



CRYPTO

—
Encryption Library

Interpeak Encryption Library

Creating network security software is a challenging task, often requiring implementation of several encryption algorithms. The Interpeak CRYPTO library facilitates this by providing numerous cryptographic routines and utilities, conveniently assembled into a single product.

Due to the design of the Internet core protocols, communication on the Internet today is vulnerable to security breaches. This means that extra measures must be taken to increase security to an acceptable level. There are basically four major aspects to secure communication.

The first is *authentication*, where both ends of a communication must identify each other. Second is message *integrity*, where the recipient of a message can verify that the contents have not been altered since it was generated by a legitimate source. Third, *privacy* makes it possible to prevent other people from intercepting and reading the contents of a message. The fourth aspect, *non-repudiation*, signifies that a message's characteristics, such as the content, sender and time of delivery, can be verified at a later date in order to substantiate a claim or an argument.

Cryptographic Library

Interpeak CRYPTO can be used to implement all of these security features for customer-specific client or server appli-

cations, as well as serve as an interface to standard Internet applications. It contains implementations of widely used services and cryptographic algorithms that can run on your embedded target system. The numerous algorithms and functions are assembled into a single, powerful crypto library, that provides a solid foundation for any security-based development. All of the Interpeak CRYPTO functions and algorithms comply with the relevant standards and specifications, and fully interoperate with other products.

RTOS Ports by Interpeak

Interpeak has ported the encryption library to a number of Realtime Operating Systems (RTOS), in order to support embedded realtime systems that require secure Internet communication, as well as an advanced high-performance RTOS.

Your Security Partner

Many qualities are required to successfully design and implement network security in an application based on an

embedded realtime operating system. The engineers must not only be skilled in RTOS design and development, but also experts on TCP/IP and network security.

However, with such demanding requirements, it is difficult to find a company or engineer who can understand all the necessary aspects of a project. Interpeak's years of experience in designing and developing embedded realtime TCP/IP and security products makes Interpeak the ideal partner for adding network security to your projects.

Support

Purchasing your project components from multiple product vendors or consultants can cause anxiety and logistical difficulties for any project. It is often hard to figure out which one of the products that is responsible for a certain problem, resulting in poor support quality and long response times. By purchasing Interpeak products, you are not only guaranteed excellent cryptographic, TCP/IP and RTOS support, but also continuity.

Standards-Based Solutions

Interpeak is committed to providing standards-based security and TCP/IP solutions. We perform extensive testing to verify that our products are fully compliant with other important standard applications from major communications companies.

The cryptographic library implementation and its underlying algorithms, ciphers, certificates, etc. all comply with all the relevant security standards and specifications.

- Extensive cryptographic library (hash/MAC algorithms, asymmetric and symmetric encryption, ASN1, X509 etc.).
- Over 30 shell-based target and host-based utility programs, e.g. certificate handling, CA scripts, CRL, encryption/decryption etc.
- Guaranteed quality, an extensive target test-suite included for verification.
- Delivered in ANSI compliant "C" source code.
- Complete ready-to-run RTOS integration with examples, makefiles etc.

Interpeak CRYPTO features.

Interpeak CRYPTO Features

The CRYPTO product also includes a powerful I/O module called BIO, which contains routines that handle filtering, buffering, encryption or decryption on basic input and output over sockets, file descriptors, memory, etc. Multiple BIO modules can be stacked to perform advanced cryptographic routines with minimum programming effort. The library contains functions for random number generation, as well as an advanced big number math library that is used for the cryptographic functions.

Furthermore, the library includes plentiful PKCS, PEM, X.509 and ASN.1 routines that deal with the storing and handling of certificates and digital objects. There are also additional utility modules, including hash tables,

lists, memory allocation, error handling and configuration file parsing.

Numerous Powerful Tools

Interpeak CRYPTO also provides a port of the OpenSSL command line tool *openssl*, a tool for using the various cryptographic functions from a shell. The tool consists of a collection of over 30 utility programs and can be run directly from a target system shell. The *openssl* tool can perform tasks such as:

- Creation of RSA, DH and DSA key parameters.
- Creation and verification of X.509 certificates, CSRs and CRLs.
- Calculation of message digests.
- Encryption/decryption with ciphers.
- PEM, PKCS#12 format conversions.

The Interpeak CRYPTO tool library can be used to run a multitude of cryptographic routines and handle the necessary tasks of a Certificate Authority (CA).

Quality Assurance

Superior product quality is often promised with little or no proof to back up the claim. The Interpeak CRYPTO product however, provides an extensive test system that thoroughly tests the robustness and functionality of the entire product. The test system consists of the *openssl* command line tool, over 20 additional command line test programs, as well as multiple shell scripts that are used to execute the programs with different arguments. The test system encrypts and decrypts files, generates various kinds of certificates, and converts back and forth between various standards and formats.

Target System Test Suite

Interpeak CRYPTO provides a target port of the extensive OpenSSL test system, making it possible to run the test system on the embedded target system. The entire target test system is included in the release in order for the customer to verify the quality of the RTOS integration, as well as the functionality and robustness of the Interpeak CRYPTO port. By running the automated target test system, users can feel confident of the quality of the Interpeak CRYPTO product.

SYMMETRIC CIPHERS

DES and triple DES
RC2, RC4 and RC5
Blowfish
CAST

SYMMETRIC MODES

ECB
CBC
OFB
CFB

ASYMMETRIC CIPHERS

RSA
Diffie-Hellman
DSA

CERTIFICATE & UTILITIES

X.509 and X.509v3
PKCS#12
PEM
ASN.1

HASH ALGORITHMS

MD2 and MD5
MDC2
SHA and SHA1
RIPEMD

MAC ALGORITHMS

HMAC-MD5
HMAC-SHA
HMAC-RIPEMD

Summary of the functions and algorithms included in the Interpeak crypto library.

The Interpeak CRYPTO product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit, www.openssl.org. The product also includes cryptographic software written by Eric Young, eay@cryptsoft.com, and software written by Tim Hudson, thj@cryptsoft.com.

Interpeak Secure Networking Software

Interpeak provides state-of-the-art networking solutions specifically designed for embedded systems. The company's embedded networking and security software is currently used in thousands of applications across the globe.

Headquartered in Stockholm, Sweden, Interpeak operates through a global network of distribution channels and has its own sales and field application force dispersed in strategic locations worldwide, including the USA, Europe, and Asia. For additional information, please visit our homepage www.interpeak.com.

All Interpeak products are trademarks or registered trademarks of Interpeak AB. Other brand and product names are trademarks or registered trademarks of their respective holders. The information in this document has been carefully reviewed, and is believed to be accurate and reliable. However, Interpeak AB assumes no liabilities for inaccuracies in this document. Furthermore, Interpeak AB reserves the right to change specifications embodied in this document without prior notice.

Version 1.22-r5. Copyright © 2005, Interpeak AB. All rights reserved.