MiddleWare Package

Cente® Suggestion to Embedded

Compact DTLSd

概　説

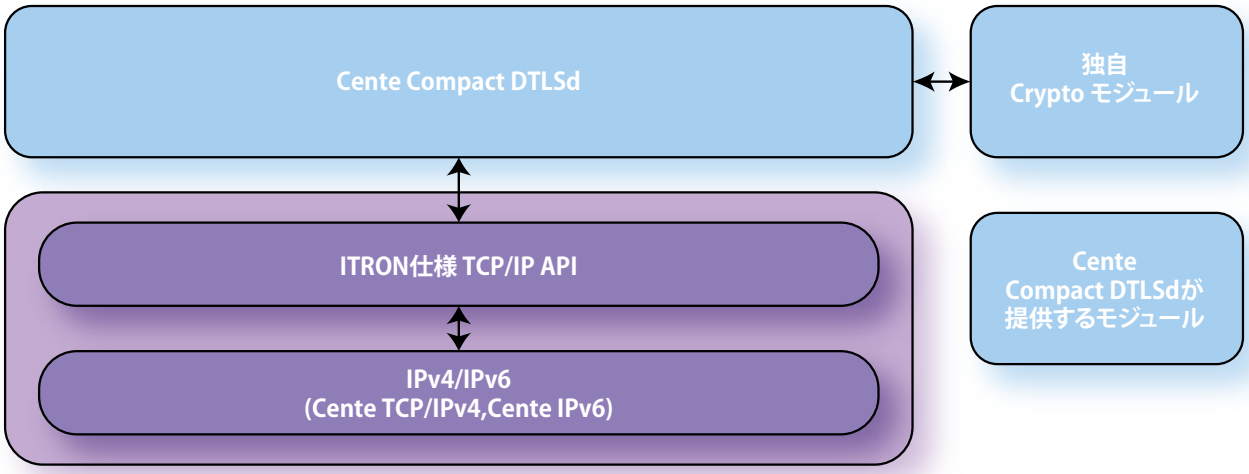
Cente Compact DTLSd は IPv4/v6 通信環境上のネットワークアプリケーション間で Datagram Transport Layer Security（DTLSv1.0/v1.2）による暗号・秘匿通信を可能とする組込み開発専用のソフトウェアモジュールです。

TCP/IP のコアモジュールである「Cente TCP/IPv4」又は「Cente IPv6」と組み合わせることで、μITRON 環境上で開発された UDP/IP 通信機器を簡単にセキュア通信環境へ移行させることができます。

Cente Compact DTLSd は、組込み向けにスクラッチから書き起こしたセキュリティソフトウェアモジュールです。コンパクトなメモリサイズ、高い移植性、拡張・変更の容易なモジュール構成など、組込み環境に適した設計となっています。

本モジュールは DTLS サーバとして動作します。DTLS クライアントは別製品（Cente Compact DTLSc）をご利用ください。

概念図



仕様・特徴

- ●DTLS対応バージョン DTLS 1.0/1.2
- ●コンパクトなサイズ
  ROM：16KByte / RAM：33KByte、1接続ごとに+25KByte
- ●暗号化アルゴリズム: DES, 3DES, AES
- ●ハッシュアルゴリズム: SHA1, SHA256
- ●鍵交換方式: RSA　（最大鍵長はカスタマイズ可能）
- ●証明書方式: X.509v1, v2, v3
- ●証明書の署名アルゴリズム：SHA1_RSA, SHA256_RSA
- ●ハードウェア暗号エンジンにも対応可能
- ●CPU/エンディアン非依存、μITRON4、3で動作可能
- ●I/Oレイヤ非依存、BSDソケットにも容易に対応可能
- ●通信途中の再ネゴシエーション(鍵の再生成)可能
- ●IPv4, IPv6両対応
- ●動的メモリ不使用

MiddleWare Package

Cente® Compact DTLSd

Suggestion to Embedded

■製品構成

●DTLSdモジュール本体

●独自crypto（暗号・ハッシュアルゴリズム）ライブラリ

■ハードウェア暗号エンジンの使用について

●Cente Compact DTLSdはソフトウェア暗号・復号アルゴリズムの他、ハードウェア暗号エンジンによる高速暗号・認証にも対応可能です。

■制限事項など

●証明書はDER形式のみ（PEMは非対応）
●私有鍵はDER形式のみ（PEMは非対応）
●クライアント証明には非対応
●セッションキャッシュ非対応
● CRLには非対応

■対応暗号スイート

DTLSD_RSA_WITH_DES_CBC_SHA
DTLSD_RSA_WITH_3DES_EDE_CBC_SHA
DTLSD_RSA_WITH_AES_128_CBC_SHA
DTLSD_RSA_WITH_AES_256_CBC_SHA
DTLSD_RSA_WITH_AES_128_CBC_SHA256
DTLSD_RSA_WITH_AES_256_CBC_SHA256
DTLSD_RSA_WITH_AES_128_GCM_SHA256 ※

※ DTLSD_RSA_WITH_AES_128_GCM_SHA256
Cente Compact Crypto AES-CCM/GCMを使うと、RFC5288で規定されているTLS_RSA_WITH_AES_128_GCM_SHA256を使用することができます。Cente Compact Crypto AES-CCM/GCMは別パッケージになります。

■関数一覧

dtlsd_init	DTLSd情報の初期化
dtlsd_recv	データを受信する
dtlsd_send	データを送信する
dtlsd_get_state	セッション状態の取得
dtlsd_disconnect	通信終了の通知
dtlsd_get_write_size	dtlsd_sendで送信できるデータサイズの取得

【販売・開発・製造】
データテクノロジー株式会社
〒190-0022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
ビー・ユー・ジー森精機株式会社
〒004-0015北海道札幌市厚別区下野幌テクノパーク1-1-14

●お問い合わせ先:詳しくはサイトをご覧ください
www.cente.jp
E-mail:sales@cente.jp
TEL:042-523-1177

【販売代理店】
株式会社 DTS インサイト
［東 京 本 社］〒151-0053 東京都渋谷区代々木4-30-3 新宿MIDWESTビル
TEL:03-6756-9405 FAX:03-6756-9409
URL:https://www.dts-insight.co.jp
E-mail:info-advice@dts-insight.co.jp

CDTLSD_20140616