



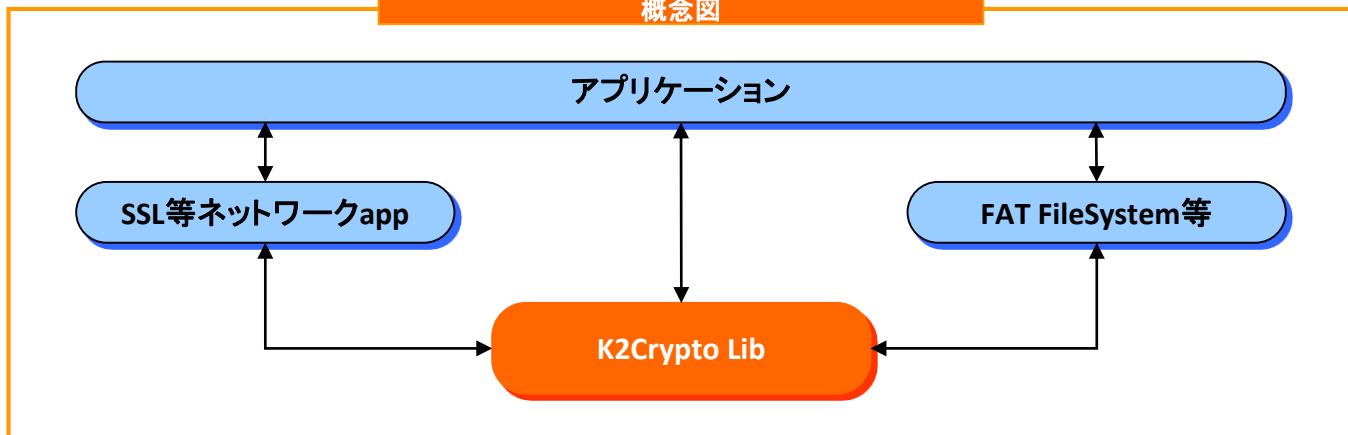
K2CryptoLib

概説

K2CryptoLibは暗号に必要なソフトウェアを収容したライブラリです。M2M/IoT環境でご利用頂けるよう、組み込みマイコン向けにチューニングをしています。収容暗号はKCipher-2(ストリーム暗号)です。KCipher-2を有効に使用するため、鍵の動的生成技術(特許第5586758号)の機能モジュールを同梱しています。

KCipher-2はKDDI研究所と九州大学が共同開発した技術で、電子政府推奨暗号(CRYPTREC)に選定されています。

概念図



仕様・特徴

- サポート暗号アルゴリズム
 - ・KCipher-2 (ストリーム形式 共通鍵暗号)
- 鍵の動的生成技術(特許第5586758号)の機能モジュールを同梱
- ROM: 40KByte(最小構成16KByte) / RAM: TBD
- 国際標準規格(ISO/IEC 18033-4)に準拠
- 米国標準暗号AESと比較し、7~10倍高速
- 搭載実績16MHz(Cortex-M0)~700MHz(ARM11)の 32bitマイコン

関数一覧

◆ 暗号化/復号

kcl_enc_initialize

kcl_encryption

kcl_dec_initialize

kcl_decryption

◆ 動的鍵生成

kcl_make_part_of_key

kcl_make_secretkey

◆ 暗号化/復号+動的鍵生成

kcl_make_part_of_key_ext

kcl_enc_initialize_ext

kcl_encryption_ext

kcl_dec_initialize_ext

kcl_decryption_ext

暗号化の初期化処理

暗号化処理

復号の初期化処理

復号処理

動的鍵生成向け鍵断片生成

暗号化鍵生成

動的鍵生成向け鍵断片生成

鍵断片利用の暗号化初期化処理

鍵断片利用の暗号化処理

鍵断片利用の復号初期化処理

鍵断片利用の復号処理



■ライセンス

●ライセンス基本条件

- 1) 開発場所(部単位)を限定いたします。
- 2) 指定MPU(型番)を限定いたします。
- 3) ライブラリ形式(使用に必要なAPIを提供)

●ライセンスの種類

1) プロジェクトライセンス

同一プロジェクト(同一製品シリーズ、上位機種、下位機種含む)の範囲に限定した使用許諾契約です。

2) 端末ライセンス(量産ライセンス)

1ヶ月単位で出荷報告を頂き、単価に基づきご請求いたします。

単価は積算数により低下しますが、1年でリセットされます。

●技術サポート

- 無償技術サポート: プロジェクトライセンスには、ご購入から1年間の無償技術サポートが付属しています。
- 年間技術サポート: 無償技術サポート期間以降は、有償にて1年単位の技術サポートの更新が可能です。
- 技術サポートには、バージョンアップサービスが含まれます。
- 技術サポートには、ライブラリの利用方法、システム設計上でのアドバイスを含まれます。
- 技術サポートの対応は、ご契約時のコンパイラに限定いたします。
- 技術サポートは原則、最新バージョンにて対応させていただきます。
- 受付時間: 弊社営業日 9:00~17:00
- 受付・応答媒体: 電子メール
- 応答時間: 3営業日以内

■価格

お問い合わせください。

【販売・開発・製造】

TSH 東京システムハウス株式会社

スマートセキュリティプロジェクト

〒141-0031 東京都品川区西五反田7-1-10 ユーズワンビル4F

TEL: 03-3493-5736 FAX: 03-3493-5188

●お問い合わせ先: 詳しくはサイトをご覧ください

【販売店】

データテクノロジー株式会社

〒190-0011 東京都立川市錦町1-8-7 立川錦町ビル8F

TEL: 042-523-1177 FAX: 042-523-7070

www.tsh-world.co.jp