Talaria TWO uses mbed TLS library for the implementation of SSL/TLS. This component provides wrapper functions for the commonly used functionalities like connect, read, write and read with timeout. This is an effort to hide the complicacy of using discrete mbed TLS APIs to perform commonly used functionality like establishing connection.

**Note**: mbed TLS APIs are available for using directly without the need of using this module.

# Header file/s

Components/ssl\_wrap/inc/ssl\_wrap.h

# Data Structure Definitions

## ssl\_auth\_mode\_t

This enum defines the various authentication modes.

|  |  |
| --- | --- |
| ***SSL\_WRAP\_VERIFY\_NONE*** | Peer certificate is not checked (default on server. insecure on client) |
| ***SSL\_WRAP\_VERIFY\_OPTIONAL*** | Peer certificate is checked; however the handshake continues even if verification fails. mbedtls\_ssl\_get\_verify\_result() can be called after the handshake is complete |
| ***SSL\_WRAP\_VERIFY\_REQUIRED*** | Peer **must** present a valid certificate; handshake is aborted if verification fails (default on client) |

Table : ssl\_auth\_mode\_t - authentication modes

## ssl\_wrap\_cert\_t

This data structure is used to provide information about the certificate like CA cert, Client cert and Client Key.

|  |  |
| --- | --- |
| ***path*** | Not used currently. Path of the certificate in file system |
| ***buf*** | Pointer to buffer having the certificate |
| ***len*** | Length of the certificate/key present in the buf |

Table : ssl\_wrap\_cert\_t – parameters

## ssl\_wrap\_cfg\_t

This data structure is used to pass the parameters while opening an SSL connection with the remote server using ssl\_wrap\_connect API.

|  |  |
| --- | --- |
| ***ca\_cert*** | CA certificate information. This is a pointer to properly initialized ssl\_wrap\_cert\_t |
| ***client\_cert*** | Client certificate information. This is a pointer to properly initialized ssl\_wrap\_cert\_t |
| ***client\_key*** | Client key information. This is a pointer to properly initialized ssl\_wrap\_cert\_t |
| ***auth\_mode*** | Authentication mode as defined in ssl\_auth\_mode\_t |
| ***max\_frag\_len*** | Value will be >= MBEDTLS\_SSL\_MAX\_FRAG\_LEN\_512 and <= MBEDTLS\_SSL\_MAX\_FRAG\_LEN\_4096 |

Table : ssl\_wrap\_cfg\_t - parameters

### http\_client\_resp\_info\_t

This data structure is used to pass information about the data received from the server when HTTP GET is done using the http\_client\_get API.

|  |  |
| --- | --- |
| ***status\_code*** | HTTP response status code |
| ***resp\_hdrs*** | Response headers. Array of strings |
| ***resp\_body*** | Response body len |
| ***resp\_len*** | Resp len, currently available in the resp\_body |
| ***resp\_total\_len*** | Total length of the response body. If 0, no total length available before hand as the body may be sent using chunked or multipart encoding |
| ***more\_data*** | More data will be followed. The callback will be called again |

Table : http\_client\_resp\_info\_t - parameters

# API Reference

## ssl\_wrap\_connect

### Overview

This API is used to securely connect to remote server using SSL/TLS.

### Definition

|  |
| --- |
| ssl\_wrap\_handle\_t  ssl\_wrap\_connect(char \*host\_name, int port, ssl\_wrap\_cfg\_t \*cfg) |

### Parameters

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| *hostname* | DNS name or the IP address of the remote server |
| *port* | Port number to connect to |
| *cfg* | SSL configuration parameters required to make the SSL connection |

Table : ssl\_wrap\_connect – parameters

### Return

Success: Pointer to SSL wrap connection handle.

Error: NULL

## ssl\_wrap\_read

### Overview

This function is used to read data received over the SSL connection established using the ssl\_wrap\_connect API. This API blocks indefinitely for the data.

### Definition

|  |
| --- |
| int  ssl\_wrap\_read(ssl\_wrap\_handle\_t handle, unsigned char \*buf, int len) |

### Parameters

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| *handle* | Handle returned by ssl\_wrap\_connect |
| *buf* | Buffer to read data in to |
| *len* | Max length of the buffer |

Table : ssl\_wrap\_read - parameters

### Return

Success: >0. Number of bytes read.

Error: -1

## ssl\_wrap\_write

### Overview

This function is used to send data over the SSL connection established using the ssl\_wrap\_connect API.

### Definition

|  |
| --- |
| int  ssl\_wrap\_write (ssl\_wrap\_handle\_t handle, unsigned char \*buf, int len) |

### Parameters

|  |  |
| --- | --- |
| ***Parameters*** | **Description** |
| *handle* | Handle returned by ssl\_wrap\_connect |
| *buf* | Buffer having data to be sent |
| *len* | Length of data to be sent |

Table : ssl\_wrap\_write - parameters

### Return

Success: >=0. Number of bytes sent.

Error: -1

## ssl\_wrap\_read\_timeout

### Overview

This function is used to tread data received over the SSL connection established using the ssl\_wrap\_connect API. This is similar to ssl\_wrap\_read, the difference being, this API will return after a specified timeout.

### Definition

|  |
| --- |
| int  ssl\_wrap\_read\_timeout(ssl\_wrap\_handle\_t handle, unsigned char\* buf, int len,  int timeout\_ms) |

### Parameters

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| *handle* | Handle returned by ssl\_wrap\_connect |
| *buf* | Buffer to read data into |
| *len* | Max length of the buffer |
| *timeout* | Timeout in seconds after which API will return with an error if no data is received from the server |

Table : ssl\_wrap\_read\_timeout - parameters

### Return

Success: >0. Number of bytes read.

Error: -1

## ssl\_wrap\_disconnect

### Overview

This function is used to disconnect the SSL connection established using the ssl\_wrap\_connect API.

### Definition

|  |
| --- |
| void  ssl\_wrap\_disconnect(ssl\_wrap\_handle\_t handle) |

### Parameters

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| *handle* | Handle returned by ssl\_wrap\_connect |

### Return

None.

# Application Example

For the example code, refer: *components/http\_client*, *components/mqtt* and other similar directories.