Cypherbridge® Systems uSSH™ SDK

Cypherbridge®
Trusted, Safe and Secure

Overview

Portable ANSI C SSH SDK for interactive shell, secure file transfer, and tunneled TCP/IP security layer.

Implement secure interactive shell and SSH tunneled application channel using the uSSH SDK. Secure telnet replacement is just the beginning. uSSH provides a flexible TCP/IP security layer for existing and new applications. The platform kit integrates with the system OS and TCP/IP. Network interfaces include Ethernet, WiFi, and LTE.

The uSSH SDK solution includes off-line utilities to manage user accounts and host keys. Build options include configurable cipher suites using the fully integrated compact math and crypto library.

uSSH can be compiled for a wide range of platforms and is integrated with leading RTOS TCP and toolchains including Keil, IAR GCC Eclipse.

Interactive Shell Application

uSSH provides a secure interactive telnet replacement with shell communications encrypted in the SSH secure tunnel

The interactive shell session is initiated using a desktop command line or GUI SSH terminal client such as openSSH, teraterm, or putty, connecting with the uSSH Server.

AUTHN. uSSH supports password or public key authentication. The username and password are sent over the encrypted channel to protect it against man-in-middle attack. The authenticated session is dispatched to the embedded shell

The shell uses a character or line-oriented message interface to interact with the user. Application commands can be added to the extensible shell.

AUTHZ. uSSH implements access levels on a per-command basis, to control access to system monitoring and administrator level configuration operations.

Embedded Client

uSSH supports embedded client for connection to peer server. This can be used for device-to-desktop, or M2M.

General Purpose Secure Tunnel

uSSH can be used for a general-purpose security tunnel using the SSH exec protocol. The exec request is processed by the uSSH command dispatcher and handed off to the application task that communicates with the client. The task can be executed in-line with the uSSH command handler, or in an RTOS service task or thread.

Secure File Transfer

SFTP and SCP Secure Copy options can be used to transfer files to and from the device. The uSSH platform kit interfaces to the file system with support for POSIX and embedded file systems, handling directory and file operations.

Extras

uSSH SDK extras include host key fingerprint generation and randomart image, for GUI based QR code and custom identification system features.

Features

- ✓ *IETF Standards based SSH 2.0 interoperates with GUI and command line SSH clients*
- ✓ *Flexible command dispatch with built-in starter shell.*
- ✓ *AUTHN password or public key*
- ✓ *AUTHZ multiple access control levels*
- ✓ *Telnet replacement using flexible secure channel API interface to application menus*
- ✓ *Configurable ECDSA and RSA host keys with offline key generator utility*
- ✓ *Configurable crypto includes ECDH, SuiteB AES128-256 CTR SHA256-SHA512 CHACHAPOLY1305*
- ✓ *Portable ANSI-C small RAM and ROM footprint with platform kit interface to RTOS and TCP/IP stack*

Secure File Transfer

- ✓ *SFTP client and server supports FileZilla, WinSCP, pUTTY pSFTP OpenSSH*
- ✓ *SCP client and server*

File System Interface

- ✓ *Interface to removable or block file media*
- ✓ *QSPI SDCard RAM*
- ✓ *Directory and File Operations*

For Pricing and Availability Contact:

Cypherbridge Systems LLC
7040 Avenida Encinas #104211 Carlsbad, CA 92011
www.cypherbridge.com
sales@cypherbridge.com
Tel: +1 (760) 814-1575

About Cypherbridge Systems:

Established in 2005, delivering a broad range of secure connectivity protocols and solutions including

- *IoT Device SDKs and Toolkits*
- *Product and System Integration*
- *Full Stack Cloud Computing*

CSL-uSSHv5-220930