コンパクトなSSL開発キット

μSSL Security Stack

Cypherbridge Systems

μSSL Security Stack は、米国 Cypherbridge Systems 社が開発した組み込み向け SSL 開発キットで、ANSI-C によるソースコードで提供されます。Thread-neutral な設計で、プロセッサ、OS、ネットワークスタックに依存することなく実装が可能です。

ライセンスモデルは実装される製品のビジネスモデルにより決められ、初期ライセンス料のお支払いのみでロイヤルティはございません。

多数のプロセッサ・OSでの稼働実績があり、主要開発環境のプロジェクトビルドを用意しています。また、ThreadX/NetX に対応したサンプルポートも用意されています。

製品仕様

- SSL3, TLS1.0, TLS1.1, TLS1.2 対応
- 暗号コア部分に libtomcrypt (OSS - BSD License) を使用
- ROM サイズ:60～70 kbytes
- RAM サイズ:基本部分 12 kbytes + メッセージバッファ 1～4 kbytes + 1セッションあたり 2.5 kbytes
- プロセッサ/RTOS 非依存
- NetX 用インターフェースレイヤ
- ANSI-C ソースコード提供
- ロイヤルティフリー

対応アルゴリズム

- AES-128, AES-256
- ARC4, DROP-ON
- DES, 3DES
- SHA-1, SHA-256, SHA-384, SHA-512
- MD2, MD5
- X509v3 証明書
- RSA 公開鍵暗号(最大2,048bits)
- Diffie-Hellman
- PKCS 1.5/2.1 OAEP padding
- HAVEGE RNG, MICRORNG

TLS ネットワークレイヤ

- HTTPS client & server sample
- SSL セッション再開処理
- SSL persistent connection
- X.509 証明書によるサーバー/クライアント認証

主な確認済みプロセッサ/OS/Tool

- Cortex-M3/M4, Sitara Cortex-A8, MSP 430, PowerPC, X86, Atmel AT91SAM, AVR32, Renesas M16C, RX62N, ADI Blackfin, ARM9, OMAP
- ThreadX/NetX, Micrium, FreeRTOS, X86 BSD, Embedded Linux, SEGGER embOS, Micro Digital SMX
- IAR/JLink, ARM/Keil

GRAPE SYSTEMS®

株式会社 グレープシステム® 営業部
〒220-6119 横浜市西区みなとみらい2-3-3 クイーンズタワーB 19F
TEL.045-222-3761 FAX.045-222-3760
E-mail : sales@info.grape.co.jp
www.grape.co.jp

2015.05.25