user does not call `matrixSslDeleteKeys` until all associated sessions have been deleted.

Define Dependencies

<code>USE_CLIENT_SIDE_SSL</code>	Must be enabled in <code>matrixsslConfig.h</code>
<code>ENABLE_SECURE_REHANDSHAKES</code>	Optionally disable support for RFC 5746

2.14 matrixSslNewServerSession

```
int32 matrixSslNewServerSession(ssl_t **ssl, const sslKeys_t *keys,
                                int32 (*certCb)(ssl_t *, psX509Cert_t *, int32),
                                sslSessOpts_t *options);
```

Parameter	Input/Output	Description
<code>ssl</code>	input/output	New context for this SSL session
<code>keys</code>	input	Key pointer that has been populated with the necessary certificate and key material (see <code>matrixSslNewKeys</code>)
<code>certCb</code>	input	Only relevant if using client authentication. <code>NULL</code> if not using client authentication, otherwise the function that will be invoked during the SSL handshake to see the internal authentication status of the client certificate chain. This callback is also the opportunity for the application to perform custom validation tests as needed.
<code>options</code>	input	Run time SSL options for SSL protocol version and elliptic curve selection. See the Session Options section for more information

Return Value	Test	Description
<code>PS_SUCCESS</code>	0	Success. The <code>ssl_t</code> context is initialized and ready for use
<code>PS_ARG_FAIL</code>	<code>< 0</code>	Failure. Bad input function parameter
<code>PS_FAILURE</code>	<code>< 0</code>	Failure. Internal memory allocation failure

Servers

When a server application has received notice that a client is requesting a secure socket connection (a socket accept on a secure port), this function should be called to initialize the new SSL session context. This function will prepare the server for the SSL handshake and the typical action to take after returning from this function is to call `matrixSslGetReadbuf` to retrieve an allocated buffer in which to copy the incoming handshake message from the client.

This function requires a pointer to an `sslKeys_t` structure that was returned from a previous call to `matrixSslNewKeys` and populated with key material from `matrixSslLoadRsaKeys` (or equivalent)

In client authentication scenarios the `certValidator` parameter must be used to register a callback on the server side to perform application specific checks on the client certificate. Setting a certificate callback is an explicit indication that client authentication will be used for this session.

If a server wants to be able to optionally enable client authentication but not require it for the initial handshake the certificate callback should be included in `matrixSslNewServerSession` but then `matrixSslSetSessionOption` with the `SSL_OPTION_DISABLE_CLIENT_AUTH` should be called immediately after. When the server later determines client authentication should be used, it can call `matrixSslSetSessionOption` with `SSL_OPTION_ENABLE_CLIENT_AUTH`.

Detailed information on the callback routine can be found below in the section entitled **The Certificate Validation Callback Function**.

The `options` parameter is required and allows the server application to specify the TLS protocol version and the elliptic curves it wishes to support for the session being created. All member values must be set to 0 or NULL (is pointer type) if the default behaviour is desired. See the **Session Options** section in this document for more details.

UPGRADE NOTE: Versions of `matrixSslNewServerSession` prior to 3.7 used a single `int32 flags` parameter as the final argument and it was used to specify the TLS protocol version. The protocol version must now be assigned to the `versionFlag` member of the `sslSessOpts_t` structure.

Memory Profile

The user must free the `ssl_t` structure using `matrixSslDeleteSession` after the useful life of the session. The caller does not need to free the `ssl` parameter if this function does not return `PS_SUCCESS`.

The `keys` pointer is referenced in the `ssl_t` context without duplication so it is essential the user does not call `matrixSslDeleteKeys` until all associated sessions have been deleted.

Define Dependencies

<code>USE_SERVER_SIDE_SSL</code>	Must be enabled in <i>matrixsslConfig.h</i>
----------------------------------	---

2.15 matrixSslGetReadbuf

```
int32 matrixSslGetReadbuf(ssl_t *ssl, unsigned char **buf);
```

Parameter	Input/Output	Description
<code>ssl</code>	input	The SSL session context
<code>buf</code>	output	Pointer to the memory location where incoming peer data should be read into

Return Value	Description
<code>>= 0</code>	Success. Indicates how many bytes are available in <code>buf</code> for incoming data
<code>PS_ARG_FAIL</code>	Failure. Bad function parameters

Servers and Clients

Any time the application is expecting to receive data from a peer this function must be called to retrieve the memory location where the incoming data should be read into. By providing a buffer to read network data into, the MatrixSSL API avoids an internal buffer copy.

The length of available bytes in `buf` is indicated in the return code. This is a maximum length and it is the user's responsibility to adhere to this size and not read data bytes beyond the given length. The mechanism for handling incoming data beyond the returned size is discussed below.

Once the user has read data into this buffer, `matrixSslReceivedData` must be called to process the data in-situ. If the return code from `matrixSslReceivedData` is `MATRIXSSL_REQUEST_RECV` this indicates that additional data needs to be read. In this case, `matrixSslGetReadbuf` must be called again for an updated pointer and buffer size to copy the additional data into.

2.16 matrixSslReceivedData

```
int32 matrixSslReceivedData(ssl_t *ssl, uint32 bytes, unsigned char **ptbuf,
                           uint32 *ptLen);
```

Parameter	Input/Output	Description
ssl	input	The SSL session context
bytes	input	The number of bytes received
ptbuf	output	If the data being received is an application-level record (or an alert) the unencrypted plaintext will be delivered to the user through this parameter. This will be a read-only pointer into the buffer that the user can process directly or copy locally for parsing at a later time.
ptLen	output	If <code>ptbuf</code> is non-NULL this is the byte length of the data

Return Value	Test	Description
MATRIXSSL_REQUEST_SEND	> 0	Success. The processing of the received data resulted in an SSL response message that needs to be sent to the peer. If this return code is hit the user should call <code>matrixSslGetOutdata</code> to retrieve the encoded outgoing data.
MATRIXSSL_REQUEST_RECV	> 0	Success. More data must be received and this function must be called again. User must first call <code>matrixSslGetReadbuf</code> again to receive the updated buffer pointer and length to where the remaining data should be read into.
MATRIXSSL_HANDSHAKE_COMPLETE	> 0	Success. The SSL handshake is complete. This return code is returned to client side implementation during a full handshake after parsing the FINISHED message from the server. It is possible for a server to receive this value if a resumed handshake is being performed where the client sends the final FINISHED message.
MATRIXSSL_RECEIVED_ALERT	> 0	Success. The data that was processed was an SSL alert message. In this case, the <code>ptbuf</code> pointer will be two bytes (<code>ptLen</code> will be 2) in which the first byte will be the alert level and the second byte will be the alert description. After examining the alert, the user must call <code>matrixSslProcessedData</code> to indicate the alert was processed and the data may be internally discarded.
MATRIXSSL_APP_DATA	> 0	Success. The data that was processed was application data that the user should process. In this return code case the <code>ptbuf</code> and <code>ptLen</code> output parameters will be valid. The user may process the data directly from <code>ptbuf</code> or copy it aside for later processing. After handling the data the user must call <code>matrixSslProcessedData</code> to indicate the plain text data may be internally discarded.
MATRIXSSL_APP_DATA_COMPRESSED	> 0	Success. The application data that is returned needs to be inflated with zlib before being processed. This return code is only possible if the <code>USE_ZLIB_COMPRESSION</code> define has been enabled and the peer has agreed to compression. Compression is not advised due to TLS attacks.

PS_SUCCESS	0	Success. This return code will be returned if the bytes parameter is 0 and there is no remaining internal data to process. This could be useful as a polling mechanism to confirm the internal buffer is empty. One real life use-case for this method of invocation is when dealing with a Google Chrome browser that uses False Start.
PS_MEM_FAIL	< 0	Failure. Internal memory allocation error
PS_ARG_FAIL	< 0	Failure. Bad input parameters
PS_PROTOCOL_FAIL	< 0	Failure. Internal protocol error

Servers and Clients

This function must be called each time data is received from the peer. The sequence of events surrounding this function is to call `matrixSslGetReadbuf` to retrieve empty buffer space, read or copy the received data from the peer into that buffer, and then call this function to allow MatrixSSL to decode the peer data. Notice the actual received buffer that is being processed is not passed as an input to this function, since it is internal to the SSL session structure. However, it is important that the `bytes` parameter correctly identifies how many bytes have been received, and thus be processed.

The return value from this function indicates how the user should respond next:

MATRIXSSL_REQUEST_RECV - The user must call `matrixSslGetReadbuf` again, copy additional peer data into the buffer, and call this function again. Typically this indicates that a partial record has been received, and more data must be read to complete the record. Also it can mean that a internal SSL record was processed internally and another record is expected to follow.

MATRIXSSL_REQUEST_SEND - The library has internally generated an SSL handshake response message to be sent to the peer. The user must call `matrixSslGetOutdata`, send the data to the peer, and then call `matrixSslSentData`.

MATRIXSSL_HANDSHAKE_COMPLETE - This is an indication that there are no remaining SSL handshake messages to be sent or received and the first application message can be sent. This is generally an important return code for a client application to handle because in most protocols it is the client that will be sending the initial application data request (such as an HTTPS GET or POST request). In this typical usage scenario, the user will then encrypt application data using the following steps: Call `matrixSslGetWritebuf` to retrieve an allocated buffer for outgoing application data, write the plaintext data to this buffer, call `matrixSslEncodeWritebuf` to encrypt the data, call `matrixSslGetOutdata` to retrieve the encrypted data, send that encrypted data to the peer, and finally call `matrixSslSentData` to notify the library the data has been sent.

NOTE: If this code is returned, there are not any additional full SSL records in the buffer available to parse, although there may be a partial record remaining. If there were a full SSL record available, for example an application data record, it would be parsed and `MATRIXSSL_APP_DATA` would be returned instead.

MATRIXSSL_APP_DATA - This means the received data was an application record and the plain text data is available in the `ptbuf` output parameter for user processing. The length of the plain text application data is indicated by the `ptLen` parameter. The user can either directly parse the read only data out of this buffer at this time or copy it aside to be parsed later. In either case it is essential the user call `matrixSslProcessedData` when finished working with it, so the buffer may be internally re-used and tested for the existence of an additional record. The user **MUST** parse or copy aside all unparsed data in the buffer, as it will be overwritten after the `matrixSslProcessedData` call.

NOTE: If application data has been appended to a handshake FINISHED message it is possible the `MATRIXSSL_APP_DATA` return code can be received without ever having received the `MATRIXSSL_HANDSHAKE_COMPLETE` return code. In this case, it is implied the handshake completed successfully because application data is being received.

MATRIXSSL_RECEIVED_ALERT - This means an alert has been decoded that the user should examine. The alert material will always be a two-byte plain text message available in the `ptbuf` parameter of the function (`ptLen` will be 2). The first byte will be the alert level. It will either be `SSL_ALERT_LEVEL_WARNING` or `SSL_ALERT_LEVEL_FATAL`. The second byte will be the alert identification as specified in the SSL and TLS RFC documents. It is sometimes possible to continue after receiving a WARNING level alert, but FATAL alerts should always result in the connection being closed. In either case the user should always call `matrixSslProcessedData` to update the library that the plain text data can be discarded.

2.17 matrixSslGetOutdata

```
int32 matrixSslGetOutdata(ssl_t *ssl, unsigned char **buf);
```

Parameter	Input/Output	Description
ssl	input	The SSL session context
buf	output	Pointer to beginning of data buffer that needs to be sent to the peer

Return Value	Description
> 0	The number of bytes in <code>buf</code> that need to be sent
0	No pending data to send
PS_ARG_FAIL	Failure. Bad input parameters

Servers and Clients

Any time the application is expecting to send data to a peer this function must be called to retrieve the memory location and length of the encoded SSL buffer. This API can also be polled to determine if there is encoded data pending that should be sent out the network.

The length of available bytes in `buf` is indicated in the return code.

There are several ways data can be encoded in outdata and ready to send:

1. After a client calls `matrixSslNewClientSession` this function must be called to retrieve the encoded CLIENT_HELLO message that will initiate the handshake
2. After a client or server calls `matrixSslEncodeRehandshake` this function must be called to retrieve the encoded SSL message that will initiate the rehandshake
3. If the `matrixSslReceivedData` function returns `MATRIXSSL_REQUEST_SEND` this function must be called to retrieve the encoded SSL handshake reply.
4. After the user calls `matrixSslEncodeWritebuf` this function must be called to retrieve the encrypted buffer for sending.
5. After the user calls `matrixSslEncodeToOutdata` this function must be called to retrieve the encrypted buffer for sending.
6. After the user calls `matrixSslEncodeClosureAlert` to encode the CLOSE_NOTIFY alert this function must be called to retrieve the encoded alert for sending.

After sending the returned bytes to the peer, the user must always follow with a call to `matrixSslSentData` to update the number of bytes that have been sent from the returned `buf`. Depending on how much data was sent, there may still be data to send within the internal outdata, and the function should be called again to ensure 0 bytes remain.

2.18 matrixSslProcessedData

```
int32 matrixSslProcessedData(ssl_t *ssl, unsigned char **ptbuf,  
                             uint32 *ptlen);
```

Parameter	Input/Output	Description
ssl	input	The SSL session context
ptbuf	output	If another full application record was present in the buffer that was returned from <code>matrixSslReceivedData</code> , this will be an updated pointer to this next decrypted record. Thus, this parameter is only meaningful if the return value of this function is <code>MATRIXSSL_APP_DATA</code> or <code>MATRIXSSL_RECEIVED_ALERT</code> .
ptlen	output	The length of the <code>ptbuf</code> parameter

Return Value	Test	Description
PS_SUCCESS	0	Success. This indicates that there are no additional records in the data buffer that require processing. The application protocol is responsible for deciding the next course of action.
MATRIXSSL_APP_DATA	> 0	Success. There is a second application data record in the buffer that has been decoded. In this return code case the <code>ptbuf</code> and <code>ptlen</code> output parameters will be valid. The user may process the data directly from <code>ptbuf</code> or copy it aside for later processing. After handling the data the user must call <code>matrixSslProcessedData</code> again to indicate the plain text data may be internally discarded.
MATRIXSSL_REQUEST_SEND	> 0	Success. This return code is possible if the buffer contained an application record followed by a SSL handshake message to initiate a re-handshake (<code>CLIENT_HELLO</code> or <code>HELLO_REQUEST</code>). In this case the SSL re-handshake response has been encoded and is waiting to be sent.
MATRIXSSL_REQUEST_RECV	> 0	Success. This return code is possible if there is a partial second record that follows in the buffer. Data storage must be retrieved via <code>matrixSslGetReadbuf</code> and passed through the <code>matrixSslReceivedData</code> call again.
MATRIXSSL_RECEIVED_ALERT	> 0	Success. There is a second record in the data buffer that is an SSL alert message. In this case, the <code>ptbuf</code> pointer will be two bytes (<code>ptlen</code> will be 2) in which the first byte will be the alert level and the second byte will be the alert description. After examining the alert, the user must call <code>matrixSslProcessedData</code> again to indicate the alert was processed and the data may be internally discarded.
PS_MEM_FAIL	< 0	Failure. Internal memory allocation failure
PS_ARG_FAIL	< 0	Failure. Bad input parameters
PS_PROTOCOL_FAIL	< 0	Failure. Internal protocol error

Servers and Clients

This essential function is called after the user has finished processing plaintext application data that was returned from `matrixSslReceivedData`. Specifically, this function must be called if the return code from `matrixSslReceivedData` was `MATRIXSSL_APP_DATA` or `MATRIXSSL_RECEIVED_ALERT`.

It is also possible that this function be called multiple times in succession if multiple SSL records have been received in a single `matrixSslReceivedData` call. See the very important section **Multi-Record Buffers** immediately below.

Plaintext application data is returned to the user through `matrixSslReceivedData` on a per-record basis whose length is stored internal to the library as part of the buffer management. This is why there are no input parameters regarding the length of the processed data. This function will destroy the plaintext record that was retrieved through the previous `matrixSslReceivedData` call (or the previous `matrixSslProcessedData` call) so if the user requires the data to persist it must be copied aside before calling this function.

Multi-Record Buffers

The `matrixSslReceivedData` function will only process a single application data record at a time. However, it is possible there will be more than one record in the buffer. In this case the return code from `matrixSslProcessedData` will indicate the status of the next record in the buffer. Any return code other than `PS_SUCCESS` (0) or a failure code (< 0) is an explicit indication that an additional record is present in the buffer and will inform the caller how it should be handled.

The multi-record return codes are a subset of the `matrixSslReceivedData` function and should be handled identically so it should be a straightforward code implementation to examine the return codes from this function in the standard processing loop. The `client.c` and `server.c` sample application files are a good reference for how to handle multi-record buffers.

2.19 matrixSslSentData

```
int32 matrixSslSentData(ssl_t *ssl, uint32 bytes);
```

Parameter	Input/Output	Description
ssl	input	The SSL session context
bytes	input	Length, in bytes, of how much data has been written out to the peer

Return Value	Test	Description
PS_SUCCESS	0	Success. No pending data remaining
MATRIXSSL_REQUEST_SEND	> 0	Success. Call <code>matrixSslGetOutdata</code> again and send more data to the peer. Indicates the number of bytes sent was not the full amount of pending data.
MATRIXSSL_REQUEST_CLOSE	> 0	Success. This indicates the message that was sent to the peer was an alert and the caller should close the session.
MATRIXSSL_HANDSHAKE_COMPLETE	> 0	Success. Will be returned to the peer if this is the final FINISHED message that is being sent to complete the handshake.
PS_ARG_FAIL	< 0	Failure. Bad input parameters.

Servers and Clients

This function must be called each time data has been sent to the peer. The flow of this function is that the user first calls `matrixSslGetOutdata` to retrieve the outgoing data buffer, the user sends part or all of this data, and then calls `matrixSslSentData` with how many bytes were actually sent.

The return value from this function indicates how the user should respond next:

MATRIXSSL_REQUEST_SEND - There is still pending data that needs to be sent to the peer. The user must call `matrixSslGetOutdata`, send the data to the peer, and then call `matrixSslSentData` again.

MATRIXSSL_SUCCESS - All of the data has been sent and the application will likely move to a state of awaiting incoming data.

MATRIXSSL_REQUEST_CLOSE - All of the data has been sent and the application should close the connection. This will be the case if the data being sent is a closure alert (or fatal alert).

MATRIXSSL_HANDSHAKE_COMPLETE - This is an indication that this peer is sending the final FINISHED message of the SSL handshake. In general this will be an important return code for client

applications to handle because most protocols will rely on the client sending an initial request to the server once the SSL handshake is complete. If a client receives this return code, a resumed handshake has just completed.

2.20 matrixSslGetWritebuf

```
int32 matrixSslGetWritebuf(ssl_t *ssl, unsigned char **buf,  
                           uint32 requestedLen);
```

Parameter	Input/Output	Description
ssl	input	The SSL session context
buf	output	Pointer to allocated storage that the user will copy plaintext application data into
requestedLen	input	The amount of buffer space, in bytes, the caller would like to use

Return Value	Test	Description
> 0		Success. The number of bytes available in buf. Might not be the same as requestedLen
PS_MEM_FAIL	< 0	Failure. Internal memory allocation error
PS_ARG_FAIL	< 0	Failure. Bad input parameters
PS_FAILURE	< 0	Failure. Internal error managing data buffers

Servers and Clients

This function is used in conjunction with `matrixSslEncodeWritebuf` when the user has application data that needs to be sent to the peer. This function will return an allocated buffer in which the user will copy the plaintext data that needs to be encoded and sent to the peer.

The event sequence for sending plaintext application data is as follows:

1. The user first determines the length of the plaintext that needs to be sent
2. The user calls `matrixSslGetWritebuf` with that length to retrieve an allocated buffer.
3. The user writes the plaintext into the buffer and then calls `matrixSslEncodeWritebuf` to encrypt the plaintext
4. The user calls `matrixSslGetOutdata` to retrieve the encoded data and length to be sent
5. The user sends the out data buffer contents to the peer
6. The user calls `matrixSslSentData` with the number of bytes that were sent

The internal buffer will grow to accommodate the `requestedLen` bytes and this function may be called multiple times (in conjunction with `matrixSslEncodeWritebuf`) before sending the data out via `matrixSslGetOutdata`. However, if the requested length is larger than the maximum allowed SSL plaintext length the return code will be smaller than the `requestedLen` value. In this fragmentation case, the caller must adhere to the returned length and only copy in as much plaintext as allowed. These two functions can then be called again immediately to retrieve a new buffer to encode the remainder of the plaintext data. It is also possible to receive a value that is smaller than `requestedLen` if using this function in MatrixDTLS when the encoded size will exceed the maximum datagram size (PMTU).

This function is most appropriate when sending a file or application data that is generated on the fly into the returned buffer. If the user wishes to encode an existing plaintext buffer the function, `matrixSslEncodeToOutdata` may be used as an alternative to this function to avoid having to copy the plaintext data into the returned buffer.

This function is specific to application level data. This function is not necessary during the SSL handshake portion of the connection because the MatrixSSL library internally generates all SSL handshake records.

2.21 matrixSslEncodeWritebuf

```
int32 matrixSslEncodeWritebuf(ssl_t *ssl, uint32 len);
```

Parameter	Input/Output	Description
ssl	input	The SSL session context
len	input	Length of plaintext data

Return Value	Test	Description
> 0		Success. The number of bytes in the encoded buffer to send to the peer. Will be a larger value than the input len parameter.
PS_ARG_FAIL	< 0	Failure. Bad input parameters
PS_PROTOCOL_FAIL	< 0	Failure. This session is flagged for closure at the time of this call
PS_FAILURE	< 0	Failure. Internal error managing buffers

Servers and Clients

This function is used in conjunction with `matrixSslGetWritebuf` when the user has application data that needs to be sent to the peer. This function will encrypt the plaintext data that has been copied into the buffer that was previously returned from a call to `matrixSslGetWritebuf`.

The event sequence for sending plaintext application data is as follows:

1. The user first determines the length of the plaintext that needs to be sent
2. The user calls `matrixSslGetWritebuf` with that length to retrieve an allocated buffer.
3. The user writes the plaintext into the buffer and then calls `matrixSslEncodeWritebuf` to encrypt the plaintext
4. The user calls `matrixSslGetOutdata` to retrieve the encoded data to be sent
5. The user sends the out data buffer contents to the peer
6. The user calls `matrixSslSentData` with the number of bytes that were sent

If the user wishes to encode an existing plaintext buffer the function `matrixSslEncodeToOutdata` may be used as an alternative to this function. This function is specific to application level data. This function is not necessary during the SSL handshake portion of the connection because the MatrixSSL library internally generates all SSL handshake records.

2.22 matrixSslEncodeToOutdata

```
int32 matrixSslEncodeToOutdata(ssl_t *ssl, unsigned char *ptBuf, uint32 len);
```

Parameter	Input/Output	Description
ssl	input	The SSL session context
ptBuf	input	Pointer to plaintext application data that will be encrypted into the internal outdata buffer for sending to the peer
len	input	Length, in bytes, of ptBuf

Return Value	Test	Description
> 0		Success. The number of bytes in the encoded buffer to send to the peer. Will be a larger value than the input <code>len</code> parameter.
PS_LIMIT_FAIL	< 0	Failure. The plaintext length must be smaller than the SSL specified value of 16KB. In MatrixDTLS this return code indicates the encoded size will exceed the maximum datagram size.
PS_MEM_FAIL	< 0	Failure. The internal allocation of the destination buffer failed.
PS_ARG_FAIL	< 0	Failure. Bad input parameters
PS_PROTOCOL_FAIL	< 0	Failure. This session is flagged for closure.
PS_FAILURE	< 0	Failure. Internal error managing buffers.

Servers and Clients

This function offers an alternative method to `matrixSslEncodeWritebuf` when the user has application data that needs to be sent to the peer. This function will encrypt the plaintext data to the internal output buffer while leaving the plaintext data untouched. This function does not require that `matrixSslGetWritebuf` be called first.

This function is specific to application level data. This function is not necessary during the SSL handshake portion of the connection because the MatrixSSL library internally generates any SSL handshake records.

The event sequence for sending plaintext application data is as follows:

1. The user calls `matrixSslEncodeToOutdata` with the plaintext buffer location and length.
2. The user calls `matrixSslGetOutdata` to retrieve the encoded data to be sent
3. The user sends the out data buffer contents to the peer
4. The user calls `matrixSslSentData` with the number of bytes that were sent

2.23 matrixSslEncodeClosureAlert

```
int32 matrixSslEncodeClosureAlert(ssl_t *ssl);
```

Parameter	Input/Output	Description
ssl	input	The SSL session context

Return Value	Test	Description
PS_SUCCESS	0	Success. The alert is ready to be retrieved and sent.
PS_PROTOCOL_FAIL	< 0	Failure. SSL context not in correct state to create the alert or there was an error encrypting the alert message.
PS_ARG_FAIL	< 0	Failure. Bad input parameter
PS_MEM_FAIL	< 0	Failure. Internal memory allocation error

Servers and Clients

The SSL specification highlights an optional alert message that SHOULD be sent prior to closing the communication channel with a peer. This function generates this CLOSE_NOTIFY alert that the peer may send to the other side to notify that the connection is about to be closed. Many implementations simply close the connection without an alert, but per spec, this message should be sent first. Our recommendation is to make an attempt to send the closure alert as a non-blocking message and ignore the return value of the attempt. This way, best efforts are made to send the alert before closing, but application code does not block or fail on a connection that is about to be closed.

After calling this function the user must call `matrixSslGetOutdata` to retrieve the buffer for the encoded alert to send.

2.24 matrixSslGetAnonStatus

```
void matrixSslGetAnonStatus(ssl_t *ssl, int32 *anon);
```

Parameter	Input/Output	Description
ssl	input	The SSL session context
anon	output	1 – Anonymous 0 - Authenticated

Clients

This function returns whether or not the server session is anonymous in the `anon` output parameter. A value of 1 indicates the peer is anonymous and a value of 0 indicates the connection has been fully authenticated. An anonymous connection in this case means the application explicitly allowed the SSL handshake to continue despite not being able to authenticate the certificate supplied by the other side with an available Certificate Authority. The mechanism to allow an anonymous connection is for the certificate validation callback function to return `SSL_ALLOW_ANON_CONNECTION`. Detailed information on the callback routine can be found below in the section entitled **The Certificate Validation Callback Function**.

`matrixSslGetAnonStatus` is only meaningful to call after the successful completion of the SSL handshake. Anonymous connections are not normally recommended but can be useful in a scenario in which encryption is the only security concern. Other reasons the caller may choose to use anonymous connections might be to allow a subset of the normal functionality to anonymous connectors or to temporarily accept a connection while a certificate upgrade is being performed.

Servers

Calling this routine from the server side is meaningless for an implementation that has not performed client authentication. In other words, it is not possible for one side of the connection to know if the peer believes the connection to be anonymous or not. This is an easy rule to remember if you recall the mechanism to allow anonymous connections is controlled through the certificate validation callback routine when the `SSL_ALLOW_ANON_CONNECTION` define is returned.

2.25 matrixSslEncodeRehandshake

```
int32 matrixSslEncodeRehandshake(ssl_t *ssl, sslKeys_t *keys,  
                                int32 (*certCb)(ssl_t *, psX509Cert_t *, int32),  
                                uint32 sessionOption, uint32 cipherSpecs[],  
                                uint16 cipherCount);
```

Parameter	Input/Output	Description
ssl	input	The SSL session context
keys	input	Populated key structure if changing key material for this re-handshake. NULL if not changing key material
certCb	input	Certificate callback function for the re-handshake if a change is being made to it. NULL to keep existing callback
sessionOption	input	<code>SSL_OPTION_FULL_HANDSHAKE</code> or 0
cipherSpecs	input	Client specific. Cipher suites for the re-handshake. Only meaningful if the <code>sessionOption</code> parameter is set to <code>SSL_OPTION_FULL_HANDSHAKE</code>
cipherCount	input	If <code>cipherSpecs</code> is used to nominate specific suites, this parameter must be the array size.

Return Value	Test	Description
PS_SUCCESS	0	Success. Handshake message is encoded and ready for retrieval.
PS_UNSUPPORTED_FAIL	< 0	Failure. Client specific. Cipher spec could not be found.
PS_PROTOCOL_FAIL	< 0	Failure. SSL context not in correct state for a re-handshake or buffer management error.
PS_ARG_FAIL	< 0	Failure. Bad input parameter
PS_MEM_FAIL	< 0	Failure. Internal memory allocation error
PS_PLATFORM_FAIL	< 0	Failure. Client specific. Error in <code>psGetEntropy</code> when encoding CLIENT_HELLO

Clients and Servers

Clients or servers call this function on an already secure connection to initiate a re-handshake. A re-handshake is an encrypted SSL handshake performed over an existing connection in order to derive new symmetric key material and/or to change the public keys or cipher suite of the secured communications.

A re-handshake can either be a full handshake or a resumed handshake and the determination is made by the input parameters to this function.

A resumed re-handshake will be used if the `keys`, `certCb`, `sessionOption`, and `cipherSpecs` parameters are all set to 0 (or `NULL` for pointers). This is an indication that there is no underlying algorithm or handshake type change that is being made to the connection and the intention is simply to re-key the encrypted communications.

If the `keys`, `certCb`, or `cipherSpecs` parameters are set, this is an indication that an “upgraded” connection is desired and a full handshake will be performed with the new parameters.

A full re-handshake can always be guaranteed if `SSL_OPTION_FULL_HANDSHAKE` is passed as the `sessionOption` parameter to this function.

After calling this function the user must call `matrixSslGetOutdata` to retrieve the buffer for the encoded HELLO message to send.

Servers

This function is called on the server side to build a HELLO_REQUEST message to be passed to a client to initiate a re-handshake. This is the only mechanism in the SSL protocol that allows the server to initiate a handshake.

As with `matrixSslNewServerSession` the nomination of a `certCb` is in explicit indication that a client authentication handshake should be performed.

Note that the SSL specification allows clients to ignore a HELLO_REQUEST message. The MatrixSSL client does not ignore this message and will send a CLIENT_HELLO message with the current session ID to initiate a resumed handshake.

Clients

If a client invokes this function a new CLIENT_HELLO handshake message will be internally generated.

For more information about re-handshaking and related security issues, see the Re-handshake section of the [MatrixSSL Developers Guide](#).

2.26 matrixSslDisableRehandshakes

```
int32 matrixSslDisableRehandshakes(ssl_t *ssl);
```

Parameter	Input/Output	Description
ssl	input	The SSL session context

Return Value	Test	Description
PS_SUCCESS	0	Success.
PS_ARG_FAIL	< 0	Failure. Bad input parameter

Clients and Servers

Clients or servers call this function on sessions to disable engaging in a re-handshake with a peer that is attempting to initiate one. Once called, this function will internally generate a NO_RENEGOTIATION alert each time a peer attempts a re-handshake.

NOTE: This ability to disable and re-enable re-handshake support overrides the “re-handshake credit” mechanism. For more information on the “re-handshake credit” mechanism see the Re-handshake section of the MatrixSSL Developers Guide.

2.27 matrixSslReEnableRehandshakes

```
int32 matrixSslReEnableRehandshakes(ssl_t *ssl);
```

Parameter	Input/Output	Description
ssl	input	The SSL session context

Return Value	Test	Description
PS_SUCCESS	0	Success.
PS_ARG_FAIL	< 0	Failure. Bad input parameter

Clients and Servers

Clients or servers call this function on sessions that have been previous disabled with `matrixSslDisableRehandshakes`. Once called, this function will internally generate the proper handshake message response next time a peer attempts a re-handshake. Once re-enabled the “re-handshake credit” mechanism is enforced as normal. One “re-handshake credit” is given when this function is called.

NOTE: This ability to disable and re-enable re-handshake support overrides the “re-handshake credit” mechanism. For more information on the “re-handshake credit” mechanism see the Re-handshake section of the MatrixSSL Developers Guide.

2.28 matrixSslSetCipherSuiteEnabledStatus

```
int32 matrixSslSetCipherSuiteEnabledStatus(ssl_t *ssl,  
                                           uint16 cipherId, uint32 status);
```

Parameter	Input/Output	Description
ssl	input	The SSL session context or NULL for a global setting
cipherId	input	A single SSL/TLS specification cipher suite ID. Values may be found in <i>matrixssllib.h</i>
status	input	PS_FALSE to disabled the cipher suite or PS_TRUE to re-enable a previously disabled cipher suite.

Return Value	Test	Description
PS_SUCCESS	0	Success. Cipher suite has been successfully enabled or disabled
PS_FAILURE	< 0	Failure. The cipher suite specified in <i>cipherId</i> was not found
PS_LIMIT_FAIL	< 0	Failure. No additional room to store disabled cipher. Increase the <i>SSL_MAX_DISABLED_CIPHERS</i> define.
PS_ARG_FAIL	< 0	Failure. Bad input parameter

Servers

This function may be called on the server side to programmatically disable (PS_FALSE) and re-enable (PS_TRUE) cipher suites that have been compiled into the library. By default, all cipher suites compiled into the library (as defined in *matrixssl/Config.h*) will be enabled and available for clients to connect with.

The disabling of a cipher suite may be done at a global level or a per-session level. If the *ssl* parameter to this routine is NULL, the setting will be global. If the server wishes to disable ciphers on a per-session basis this function must be called immediately after *matrixSslNewServerSession* using the new *ssl_t* structure that was returned from that session creation function. If a cipher suite has been globally disabled the per-session setting will be ignored.

The maximum number of cipher suites that may be disabled on a per-session basis is determined by the value of *SSL_MAX_DISABLED_CIPHERS*. The default is 8. There is no limit to the number of cipher suites that may be globally disabled.

2.29 matrixSslDeleteSession

```
void matrixSslDeleteSession(ssl_t *ssl);
```

Parameter	Input/Output	Description
ssl	input	The SSL session context

Servers and Clients

This function is called at the conclusion of an SSL session that was created using *matrixSslNewServerSession* or *matrixSslNewClientSession*. This function will free the internally allocated state and buffers associated with the session. It should be called after the corresponding socket or network transport has been closed.

2.30 matrixSslDeleteSessionTicketKey

```
int32 matrixSslDeleteSessionTicketKey(sslKeys_t *keys,  
                                       unsigned char name[16]);
```

Parameter	Input/Output	Description
keys	input	The keys context
name	input	The name of the key to delete from the session ticket key list

Servers

If a session ticket key needs to be removed from the list, this function will perform that. If the first entry in the list is removed the new first entry will become the key used to encrypt newly issued tickets. If the final entry in the list is removed, the servers will no longer support the session ticket mechanism.

Return Value	Test	Description
PS_SUCCESS	0	Success. Key was found and deleted
PS_FAILURE	< 0	Failure. The key was not found

2.31 matrixSslDeleteKeys

```
void matrixSslDeleteKeys(sslKeys_t *keys);
```

Parameter	Input/Output	Description
keys	input	A pointer to an <code>sslKeys_t</code> value returned from a previous call to <code>matrixSslNewKeys</code>

Servers and Clients

This function is called to free the key structure and elements allocated from a previous call to `matrixSslNewKeys`. Any key material that was loaded into the key structure using `matrixSslLoadRsaKeys`, `matrixSslLoadEcKeys`, `matrixSslLoadDhParams`, **OR** `matrixSslLoadPsk` will also be freed and the dedicated memory pool (if `USE_MATRIX_MEMORY_MANAGEMENT`) will be closed.

2.32 matrixSslClose

```
void matrixSslClose(void);
```

Servers and Clients

This function performs the one-time final cleanup for the MatrixSSL library. Applications should call this function as part of their own de-initialization.

2.33 matrixSslNewHelloExtension

```
int32 matrixSslNewHelloExtension(tlsExtension_t **extension,  
                                void *poolUserPtr);
```

Parameter	Input/Output	Description
extension	output	Newly allocated <code>tlsExtension_t</code> structure to be used as input to <code>matrixSslLoadHelloExtension</code>
poolUserPtr	input	Optional user context for the creation of the memory pool that will hold the extension material. Only relevant to commercial versions when <code>USE_MATRIX_MEMORY_MANAGEMENT</code> is enabled. NULL otherwise.

Return Value	Test	Description
PS_SUCCESS	0	Success. The <code>extension</code> parameter is ready for use
PS_MEM_FAIL	< 0	Failure. Internal memory allocation failure

Clients

Facilitates support for the client side hello extension mechanism defined in RFC 3546. This function allocates a new `tlsExtension_t` that `matrixSslLoadHelloExtension` will use to populate with extension data. This populated extension parameter will eventually be passed to `matrixSslNewClientSession` in the extensions input parameter so that `CLIENT_HELLO` will be encoded with the desired hello extensions.

If the client is expecting the server to reply with extension data in the `SERVER_HELLO` message, the client should register an extension callback routine when calling `matrixSslNewClientSession`.

Memory Profile

The user must free `tlsExtension_t` with `matrixSslDeleteHelloExtension` after the useful life. The extension data is internally copied into the `CLIENT_HELLO` message during the call to `matrixSslNewClientSession` so `matrixSslDeleteHelloExtension` may be called immediately after `matrixSslNewClientSession` if the user does not require further use.

2.34 matrixSslLoadHelloExtension

```
int32 matrixSslLoadHelloExtension(tlsExtension_t *extension,  
                                  unsigned char *extData, uint32 extLen, uint32 extType);
```

Parameter	Input/Output	Description
extension	input	Previously allocated <code>tlsExtension_t</code> structure from a call to <code>matrixSslNewExtension</code>
extData	input	A single, fully encoded hello extension to be included in the <code>CLIENT_HELLO</code> message. Formats for extensions can be found in RFC 3546
extLen	input	Length, in bytes, of <code>extData</code>
extType	input	The standardized extension type.

Return Value	Test	Description
PS_SUCCESS	0	Success. The data has been added to the extension
PS_MEM_FAIL	< 0	Failure. Memory allocation failure
PS_ARG_FAIL	< 0	Failure. Bad input parameters

Clients

Enables basic support for the client side hello extension mechanism, as defined in RFC 3546.

Extension data to the `extData` must be formatted per specification. For example, the `ServerNameList` extension must be encoded in the format per RFC 3546:

```
struct {
    NameType name_type;
    select (name_type) { case host_name: HostName; } name;
} ServerName;

enum { host_name(0), (255) } NameType;

opaque HostName<1..2^16-1>;

struct { ServerName server_name_list<1..2^16-1> } ServerNameList;
```

The `extType` parameter will also be a value as specified by a standards body. The extensions defined in RFC 3546, for example:

```
enum {
    server_name(0), max_fragment_length(1),
    client_certificate_url(2), trusted_ca_keys(3),
    truncated_hmac(4), status_request(5), (65535)
} ExtensionType;
```

It is possible to call this function multiple times for each extension that needs to be added. On success, this populated extension parameter will be passed to `matrixSslNewClientSession` in the `extensions` input parameter so that `CLIENT_HELLO` will be encoded with the desired hello extensions.

Note the current level of support in MatrixSSL does not include the additional handshake messages of `CERTIFICATE_URL` and `CERTIFICATE_STATUS` that accompany some of these extension types. For information on how to fully support these features, please contact Inside Secure.

If the client is expecting the server to reply with extension data in the `SERVER_HELLO` message, the client should register an extension callback routine when calling `matrixSslNewClientSession`.

Memory Profile

The `extData` memory is internally copied into the `extension` structure so the caller may immediately free `extData` upon return from this function.

2.35 matrixSslDeleteHelloExtension

```
void matrixSslDeleteHelloExtension(tlsExtension_t *extension);
```

Parameter	Input/Output	Description
extension	input	A pointer to an <code>tlsExtension_t</code> value returned from a previous call to <code>matrixSslNewHelloExtension</code>

Clients

This function is called to free the structure allocated from a previous call to `matrixSslNewHelloExtension`. Any extension material that was loaded into the key structure using `matrixSslLoadHelloExtension` will also be freed.

It is possible to call this function immediately after `matrixSslNewClientSession` returns because the extension data will have been internally copied into the `CLIENT_HELLO` message.

Define Dependencies

USE_CLIENT_SIDE_SSL	Must be enabled in matrixsslConfig.h
---------------------	--------------------------------------

2.36 matrixSslsSessionCompressionOn

```
int32 matrixSslIsSessionCompressionOn(ssl_t *ssl);
```

Parameter	Input/Output	Description
ssl	input	The ssl session context

Return Value	Test	Description
PS_TRUE	> 0	Yes, the session has been negotiated to a compressed state and application data must be compressed before encryption
PS_FALSE	== 0	No, application data should not be compressed prior to encrypting

Servers and Clients

This function is called to test whether the session has been negotiated to a zlib compression state. This would only be possible if `USE_ZLIB_COMPRESSION` has been enabled for the library. If this function returns `PS_TRUE`, all application data must be compressed by the application prior to sending it to the MatrixSSL public APIs for encryption.

2.37 matrixSslRegisterSNICallback

```
void matrixSslRegisterSNICallback(ssl_t *ssl,
    void (*sni_cb)(void *ssl, char *hostname, int32 hostnameLen,
        sslKeys_t **newKeys));
```

Parameter	Input/Output	Description
ssl	input	The ssl session context.
sni_cb	input	The callback being registered

Servers

This function is to support the Server Name Indication hello extensions. It is relevant to servers that are expecting clients to connect with an explicit server hostname in the `CLIENT_HELLO`. The server will use this mechanism to locate the correct X.509 certificate and private key to accommodate the client.

This function **MUST** be called immediately after `matrixSslNewServerSession`, prior to any data processing, so that the callback can be registered before the parsing of the `CLIENT_HELLO` message. The server still must invoke `matrixSslNewServerSession` with valid default keys to initialize the state for cases in which a client does not provide a Server Name Indication extension.

When the user callback is invoked, the `hostname` and `hostnameLen` will be used to identify the proper key material and that key material will be passed back in the output double pointer `newKeys` in the `sslKeys_t` structure format. It is the responsibility of the application to manage the `sslKeys_t` structure by calling one of the `matrixSslLoad` variants (`matrixSslLoadRsaKeys` for example) from the key load family of APIs and to destroy the `sslKeys_t` structure using `matrixSslDeleteKeys` after the useful life.

The success or failure of locating and loading the proper key material is indicated through the successful assignment of `newKeys`. If keys cannot be found or loaded a `NULL` assignment should be made to `newKeys`. In this case the server will send a fatal `UNRECOGNIZED_NAME` alert to the client.

Memory Profile

The application is responsible for managing the `sslKeys_t` structure that is returned in the `newKeys` output parameter of the callback.

Define Dependencies

USE_SERVER_SIDE_SSL	Must be enabled in <i>matrixsslConfig.h</i>
---------------------	---

2.38 matrixSslCreateSNIext

```
int32 matrixSslCreateSNIext(psPool_t *pool, unsigned char *host,
                           int32 hostLen, unsigned char **extOut, int32 *extLen);
```

Parameter	Input/Output	Description
pool	input	The memory pool to use in the allocation of the output buffer. NULL if not needed.
host	input	The hostname of the server that the client wishes to connect to
hostLen	input	The byte length of the host parameter
extOut	output	The returned formatted SNI extension buffer
extLen	output	The byte length of the output extOut parameter

Return Value	Test	Description
PS_SUCCESS	== 0	Success
PS_MEM_FAIL	< 0	Memory allocation failure

Clients

This utility function helps format the Server Name Indication extension for including in the CLIENT_HELLO message. The resulting output in `extOut` should be fed into the `matrixSslLoadHelloExtension` API with the value of `EXT_SNI` as the `extType`.

Memory Profile

The application should free the returned `extOut` memory buffer after the call to `matrixSslLoadHelloExtension` since that function will copy the data internally.

2.39 matrixSslRegisterALPNCallback

```
void matrixSslRegisterALPNCallback(ssl_t *ssl,
                                   void (*srv_alpn_cb)(void *ssl, short protoCount,
                                                         char *proto[MAX_PROTO_EXT],
                                                         int32 protoLen[MAX_PROTO_EXT], int32 *index));
```

Parameter	Input/Output	Description
ssl	input	The ssl session context
srv_alpn_cb	input	The ALPN callback being registered

Servers

This function is to support the Application Layer Protocol Negotiation hello extension defined in RFC 7301. It is relevant to servers that are expecting clients to use this extension to negotiate the protocol that will be used at the conclusion of the TLS handshake.

This function **MUST** be called immediately after `matrixSslNewServerSession`, prior to any data processing, so that the callback can be registered before the parsing of the CLIENT_HELLO message.

The server ALPN callback that is registered must have a prototype of:

```
void ALPN_callback(void *ssl, short protoCount, char *proto[MAX_PROTO_EXT],
    int32 protoLen[MAX_PROTO_EXT], int32 *index)
```

The `ssl` parameter is the session context and may be typecast to an `ssl_t*` type if access is required.

The `protoCount` is the number of protocols that the client has sent in the CLIENT_HELLO extension. It is the count of the number of array entries in the `proto` and `protoLen` parameters to follow.

The `proto` parameter is the priority-ordered list of string protocol names the client wants to communicate with following the TLS handshake. The `protoLen` parameter holds the string lengths of the `proto` counterpart parameter for each protocol.

The `index` parameter is an **output** that the callback logic will assign based on the desired action:

- The index of the `proto` array member the server has agreed to use. **The index is the zero-based index to the array** so a return value of 0 will indicate the first protocol in the list. This selection will result in the server including its own ALPN extension in the SERVER_HELLO message with the chosen protocol.
- A negative value assigned to `index` indicates the server is not willing to communicate using any of the protocols. A fatal “no_application_protocol” alert will be sent to the client and the handshake will terminate.
- If the callback does not assign any value to the outgoing parameter, the server will not take any action. That is, neither a reply ALPN extension nor an alert will be sent to the client and the handshake will continue normally.

Define Dependencies

USE_ALPN	Must be enabled in <i>matrixsslConfig.h</i>
----------	---

2.40 matrixSslCreateALPNext

```
int32 matrixSslCreateALPNext(psPool_t *pool, int32 protoCount,
    unsigned char *proto[], int32 protoLen[],
    unsigned char **extOut, int32 *extLen);
```

Parameter	Input/Output	Description
pool	input	The memory pool to use in the allocation of the output buffer. NULL if not needed.
protoCount	input	The count of protocols provided in the <code>proto</code> and <code>protoLen</code> parameters
proto	input	The string array of protocols the client is able to use in communications with the server
protoLen	input	The integer array of lengths corresponding to the protocols in the <code>proto</code> parameter

extOut	output	The returned formatted ALPN extension buffer
extLen	output	The byte length of the output extOut parameter

Return Value	Test	Description
PS_SUCCESS	== 0	Success
PS_MEM_FAIL	< 0	Memory allocation failure
PS_ARG_FAIL	< 0	The protoCount param is larger than the MAX_PROTO_EXT define or a protocol string length is too large

Clients

This utility function helps format the Application Layer Protocol Negotiation extension for including in the CLIENT_HELLO message. The resulting output in `extOut` should be fed into the `matrixSslLoadHelloExtension` API with the value of `EXT_ALPN` as the `extType`.

Memory Profile

The application should free the returned `extOut` memory buffer after the call to `matrixSslLoadHelloExtension` since that function will copy the data internally.

Define Dependencies

USE_ALPN	Must be enabled in <i>matrixsslConfig.h</i>
----------	---

2.41 matrixSslLoadOCSPResponse

```
int32 matrixSslLoadOCSPResponse(sslKeys_t *keys,
                                const unsigned char *OCSPResponse, uint16_t OCSPResponseLen);
```

Parameter	Input/Output	Description
keys	input	An allocated sslKeys_t structure in which to add the OCSP response buffer
OCSPResponse	input	The ASN.1 X.509 OCSP response for the server's identity certificate
OCSPResponseLen	input	The byte length of OCSPResponse

Return Value	Test	Description
PS_SUCCESS	== 0	Success
PS_MEM_FAIL	< 0	Memory allocation failure
PS_ARG_FAIL	< 0	Input parameters are NULL or 0

Servers

A server application wishing to support OCSP stapling must keep an updated OCSP response loaded into the key material by calling `matrixSslLoadOCSPResponse`. This function takes a fully formed OCSPResponse ASN.1 buffer and loads it into the provided `sslKeys_t` structure. When a new OCSP response is fetched, the same `matrixSslLoadOCSPResponse` API can be called to delete any previous response and load the update.

When a client sends the `status_request` extension the server will look to see if an OCSP response is available in the `sslKeys_t` structure and reply with a `status_request` extension and the `CERTIFICATE_STATUS` message.

Memory Profile

The OCSP response will be freed when `matrixSslDeleteKeys` is called.

Define Dependencies

USE_OCSP	Must be enabled in <i>cryptoConfig.h</i>
----------	--

2.42 matrixSslWriteOCSPRequest

```
int32 matrixSslWriteOCSPRequest(psPool_t *pool, psX509Cert_t *cert,  
                                psX509Cert_t *certIssuer, unsigned char **request,  
                                uint32_t *requestLen);
```

Parameter	Input/Output	Description
pool	input	The memory pool to use in the allocation of the output buffer. NULL if not needed.
cert	input	The certificate for which the OCSP request is being made
certIssuer	input	The issuing certificate of the subject cert
request	output	The DER stream of the generated OCSP request
requestLen	output	Byte length of request

Return Value	Test	Description
PS_SUCCESS	== 0	Success
PS_MEM_FAIL	< 0	Memory allocation failure

This function will generate an OCSP request that can be sent to an OCSP responder to retrieve an updated response.

The `./apps/ssl/server.c` example application has a sample usage of this API along with how to insert the request into an HTTP POST to send the request and receive the response from an OCSP responder.

Memory Profile

The `request` must be freed with `psFree`.

Define Dependencies

USE_OCSP	Must be enabled in <i>cryptoConfig.h</i>
----------	--

3 MATRIXDTLS API

DTLS is an extension of the TLS protocol that enables the same strong level of security to be implemented over non-reliable transport mechanisms such as UDP. In addition to this API documentation, the MatrixDTLS Developer's Guide discusses all the differences that a developer needs to know when implementing MatrixDTLS.

3.1 Debug Configuration

The *matrixssl/Config.h* file contains the full set of compile-time configurable options for the protocol. Most of the features are documented in the *MatrixSSL Developer Guide*.

3.2 Integration Notes

With the exception of two functions, the entire MatrixSSL public API set is available for use in MatrixDTLS and this MatrixSSL API document is the primary technical reference for the interface for both products.

In MatrixDTLS the function `matrixDtlsGetOutdata` is used instead of `matrixSslGetOutdata` and the function `matrixDtlsSentData` is used instead of `matrixSslSentData`. The prototypes for these functions are identical to their MatrixSSL counterparts and are documented below.

The only other change that is required for DTLS use is to pass `SSL_FLAGS_DTLS` in the `versionFlag` member of the `options` structure as the final parameter to `matrixSslNewClientSession` and `matrixSslNewServerSession`.

3.3 matrixDtlsGetOutdata

```
int32 matrixDtlsGetOutdata(ssl_t *ssl, unsigned char **buf);
```

Parameter	Input/Output	Description
ssl	input	The SSL session context
buf	output	Pointer to beginning of data buffer that needs to be sent to the peer

Return Value	Description
0	No pending data to send
> 0	The number of bytes in <code>buf</code> that need to be sent
PS_ARG_FAIL	Failure. Bad input parameters

This function must be used instead of `matrixSslGetOutdata`

Servers and Clients

Any time the application is expecting to send data to a peer this function must be called to retrieve the memory location and length of the encoded DTLS buffer. This API is used in conjunction with `matrixDtlsSentData` and MUST be called in a loop until it returns 0.

The length of encoded bytes in `buf` that needs to be sent is passed through the return code and that value will always be within the Maximum Transmission Unit that was set by default with the `DTLS_PMTU` define or the updated value set by `matrixDtlsSetPmtu`.

The unique DTLS functionality included in this version of `GetOutdata` is that it will return an encoded flight of handshake messages that has previously been sent. This resend case must be determined by the application itself if a timeout from the peer has occurred. This case is highlighted as number 7 in the following list.

There are several ways data can be encoded into outdata and ready to send:

1. After a client calls `matrixSslNewClientSession` this function must be called to retrieve the encoded CLIENT_HELLO message that will initiate the handshake
2. After a client or server calls `matrixSslEncodeRehandshake` this function must be called to retrieve the encoded SSL message that will initiate the re-handshake
3. If the `matrixSslReceivedData` function returns `MATRIXSSL_REQUEST_SEND` this function must be called to retrieve the encoded SSL handshake reply.
4. After the user calls `matrixSslEncodeWritebuf` this function must be called to retrieve the encrypted buffer for sending.
5. After the user calls `matrixSslEncodeClosureAlert` to encode the CLOSE_NOTIFY alert this function must be called to retrieve the encoded alert for sending.
6. After the user calls `matrixSslEncodeToOutdata` this function must be called to retrieve the encrypted buffer for sending.
7. If the application logic has determined a DTLS timeout has occurred during the handshake phase this function must be called to rebuild the previous flight of handshake message to be resent to the peer.

After sending the returned bytes to the peer, the user must always follow with a call to `matrixDtlsSentData` to update the number of bytes that have been sent from the returned `buf`. After each call to `matrixDtlsSentData` this function must be called again to set the resend state machine to the proper state.

3.4 matrixDtlsSentData

```
int32 matrixDtlsSentData(ssl_t *ssl, uint32 bytes);
```

Parameter	Input/Output	Description
ssl	input	The SSL session context
bytes	input	Length, in bytes, of how much data has been written out to the peer

Return Value	Test	Description
MATRIXSSL_REQUEST_SEND	> 0	Success. Call <code>matrixDtlsGetOutdata</code> again and send more data to the peer. The number of <code>bytes</code> sent was not the full amount of pending data.
MATRIXSSL_SUCCESS	0	Success. No pending data remaining.
MATRIXSSL_REQUEST_CLOSE	> 0	Success. If this was an alert message that was being sent, the caller should close the session.
MATRIXSSL_HANDSHAKE_COMPLETE	> 0	Success. Will be returned to the peer if this is the final FINISHED message that is being sent to complete the handshake.
PS_ARG_FAIL	< 0	Failure. Bad input parameters.

This function must be used instead of `matrixSslSentData`

Servers and Clients

This function must be called each time data has been sent to the peer. The flow of this function is that the user first calls `matrixDtlsGetOutdata` to retrieve the outgoing data buffer, the user sends part or all of this data, and then calls `matrixDtlsSentData` with how many bytes were actually sent.

The return value from this function indicates how the user should respond next:

MATRIXSSL_REQUEST_SEND - There is still pending data that needs to be sent to the peer. The user must call `matrixDtlsGetOutdata`, send the data to the peer, and then call `matrixDtlsSentData` again.

MATRIXSSL_SUCCESS - All of the data has been sent and the application will likely move to a state of awaiting incoming data. The application must call `matrixDtlsGetOutdata` next.

MATRIXSSL_REQUEST_CLOSE - All of the data has been sent and the application should close the connection. This will be the case if the data being sent is a closure alert (or fatal alert).

MATRIXSSL_HANDSHAKE_COMPLETE - This is an indication that this peer is sending the final FINISHED message of the SSL handshake. In general this will be an important return code for client applications to handle because most protocols will rely on the client sending an initial request to the server once the SSL handshake is complete. If a client receives this return code, a resumed handshake has just completed. For details on how to handle handshake completion see the MatrixDTLS Developer's Guide. The application must call `matrixDtlsGetOutdata` next.

3.5 matrixDtlsSetPmtu

```
int32 matrixDtlsSetPmtu(int32 pmtu);
```

Parameter	Input/Output	Description
pmtu	input	The new Path Maximum Transmission Unit size for a datagram. <0 to reset the default value defined by <code>DTLS_PMTU</code>

Return Value	Description
> 0	The new PMTU value

Servers and Clients

This function is used to modify the global PMTU setting for the library. It is essential that the server and client in a DTLS connection agree on the maximum datagram size they can send and receive. Unlike standard SSL/TLS protocols, fragmentation is not supported at the transport layer. In DTLS, a fragment must be encoded into a single datagram. The library handles this transparently.

3.6 matrixDtlsGetPmtu

```
int32 matrixDtlsGetPmtu(void);
```

Return Value	Description
> 0	The current PMTU value

Servers and Clients

Retrieve the current PMTU value.

4 MATRIXSSL X.509 API

For documentation of MatrixSSL's X.509 APIs, including the certificate parsing, certificate generation and CRL APIs, please consult the separate *MatrixSSL Certificates and CRLs* document, included in the *MatrixSSL Commercial* and *MatrixSSL FIPS Editions*.

5 SESSION OPTIONS

The final parameter to `matrixSslNewClientSession` and `matrixSslNewServerSession` is an `sslSessOpts_t` pointer that allows per-session control for some TLS features.

```
typedef struct {
    short    ticketResumption;
    short    maxFragLen;
    short    truncHmac;
    short    extendedMasterSecret;
    short    trustedCAindication;
    short    OCSPstapling;
    int32    ecFlags;
    int32    versionFlag;
    void     *userPtr;
    void     *memAllocPtr;
    psPool_t *bufferPool;
} sslSessOpts_t;
```

All numeric member values must be set to 0 and pointers must be set to NULL if the default behaviour is desired.

A summary table of possible values is given after the discussion for each feature.

5.1 TLS version

The `versionFlag` member of `sslSessOpts_t` can be optionally set if a specific TLS version is desired for a session. See Table 3 below for possible values.

Clients

If using the `versionFlag` member to pass in a specific TLS protocol version, this will become the version passed to the server in the CLIENT_HELLO message. If the server does not support the requested version and returns an earlier protocol version in the SERVER_HELLO message the client will negotiate to that version. In effect, this protocol setting is nominating the latest version the client is willing to support rather than specifying the protocol that MUST be used. If a client truly wants to force a single protocol version, the compile-time defines for disabling certain protocol versions must be used in conjunction with this mechanism.

Servers

If using the `versionFlag` parameter to pass in a specific TLS protocol version, this will become the version passed to the client in the SERVER_HELLO message. If the client has requested an earlier protocol version in CLIENT_HELLO than what the server has forced here, the server will send a PROTOCOL_VERSION alert to the client.

5.2 Stateless Session Ticket Resumption

The `ticketResumption` member is used to enable stateless session ticket resumption (RFC 5077) on a per-session basis.

Clients

The `ticketResumption` member may be set to 1 if the stateless session ticket resumption method is to be used instead of the standard method (default). The `USE_STATELESS_SESSION_TICKETS` compile-time define must be enabled to support the feature.

Servers

Servers do not use this parameter. If `USE_STATELESS_SESSION_TICKET` is enabled and the server has registered some key material with `matrixSslLoadSessionTicketKeys`, the server will always grant the client request if presented.

5.3 Extended Master Secret

The “extended master secret” as specified in RFC 7627 is an important security feature for TLS implementations that use session resumption. The extended master secret feature associates the internal TLS master secret directly to the connection context to prevent man-in-the-middle attacks during session resumption. One such attack is a synchronizing triple handshake as described in “Triple Handshakes and Cookie Cutters: Breaking and Fixing Authentication over TLS”.

This feature is always enabled by default in both MatrixSSL clients and servers. The `extendedMasterSecret` option may be used to REQUIRE the use of the extension by the peer. The peer agreement mechanism is the CLIENT_HELLO and SERVER_HELLO “extended_master_secret” extension.

Clients

A client will always include the `extended_master_secret` extension when creating the CLIENT_HELLO message. If the server replies with an `extended_master_secret`, the upgraded master secret generation will be used. If the server does not reply with an `extended_master_secret`, the standard master secret generation will be used for the connection.

A client MAY *require* that a server support the `extended_master_secret` feature by setting the `extendedMasterSecret` member of `sslSessOpts_t` to 1. If `extendedMasterSecret` is set, the client will send a fatal `handshake_failure` alert to the server if the `extended_master_secret` extension is not included in the SERVER_HELLO.

Servers

A server will always reply with the `extended_master_secret` extension if the client includes it in the CLIENT_HELLO message.

A server MAY *require* that a client support the `extended_master_secret` feature by setting the `extendedMasterSecret` member of `sslSessOpts_t` to 1. The `sslSessOpts_t` structure is passed to `matrixSslNewServerSession` when starting a TLS session. If `extendedMasterSecret` is set, the server will send a fatal `handshake_failure` alert to the client if the `extended_master_secret` extension is not included in the CLIENT_HELLO.

When creating the session resumption information (either the standard session table or the stateless session ticket) the server will flag whether the extended master secret was used for the initial connection. When a client attempts session resumption, the CLIENT_HELLO must include the `extended_master_secret` extension if it was used in the initial connection. Likewise, if the initial connection did not use the `extended_master_secret` the session resumption CLIENT_HELLO must also exclude that extension. If there is a mismatch, the server will not allow the session resumption and a full handshake will occur instead.

5.4 Maximum Fragment Length

The `maxFragLen` member controls the Maximum Fragment Length Negotiation of RFC 6066

Clients

Set the `maxFragLen` member to 512, 1024, 2048 or 4096 if the client would like to request a smaller TLS fragment length from the 16KB default for this session. The server is free to deny the request.

Servers

Servers may use the `maxFragLen` member to deny a client request to change the default. Set the value to -1 to deny the feature for this session.

5.5 Truncated HMAC

The `truncHmac` member controls the Truncated HMAC negotiation of RFC 6066

Clients

Set to the `truncHmac` member to `PS_TRUE` to request a TLS session with a 10 byte truncated HMAC feature. The server is free to deny the request.

Servers

Servers may use the `truncHmac` member to deny a client request to use truncated HMAC. Set the value to -1 to deny the feature for this session.

5.6 Elliptic Curve Specification

The `ecFlags` member controls which set of available Elliptic Curves the client or server is willing to support for the TLS session

NOTE: The choice of curves is also tied to the key material that is loaded in the client. For example, if a client has loaded a Certificate Authority with a SECP192R1 public key and that curve is not specified in a custom `ecFlags` list, the session initialization will fail.

Clients

Populate the `ecFlags` mask using the set of `SSL_OPT_<NAME>` curve defines to specify a specific set of supported curves for this session. When populated, the strongest curves will be presented first in the list of supported curves. If not populated, the default will send all curves that are compiled into the library and will be presented in a weakest-first order.

Servers

Populate the `ecFlags` mask using the set of `SSL_OPT_<NAME>` curve defines to specify a specific set of supported curves for this session. When populated, the server will ensure the client is sending at least one curve that matches the custom list. If not populated, the default will match against all curves that are compiled into the library.

5.7 Trusted CA Indication

The `trustedCAindication` member controls whether the client will send its list of loaded CA files to the server in the `CLIENT_HELLO` message. This feature enables TLS peers to know whether they share the correct key material early in the handshake.

Clients

Set the `trustedCAindication` member to 1 to enable the feature. The MatrixSSL library uses the `cert_sha1_hash` option when presenting the CA list to the server.

5.8 OCSP Revocation

The Online Certificate Status Protocol (OCSP) is an alternative to the Certificate Revocation List (CRL) mechanism for performing certificate revocation tests on server keys. TLS integrates with OCSP in a mechanism known as “OCSP stapling”. This feature allows the client to request that the server provide a time-stamped OCSP response when presenting the X.509 certificate during the TLS handshake. The primary goal for this scheme is to allow resource constrained clients to perform certificate revocation tests without having to communicate with an OCSP Responder themselves.

The `USE_OCSP` define in `cryptoConfig.h` must be enabled for this feature to be available.

Clients

A client application can request OCSP stapling by setting the `OCSPstapling` member of the `sslSessOpts_t` structure. This flag will trigger the creation of the Certificate Status Request extension in the `CLIENT_HELLO` message. The resulting `status_request` extension will not specify any responder identification hints or request extensions. This indicates that the server is free to provide whatever OCSP response is relevant to its identity certificate.

In order to validate the signature of provided OCSP response, the client will have to hold the Certificate Authority of the OCSP responder. There are two places the MatrixSSL library will search for this CA file. The first place the library will look is in the CA material that is loaded in the standard `matrixSslLoadRsaKeys` (or `matrixSslLoadEcKeys`) API. If the CA file is not located in this pre-loaded key material, the library will next look to the server's certificate chain. In practice, many TLS servers that implement OCSP stapling will create a certificate chain in which the parent certificate of the primary identity certificate also acts as the OCSP responder. At the time of the OCSP validation test, the `CERTIFICATE` message will have already been processed and validated. If the client has confirmed the server to have a valid chain of trust, it is appropriate to trust that same certificate chain to provide the OCSP response. If the client is unable to locate the CA file for the public key of the OCSP responder the handshake will fail.

In order to validate the time stamp of the OCSP response the client library will invoke the `checkOCSPtimestamp` function `x509.c`. The default time window for accepting an OCSP response is 1 week and can be changed using the `OCSP_VALID_TIME_WINDOW` define in `cryptolib.h`

The OCSP stapling specification does not have guidance on how a client should behave if a server does not provide a `CERTIFICATE_STATUS` message when requested. The `USE_OCSP_MUST_STAPLE` define is included to allow the client application to require that the server provide the message. If `USE_OCSP_MUST_STAPLE` is enabled and the client has requested `CERTIFICATE_STATUS`, the handshake will abort if the server does not provide one.

Servers

Servers do not make use of the `OCSPstapling` member of `sslSessOpts_t`. Instead, a server application wishing to support OCSP stapling must keep an updated OSCP response loaded into the key material by calling `matrixSslLoadOCSPResponse`. This function takes a fully formed `OCSPResponse` ASN.1 buffer and loads it into the provided `sslKeys_t` structure. When a new OSCP response is fetched, the same `matrixSslLoadOCSPResponse` API can be called to update the `sslKeys_t` structure.

When a client sends the `status_request` extension the server will look to see if an OCSP response is available in the `sslKeys_t` structure and reply with a `status_request` extension and the `CERTIFICATE_STATUS` message that contains the OCSP response.

5.9 User Defined Opaque TLS Session Pointer

The `userPtr` member of the `ssl_t` structure may optionally be assigned as part of the session creation process by assigning the `userPtr` member of the session options. This is an opaque, application-specific context to enable implementation to associate custom information with an SSL session. This context may come in handy during the certificate callback, for example. It is not necessary to assign a `userPtr` member at session creation time if the opaque data is not yet known. A user may set, change, or remove the `ssl->userPtr` member any time during the lifecycle of the session once it is created. The value will never be referenced inside the MatrixSSL library.

5.10 User Defined Opaque Memory Allocation Pointer

The `memAllocPtr` member is a customization aid for integrators that are implementing their own memory allocation routines. This value will be passed to each `psOpenPool` call as the final `void *userPtr` parameter for each internal invocation in the MatrixSSL library that is related to this session. This will enable the user to associate custom data with a `psPool_t` context so that each memory allocation and free can be associated with a specific TLS session.

To implement a custom memory allocation mechanism, the customer must define `USE_MATRIX_MEMORY_MANAGEMENT` and implement `psOpenPool`, `psMalloc`, `psFree`, `psRealloc`, and `psClosePool`. A custom `psPool_t` structure will also be created. This `memAllocPtr` will be passed to `psOpenPool` where the implementation can use it to create a context to the `psPool_t` output. The `psPool_t` is input to the `psMalloc` and `psFree` routines.

For more information, see the MatrixSSL Deterministic Memory document or contact Inside Secure support.

5.11 User Defined TLS Buffer Memory Pool

The `bufferPool` pointer only applies to integrators that are using the MatrixSSL deterministic memory feature (`USE_MATRIX_MEMORY_MANAGEMENT` enabled). The `ssl_t` structure members, `inbuf` and `outbuf`, do not typically reside within a memory pool. If `bufferPool` is populated this pool will be used for the memory management of these members. These are the structure members that hold the incoming and outgoing TLS data during the handshake and during application data exchange. The allocation for these buffers using `psMalloc` and `psRealloc` are done under the `NULL` pool by default, which results in a standard platform `malloc` and `realloc` call. If an implementation requires that all data must be stored in a pool or must be associated with the SSL session, this `bufferPool` must be populated with a memory pool that was created by a call to `psOpenPool`. The user must control the lifecycle of this buffer pool by manually closing the pool with `psClosePool` when the session is closed.

NOTE: The size of the pool should be large enough to hold two 18KB data buffers. This value of 36KB will enable the maximum SSL record sizes to be used. If the maximum fragment length feature is in use it is possible this value could be decreased.

5.12 Session Options Summary Table

	Client	Server
int32 versionFlag	Optional SSL protocol version. Choices are <code>SSL_FLAGS_SSLV3</code> , <code>SSL_FLAGS_TLS_1_0</code> , <code>SSL_FLAGS_TLS_1_1</code> , or <code>SSL_FLAGS_TLS_1_2</code> . Must augment flags value with <code>SSL_FLAGS_DTLS</code> for MatrixDTLS product.	Optional SSL protocol version. Choices are <code>SSL_FLAGS_SSLV3</code> , <code>SSL_FLAGS_TLS_1_0</code> , <code>SSL_FLAGS_TLS_1_1</code> , or <code>SSL_FLAGS_TLS_1_2</code> . Must augment flags value with <code>SSL_FLAGS_DTLS</code> for MatrixDTLS product.
short ticketResumption	Set to 1 to enable stateless ticket session resumption. The <code>USE_STATELESS_SESSION_TICKETS</code> define must be enabled to support the feature. Standard session resumption will be used otherwise.	N/A (Server will support stateless session resumption if the <code>USE_STATELESS_SESSION_TICKETS</code> define is enabled)
short extendedMasterSecret	On by default. Set to 1 to require the use of <code>extended_master_secret</code>	On by default. Set to 1 to require the use of <code>extended_master_secret</code>
short maxFragLen	Set to 512, 1024, 2048 or 4096 if desired. The default of 0 will result in the maximum length of 16KB per TLS specifications.	Set to -1 to deny a client request to change the maximum fragment length for the session.
short truncHmac	<code>PS_TRUE</code> if wish to enable and send the <code>CLIENT_HELLO</code> extension to request the feature from the server	Set to -1 to deny a client request to use a truncated HMAC for the session.
int32 ecFlags	A flag mask created from the following supported EC curves: <code>SSL_OPT_SECP192R1</code> <code>SSL_OPT_SECP224R1</code> <code>SSL_OPT_SECP256R1</code> <code>SSL_OPT_SECP384R1</code> <code>SSL_OPT_SECP521R1</code> <code>SSL_OPT_BRAIN224R1</code>	A flag mask created from the following supported EC curves: <code>SSL_OPT_SECP192R1</code> <code>SSL_OPT_SECP224R1</code> <code>SSL_OPT_SECP256R1</code> <code>SSL_OPT_SECP384R1</code> <code>SSL_OPT_SECP521R1</code> <code>SSL_OPT_BRAIN224R1</code>

	SSL_OPT_BRAIN256R1 SSL_OPT_BRAIN384R1 SSL_OPT_BRAIN512R1	SSL_OPT_BRAIN256R1 SSL_OPT_BRAIN384R1 SSL_OPT_BRAIN512R1
void *userPtr	Assign a custom opaque pointer that will be occupy the <code>userPtr</code> member of the <code>ssl_t</code> session structure.	Assign a custom opaque pointer that will be occupy the <code>userPtr</code> member of the <code>ssl_t</code> session structure.
void *memAllocPtr	Becomes the <code>userPtr</code> parameter for each call to <code>psOpenPool</code> for this session	Becomes the <code>userPtr</code> parameter for each call to <code>psOpenPool</code> for this session
psPool_t *bufferPool	A user provided memory pool for the allocations of the <code>outbuf</code> and <code>inbuf</code> data buffers for the TLS session.	A user provided memory pool for the allocations of the <code>outbuf</code> and <code>inbuf</code> data buffers for the TLS session.

Table 1 - Session Options

6 THE CERTIFICATE VALIDATION CALLBACK FUNCTION

This section describes the `certValidator` parameter of the `matrixSslNewClientSession` and `matrixSslNewServerSession` functions.

6.1 Application Layer Certificate Acceptance

This callback offers a mid-handshake opportunity for a user to intervene in the authentication process. After receiving the CERTIFICATE handshake message the callback will be invoked and the user can determine whether the handshake should continue or whether a fatal alert should be sent and the handshake terminated. The callback will be invoked with the certificate material sent by the peer as well as the status of the X.509 and public-key (RSA or ECC) authentication performed internally by the MatrixSSL library.

The registered callback function must have the following prototype:

```
int32 certValidator(ssl_t *ssl, psX509Cert_t *certInfo, int32 alert);
```

The `ssl` parameter is the session context and must be treated as read-only.

The incoming `certInfo` parameter is the incoming `psX509Cert_t` structure containing information about the peer certificate or certificate chain. It is the certificate information in this structure that an application will generally wish to examine. This certificate information is read-only from the perspective of the validating callback function. The structure members are specified in the **psX509Cert_t Structure** section of this document. The most important member of the structure for the purposes of the certificate callback is the `authStatus` member and is detailed below.

If this authentication is operating on a certificate chain, the `next` member of the `psX509Cert_t` structure will link to the next certificate. The `next` member should be the parent (or issuer) of the current certificate.

The incoming `alert` parameter will quickly indicate whether or not the certificate passed the internal X.509 and RSA (or other public-key authentication) authentication checks. The alert member will be `MATRIXSSL_SUCCESS` (0) if the certificate chain was valid and the issuing CA was found and could successfully authenticate the peer's certificate.

If `alert` is `> 0` there is at least one authentication error in the server's certificate chain. The `alert` value is a translation of an authentication problem to a TLS alert type. The TLS alert identification will be set to one of the following based on the type of authentication error that was hit.

Value for incoming alert parameter	Description
0	Authentication success. The certificate chain received from the peer was valid and the issuing CA file was found and successfully identified as the issuer.
SSL_ALERT_BAD_CERTIFICATE	Authentication failure. This alert is an indication that the certificate chain from the peer did not self-validate OR the correctly named CA was found but the mathematical signature test did not pass. It is highly recommended that the user callback adhere to the alert and terminate the handshake.
SSL_ALERT_UNKNOWN_CA	Authentication failure. This alert is an indication that the certificate chain from the peer is valid but the issuing CA could not be found. It is highly recommended that the user callback adhere to the alert and terminate the handshake.
SSL_ALERT_ILLEGAL_PARAMETER	Authentication failure. This alert is an indication that the certificate chain from the peer correctly self-validated and the mathematical authentication against a CA was successful, however, an X.509 v3 certificate extension violation was detected in the CA. This return code, then, is meant to indicate to the user that the CA they have loaded has a problem (as opposed to the peer having a bad certificate). The user callback SHOULD adhere to the alert and terminate the handshake and fix whatever problem their CA has.

SSL_ALERT_CERTIFICATE_REVOKED	Authentication failure. The certificate has been checked against a user provided Certificate Revocation List and determined to be untrusted. It is highly recommended that the user callback adhere to the alert and terminate the handshake.
SSL_ALERT_CERTIFICATE_EXPIRED	Authentication failure. One of the certificates in the chain is no longer valid in time. The notBefore or notAfter fields in the certificate do not fit in the current time and date window.
SSL_ALERT_CERTIFICATE_UNKNOWN	Authentication failure. The end-entity certificate name did not match the string that was passed to <code>expectedName</code> in <code>matrixSslNewClientSession</code> .

Table 2 - Certificate Callback Incoming "alert" Values

The `alert` value represents only **the first authentication error of a certificate chain**. In cases where a server only has a single certificate, the alert value is always an indication of a problem on that single certificate. However, if a server is using a certificate chain, the certificate callback might need to walk the chain to find more specific problems than what the `alert` is reporting.

For example, if a use-case has determined that "minor" alerts such as `SSL_ALERT_CERTIFICATE_EXPIRED` can be ignored, it is not sufficient to simply return 0 from the callback if the alert is set to this value. It could be the case that this expiration occurred on the child-most certificate and the parent-most certificate has a more serious authentication problem such as an invalid signature or that the CA file to authenticate it was never found at all.

The individual certificates in the `certInfo` parameter will indicate their own authentication status through the `authStatus` member of the `psX509Cert_t` structure. This is particularly important if certificate chains are being used and the user would like to identify a specific certificate that did not internally authenticate. The callback can walk the subject certificate chain using the `next` member of the structure to find the `authStatus` members that are not set to `PS_CERT_AUTH_PASS`.

Values for <code>authStatus</code> member of certificate structure	Description
<code>PS_CERT_AUTH_PASS</code>	The certificate was authenticated fully
<code>PS_CERT_AUTH_FAIL_BC</code>	BasicConstraints failure. The issuing certificate did not have CA permissions to issue certificates
<code>PS_CERT_AUTH_FAIL_DN</code>	DistinguishedName failure. The issuing CA did not match the name that the subject identified as its issuer.
<code>PS_CERT_AUTH_FAIL_REVOKED</code>	A CRL has reported the certificate has been revoked
<code>PS_CERT_AUTH_FAIL_SIG</code>	The mathematical signature operation failed.
<code>PS_CERT_AUTH_FAIL_AUTHKEY</code>	The authorityKeyId extension of the subject cert does not match the subjectKeyId of the issuing certificate.
<code>PS_CERT_AUTH_FAIL_PATH_LEN</code>	The certificate chain is longer than allowed as specified by the <code>pathLen</code> field in the <code>basisConstraints</code> extension.
<code>PS_CERT_AUTH_FAIL_EXTENSION</code>	All the above tests passed but there was a violation of the x.509 extension rules. The <code>authFailReason</code> member can be examined to find the specific extension that failed.

Regardless of the internal authentication tests and `alert` value, the callback function will ultimately determine whether or not to continue the SSL handshake through the return value it chooses.

Return Value from the Certificate Callback Function	Description
0	Continue handshake. The user callback is indicating that it accepts the certificate material. If an authentication alert was internally set, it will be ignored and cleared.
> 0	Fail the handshake; return a fatal alert , and close connection with peer. The positive value is the SSL alert ID as defined in <code>matrixssl.h</code> . The incoming alert parameter may be one of <code>SSL_ALERT_BAD_CERTIFICATE</code> , <code>SSL_ALERT_ILLEGAL_PARAMETER</code> ,

	SSL_ALERT_CERTIFICATE_UNKNOWN, SSL_ALERT_CERTIFICATE_REVOKED, SSL_ALERT_CERTIFICATE_EXPIRED or SSL_ALERT_UNKNOWN_CA and it is recommended those be passed through in the return code. Other alert codes can be found in the table below.
< 0	Fail the handshake; issue a fatal INTERNAL_ERROR alert, and close connection with peer. This return code should be used if the user callback code itself encounters an unrecoverable error.
SSL_ALLOW_ANON_CONNECTION	Continue handshake. The user callback is acknowledging that the certificate has not been authenticated but it is being allowed to continue. See the section below for more information.

Table 3 - Certificate Callback Return Value Ranges

SSL Alerts for Failed Authentication

The MatrixSSL library will perform the following tests to authenticate a certificate:

1. If the X.509 certificate is not version 3, the certificate parse will fail and SSL_ALERT_BAD_CERTIFICATE will be sent to the peer. The certificate callback will not be invoked in this parse failure case.
2. The X.509 basicConstraints extension will be checked to ensure the CA is truly a CA
3. The DistinguishedName issuerName will be matched against the subject subjectName.
4. The revocation status (if feature is enabled) is checked
5. The mathematical public key signature validation operation is performed.
6. The X.509 extension tests on KeyUsage and SubjectKeyId/AuthKeyId are performed
7. The path length of the certificate chain is tested against the pathLen member of the basicConstraints extension
8. The certificate callback can be used to perform additional authentication tests and return the alert status based on custom tests. The following table shows the possible options that may be returned.

Fatal Alert Return Values for Certification Callback	Description
SSL_ALERT_BAD_CERTIFICATE	A certificate was corrupt, contained signatures that did not verify correctly, etc. This value could already be the incoming alert value.
SSL_ALERT_UNKNOWN_CA	A valid certificate chain or partial chain was received, but the certificate was not accepted because the CA certificate could not be located or couldn't be matched with a known, trusted CA. This value could already be the incoming alert value.
SSL_ALERT_CERTIFICATE_REVOKED	The certificate was revoked by its signer. This value could already be the incoming alert value.
SSL_ALERT_CERTIFICATE_EXPIRED	A certificate has expired or is not currently valid based on the notBefore and notAfter values.
SSL_ALERT_CERTIFICATE_UNKNOWN	Some other (unspecified) issue arose in processing the certificate, rendering it unacceptable.
SSL_ALERT_ACCESS_DENIED	A valid certificate was received, but when access control was applied, the sender decided not to proceed with negotiation.
SSL_ALERT_UNSUPPORTED_CERTIFICATE	A certificate was of an unsupported type.
SSL_ALERT_ILLEGAL_PARAMETER	MatrixSSL uses this alert to distinguish an X.509 extension violation in the CA file (as opposed to an extension violation in the received certificate chain)

Table 4 - Certificate Callback SSL_ALERT Return Values

Anonymous Connections

The callback may also choose to return `SSL_ALLOW_ANON_CONNECTION` if the user wishes to continue a connection despite a `PS_CERT_AUTH_FAIL_X` indication on any of the certificates. If this return value is used, the handshake will continue and will result in a secure (data encryption) but unauthenticated SSL connection. If this return value is used, the `matrixSslGetAnonStatus` function may be used during the lifetime of the connection to verify the status.

It is important to note that this anonymous connection mechanism is not related to anonymous cipher suites. The certificate validation callback is only invoked for cipher suites that utilize public key authentication. Therefore, it is not advised to allow anonymous connections using this mechanism. If anonymous connections are desired, it is recommended that an anonymous cipher suite be used instead.

Server (Client-Authentication)

In client authentication handshakes the server will need to implement the callback function as well.

By default, the MatrixSSL server will immediately terminate the handshake if the client replies to the server `CERTIFICATE_REQUEST` message with an empty `CERTIFICATE` message. If the server wishes to potentially continue the connection, the compile time define

`SERVER_WILL_ACCEPT_EMPTY_CLIENT_CERT_MSG` in *matrixssl/Config.h* must be enabled. If enabled, the certificate callback function will be invoked with a `NULL` `certInfo` parameter and an alert status of `SSL_ALERT_BAD_CERTIFICATE`. If the user callback determines the handshake can continue without client-authentication the handshake is effectively “downgraded” on the fly to a standard handshake.

6.2 psX509Cert_t Structure

Parsed information from X.509 certificates is stored in the `psX509Cert_t` structure, defined in `crypto/keyformat/x509.h`. The X.509 format is somewhat complex, so we document the most important fields here.

This data type is most important in the context of the session creation APIs in which the application registers a custom function to be invoked during the SSL handshake to validate the peer certificate. This registered callback function may wish to perform custom checks on the individual members of the `psX509Cert_t` structures that are passed in.

version	X.509 version. MatrixSSL supports v3 certificates only. 0 = v1, 1 = v2, 2 = v3
serialNumber	Serial number issued to this certificate. Some certificates insert non-integer values for this member
serialNumberLen	Byte length of <code>serialNumber</code>
issuer	Distinguished Name of the CA that issued this certificate. See <code>x509DNAttributes_t</code>
subject	Distinguished Name of this certificate. See <code>x509DNAttributes_t</code>
notBeforeTimeType notAfterTimeType	Format specification for the <code>notBefore</code> and <code>notAfter</code> members of this structure. Either <code>ASN_UTCTIME</code> or <code>ASN_GENERALIZEDTIME</code>
notBefore	NULL terminated <code>UTCTime</code> or <code>GeneralizedTime</code> indicating the valid start date for the certificate
notAfter	NULL terminated <code>UTCTime</code> or <code>GeneralizedTime</code> indicating the valid end date for the certificate
publicKey	The public key of this certificate. See <code>psPubKey_t</code>

pubKeyAlgorithm	The algorithm identifier for the public key encryption mechanism this certificate is using. Either <code>OID_RSA_KEY_ALG</code> or <code>OID_ECDSA_KEY_ALG</code>
certAlgorithm	The algorithm identifier the issuing CA used to sign this certificate. Supported values are found in the <code>/* Signature algorithms */</code> section of the <i>cryptolib.h</i> file. This value must match <code>sigAlgorithm</code> and that is tested internally during certificate parsing.
sigAlgorithm	The verification of the signature algorithm the issuing CA used for this certificate. The <code>/* Signature algorithms */</code> section of the <i>cryptolib.h</i> file defines the possible values. This value must match <code>certAlgorithm</code> and that is tested during certificate parsing.
signature	The full CA-generated digital signature for this certificate that binds the subject to the CA private key
signatureLen	The byte length of signature
sigHash	The digest hash portion of the signature used internally for public key authentication
uniqueIssuerId	Optional certificate field to handle possible reuse of the issuer name. See section 4.1.2.8 of RFC 3280 for more information.
uniqueIssuerIdLen	Byte length of <code>uniqueIssuerId</code>
uniqueSubjectId	Optional certificate field to handle possible reuse of the subject name. See section 4.1.2.8 of RFC 3280 for more information.
uniqueSubjectIdLen	Byte length of <code>uniqueSubjectId</code>
extensions	The X.509 certificate extensions for this certificate. See <code>x509v3extensions_t</code>
authStatus	<p>This flag is set on subject certificates when <code>psX509AuthenticateCert</code> is called. The value indicates the public key authentication status of whether the issuer certificate is the CA of the subject certificate. MatrixSSL calls this internally before the user's custom certificate verification callback is invoked so the user can examine it. The value may be;</p> <p><code>PS_FALSE</code> = untested (chain validation stops on first certificate to fail so this should only be set on certificates beyond the one that did not pass)</p> <p><code>PS_CERT_AUTH_PASS</code> = successfully authenticated</p> <p><code>PS_CERT_AUTH_FAIL_BC</code> = failed authentication because the issuing certificate did not have CA permissions</p> <p><code>PS_CERT_AUTH_FAIL_DN</code> = failed authentication because the Distinguished Name of the issuer did not match the DN of the issuer</p> <p><code>PS_CERT_AUTH_FAIL_SIG</code> = failed authentication because the public key signature did not validate</p> <p><code>PS_CERT_AUTH_FAIL_EXTENSION</code> = failed authentication because an x.509 extension parameter was violated</p>
authFailFlags	<p>If <code>authStatus</code> is <code>PS_CERT_AUTH_FAIL_EXTENSION</code> this flag will further specify the problem(s):</p> <p><code>PS_CERT_AUTH_FAIL_KEY_USAGE_FLAG</code> – KeyUsage did not specify certificate signing</p> <p><code>PS_CERT_AUTH_FAIL_EKU_FLAG</code> – The ExtendedKeyUsage extension exists but did not specify TLS usage</p> <p><code>PS_CERT_AUTH_FAIL_SUBJECT_FLAG</code> – The Server Name Indication extension could not be matched</p> <p><code>PS_CERT_AUTH_FAIL_DATE_FLAG</code> – The certificate is expired (or not yet valid)</p>
unparsedBin	The raw ASN.1 binary stream of this certificate (if applicable).
binLen	Byte length of <code>unparsedBin</code>

next	Pointer to the next <code>psX509Cert_t</code> if this is a chain of certificates
------	--

Table 5 - Important `psX509_t` Structure Members

The DistinguishedName X.509 attribute is the plaintext description of the certificate owner and issuer.

country state locality organization orgUnit commonName	The self-identifying collection of supported string attributes that comprise the Distinguished Name. Distinguished Names are used to identify the subject and issuer of an X.509 certificate.
countryType stateType localityType organizationType orgUnitType commonNameType	These members specify the ASN.1 string type for their corresponding <code>char*</code> string members (ie. <code>countryType</code> for country). Types can be found in the <i>crypto/keyformat/asn1.h</i> header file <code>ASN_UTF8STRING</code> (8-bit chars) == 12 <code>ASN_PRINTABLESTRING</code> (8-bit chars) == 19 <code>ASN_IA5STRING</code> (8-bit chars) == 22 <code>ASN_BMPSTRING</code> (16-bit chars) == 30
countryLen stateLen localityLen organizationLen orgUnitLen commonNameLen	These members specify the byte length for their corresponding <code>char*</code> string members. The length includes two terminating NULL bytes.
hash	A digest representation of the above attributes used for easy comparisons of DN
dnenc	The unparsed ASN.1 stream of the DN (if applicable)
dnencLen	Byte length of <code>dnenc</code>

Table 6 - `x509DNAttributes_t` Structure Members

X.509 extensions are held in the `extensions` member.

bc	The critical Basic Constraints extension. See <code>x509extBasicConstraints_t</code>
san	The Subject Alternative Name extension. This extension is used to associate additional identities with the certificate subject. Common alternate identities include email addresses and IP addresses. See <code>x509GeneralName_t</code>
keyUsage	The BIT STRING value of KeyUsage. For the purposes of SSL, the only interesting bit in the encoding should be the 5 th bit (of zero based) of the 2 nd byte that identifies <code>keyCertSign</code> .
keyUsageLen	The length of the entire BIT STRING captured in the above member.
extendedKeyUsage	
extendedKeyUsageCritical	
nameConstraints	
certificatePolicy	
policyConstraints	
policyMappings	

authorityInfoAccess	
sk	
ak	

Table 7 - x509v3extensions_t Structure Members

x509extBasicConstraints_t Members

ca	Indicates whether this certificate is a Certificate Authority. Possible values are: CA_TRUE (CA), CA_FALSE (not a CA), CA_UNDEFINED (basic constraints extension is not present in the certificate).
pathLenConstraint	If ca is CA_TRUE, this member indicates the maximum length that a certificate chain may extend beyond this CA.

x509GeneralName_t Members

id	Integer identifier of the name type. id to name mappings 0 = "other", 1 = "email", 2 = "DNS", 3 = "x400Address", 4 = "directoryName", 5 = "ediPartyName", 6 = "URI", 7 = "iPAddress", 8 = "registeredID", x = "unknown"
name	String identifier for the name type. Possible values are the quoted names from the list above.
data	The data value for the alternate name
dataLen	Byte length of data
next	The next x509GeneralName_t alternate name in this extension.

7 QUICK REFERENCE

API	Description	API Dependencies
matrixSslOpen matrixSslClose	One time initialization and clean up for MatrixSSL	
matrixSslNewKeys matrixSslDeleteKeys matrixSslLoadRsaKeys	Key management functions	matrixSslNewKeys must be called prior to calling matrixSslLoadRsaKeys
matrixSslNewClientSession matrixSslNewServerSession matrixSslDeleteSession	Respective session initialization and common session deletion	
matrixSslGetOutdata	Retrieve encoded data that is ready to be sent out over the wire to the peer	Must be followed by a call to matrixSslSentData
matrixSslReceivedData	Any data received from the peer must be passed to this function	An empty data buffer must have been retrieved by a prior call to matrixSslGetReadbuf
matrixSslProcessedData	Must be called each time the application is done processing plaintext data	Plaintext data will only be given to the application when the return code from matrixSslReceivedData or matrixSslProcessedData is MATRIXSSL_APP_DATA or MATRIXSSL_RECEIVED_ALERT
matrixSslGetWriteBuf matrixSslEncodeWriteBuf - OR - matrixSslEncodeToOutdata	Used for encoding plaintext application data after SSL handshake that will be sent to the peer	matrixSslGetWriteBuf must be called to get an empty buffer in which to copy plaintext. matrixSslEncodeWriteBuf must be called to do the actual encryption. Encrypted data must be retrieved with matrixSslGetOutdata

APPENDIX A - LIST OF TABLES

Table 1 - Session Options.....	53
Table 2 - Certificate Callback Incoming “alert” Values.....	55
Table 3 - Certificate Callback Return Value Ranges	56
Table 4 - Certificate Callback SSL_ALERT Return Values	56
Table 5 - Important psX509_t Structure Members.....	59
Table 6 - x509DNattributes_t Structure Members	59
Table 7 - x509v3extensions_t Structure Members	60