Fusion Embedded™ HTTPS

Build Web-based management into your Internet Appliance application with Fusion Embedded HTTPS client and server. Fusion Embedded HTTPS adds the HTTPS communication protocol to the Fusion Embedded Web Server. HTTPS is implemented in a transparent way, which means that the original web server does not need to be changed in any way. All CGI-scripts and equivalent can be left unchanged.

Security Services Added to Web Interface

- Client and server authentication using X509 certificate Encryption Integrity information modified since it left the sender is detected.
- Replay detection, information that is replayed is rejected
- The HTTPS protocol uses TLS, the de-facto standard for web security
- All important webbrowsers suppport TLS
- No changes are needed on the clients, meaning the end-users can continue to use current browser

Fusion Embedded HTTPS allows you to serve up user-friendly HTML pages with images and data to allow monitoring of your Information Appliance from any Web browser in the world. It also allows users to control the Internet Appliance through forms-based pages that interact with the Internet Appliance to change the state of the device.

With Fusion Embedded HTTPS you can embed monitoring and control functions into your deployed Internet Appliances–employing the most recent security features while still reducing the cost of ownership for your customers. The APIs allow great flexibility in integrating with an application. They are designed to be fully portable written in ANSI C and requiring minimal operating system features.

Included with Fusion Embedded HTTPS Client & Server

- TLS Support which provides a foundation for Secure FTP and Secure Telnet
- Embedded HTTPS Web Server Security Package

Fusion Embedded HTTPS can also be implemented as an TLS proxy, based on Embedded TLS with a resulting product that is transparent, elegant and secure.

Features

- API designed to allow focus on web application development, not HTTP protocol syntax
- HTTP 1.0/1.1 compliant
- Multiple concurrent request
- Small memory footprint (7KB-11KB ROM)
- GET, POST Support
- Transfer chunked encoding support
- Full access and exposure to headers
- File system supported, optional
- Form item decoding
- Compliant with IETF RFC 2616
- Easily portable
- Single or multithreaded system operation
- Keep-alive connection support
- No modification needed to Web
- Server or CGI function hooks.
- All well-known web browsers support
- TLS
- Strong encryption (128 bit keys)
- Highly configurable
- Simple to install and use
- Issues PKCS#10 certificate requests for easy integration with Certificate Authorities, e.g. VeriSign
- Portable C source code included Manual Configuration of Security Associations (SA) Security policies based on individual or ranges of IP address(es), Port number(s) and/or protocol number
- Royalty-free license for OEMs
- ANSI C Embedded Source Code

Email: info@unicoi.com **Phone**: +1 (678) 208-2250 410 Peachtree Parkway, Cumming, GA 30041