



Key Points

- Secure webpages
- Secure data communications
- Small footprint
- SSL Key sizes from 128 to 1024 bits
- SSH key sizes from 512 to 4096 bits
- World-class technical support
- Customize to suit any application with low-cost development kit

NetBurner Embedded SSL / SSH Security Suite

Overview

The NetBurner SSH & SSL Security Suite is a small footprint security solution for embedded network devices. This package enables data encryption to protect from unauthorized device monitoring, control, or configuration.

- SSL is a cryptographic protocol that provides security and ensures data integrity for transmissions made over a TCP/IP network. It is primarily used to enable devices to serve secure webpages (HTTPS) over a local network or the Internet.
- SSH enables data to be exchanged between two network devices over a secure channel—it's a secure replacement for TELNET and other insecure remote shells.

SSL (Secure Sockets Layer)

The NetBurner SSL implementation was written from the ground up to provide high performance and a small memory footprint of approximately 90K bytes. The SSL module is integrated with the NetBurner TCP/IP stack and web server, enabling you to add secure web pages to your product with just a few function calls. Unlike 8-bit and 16-bit micro-controllers, the 32-bit NetBurner processor platforms can easily handle the demands of connecting and transmitting data using SSL. Authentication is achieved by using public key certificates, which require a functioning PKI (public-key infrastructure). You can setup a local trusted PKI or use one of the many trusted certificate authorities on Internet such as Thawte, or VeriSign.

SSH (Secure Shell)

SSH enables secure data exchange between embedded network devices on a network or the Internet. It replaces TELNET and other insecure remote shells with a secure alternative. Server authentication (username and password) is required for security but the administrator can allow anonymous operation.

Specifications

Security and Authentication (SSL & SSH)

- SSHV1 and SSHV2
- SSL V3.0
- SSL Server and SSL client mode capability
- Encryption: AES (128/256), 3DES, DES, Blowfish, Twofish, CAST128, ARCFOUR(RC4), ARCTWO(RC2)
- Hashing Algorithms: MD2, MD4, MD5, SHA1 and SHA1-96
- Key exchange: RSA, DSA
- X.509 Certificate verification: RSA
- SSH server only

Compile Options

- Adding Blowfish, Twofish (128/256).
- User provided user authentication, certificate and key access.
- Permanent RSA and DSA keys are 512 bits wide.

Example Code

- Server for two serial ports with user authentication, certificate access, key access.
- Command processor with two serial ports.
- PEM encoded certificates and public/private key pairs (OpenSSH style)

Part Numbers

NetBurner Embedded SSL/SSH Security Suite

P/N: NBSSL-MOD-LIC

Only required if you are using a development kit.

Ordering Information

E-mail: sales@netburner.com

Online Store: www.Netburner.com

Telephone: 1-800-695-6828