

Columbitech Mobile VPN

Embedded SDK



COLUMBITECH

Columbitech Embedded SDK is a software library, which enables device manufacturers to create secure VPN clients for any wireless device on any standard or non standard operating system or CPU. The SDK adds session persistence and FIPS140-2 validated cryptographic protection to any device, communicating over Wi-Fi, 3G, 4G, or satellite networks.

The library is written in ANSI C, which makes it portable to any platform with a C-compiler. It is suitable for devices with limited memory and processing capabilities. The embedded client is composed of the following modules, which can be combined to form a suitable mobile VPN client solution:

- *eClient – Embedded Client Module*
The main module that initiates and controls the other modules.
- *eWTLS – Embedded Wireless TLS Module*
Includes the security layer responsible for encryption, decrypting, integrity check, certificate validation etc. This module is mandatory.
- *eWVPN – Embedded Wireless VPN Module*
Handles the internal WVPN-protocol, which controls user authentication and performs data compression. This module is mandatory.
- *eConfig – Embedded Configuration Module*
Enables easy configuration of the client using a standard text file format. This module is optional and can be replaced by any customer made configuration.
- *eTRUDP – Embedded Tiny Reliable UDP Module*
Makes it possible for small devices to use a reliable transport protocol that can be used over UDP. This module is normally used when it is not possible to use TCP as transport layer. The module is optional.
- *eCrypt – Embedded Cryptographic Module*
Stand alone library containing security algorithms such as AES symmetric encryption, RSA for asymmetric encryption and SHA-1 for secure hashing. The module is written in both optimized C and assembler code. It is optional and designed to make it easy to replace one or more algorithms with external implementations.

Specification

- Executes on 16 and 32-bits processor architectures.
- Available in assembler optimized versions for certain processors, such as Intel 8086/8080 and Intel Pentium.
- Is delivered as a standard C API with object libraries for the most common platforms.
- Uses only static memory, no dynamic memory allocation is needed.
- Requires minimal amount of memory – normally less than 64 Kbytes.
- FIPS 140-2 validated.
- Supports the Datagram Transport Layer Security (DTLS) protocol.

More information

For availability and pricing details, please call +1 866 855 1874 (North America) or +46 8 556 08 100 (Sweden) or e-mail info@columbitech.com. Visit www.columbitech.com for more information.