

MiddleWare Package

Cente Compact Crypto

MiddleWare Package

Cente Compact Crypto Plus

概 説

Cente Compact Crypto はオープンソースなどを使わず独自に開発した、暗号・認証ライブラリです。BSD や GPL などのライセンスに影響されことなく使用することができます。

AES、ARC4、DES、3DES、MD5、SHA1、SHA256、SHA384、SHA512 など、一般的によく使用されるアルゴリズムを厳選し、組み込み機器用にコンパクトなフットプリントを実現しています。

Cente ミドルウェアの既存パッケージで使用しているモジュールですが、本ライブラリを単独で使いたいというご要望にお応えしてパッケージにしました。

Cente Compact Crypto Plus は、Cente Compact Crypto のオプションパッケージです。

Cente Compact Crypto と組み合わせることで、鍵交換に DHE, ECDHE を、認証に ECDSA を、共通鍵暗号方式に AES-GCM, ChaCha20-Poly1305 を使用できます。

仕様・特徴

《Cente Compact Cryptoパッケージ》

- サポート暗号・認証アルゴリズム
 - ・対称鍵暗号
DES, 3DES, ARC4, AES
 - ・公開鍵暗号
RSA
 - ・証明書
X.509, X.509v3
 - ・ハッシュアルゴリズム
HMAC, MD4, MD5, SHA1, SHA256, SHA384, SHA512
- RSA対応鍵長
3072bit まで対応
- メモリサイズ
ROM: 55KByte / RAM: 100Byte
※ RSAは多倍長計算に数十KByteの RAM領域を必要とします。

《Cente Compact Crypto Plusパッケージ》

- サポート暗号・認証アルゴリズム
 - ・対称鍵暗号
AES-GCM, ChaCha20-Poly1305
 - ・鍵交換
DHE, ECDHE
 - ・認証
ECDSA
- メモリサイズ
ROM: 90KByte / RAM: 100Byte
※ Cente Compact Cryptoを含んだメモリサイズです。
※ RSA, DH, DSA, ECCは多倍長計算に数十KByteの RAMを必要とします。

関数一覧

《DES》	
des_set_enc_key	DESエンコード用キースケジュール作成
des_set_dec_key	DESデコード用キースケジュール作成
des_ecb	DES ECB処理(エンコード・デコード)
des_cbc_enc	DES CBCエンコード
des_cbc_dec	DES CBCデコード
《ARC4》	
arc4_set_key	ARC4キースケジュール作成
arc4_crypt	ARC4処理(エンコード・デコード)
《擬似乱数》	
rand_get	ランダムデータ取得
rand_add_entropy	エントロピー供給

《3DES》	
des3_set_enc_key	3DESエンコード用キースケジュール作成
des3_set_dec_key	3DESデコード用キースケジュール作成
des3_ecb	3DES ECB処理(エンコード・デコード)
des3_cbc_enc	3DES CBCエンコード
des3_cbc_dec	3DES CBCデコード
《AES》	
aes_block_enc	AES1ブロックのエンコード
aes_block_dec	AES1ブロックのデコード
aes_ecb_enc	AES ECBエンコード
aes_ecb_dec	AES ECBデコード
aes_cbc_enc	AES CBCエンコード
aes_cbc_dec	AES CBCデコード
aes_cfb_enc	AES CFBエンコード
aes_cfb_dec	AES CFBデコード
aes_set_enc_key	AESエンコード用キースケジュール作成
aes_set_dec_key	AESデコード用キースケジュール作成

■関数一覧

《RSA》	
rsa_pub_crypt	Public鍵での演算
rsa_pub_crypt_p	Public鍵での演算(ワークエリア指定)
rsa_pkcs1_encrypt	PKCS#1エンクリプト
rsa_pkcs1_encrypt_p	PKCS#1エンクリプト(ワークエリア指定)
rsa_pkcs1_decrypt	PKCS#1デクリプト
rsa_pkcs1_decrypt_p	PKCS#1デクリプト(ワークエリア指定)
《X.509》	
x509_parse	X.509証明書のパースとT_X509構造体へのセット
x509_get_rsakey	T_X509構造体からRSA鍵を取得
x509_get_time	T_X509構造体から有効期限を取得
x509_is_issued	2つのX.509証明書が親子関係にあるか検証
x509_is_issued_p	2つのX.509証明書が親子関係にあるか検証(ワークエリア指定)
《MD5》	
md5_init	MD5コンテキスト初期化
md5_update	MD5ダイジェスト計算
md5_final	MD5ダイジェスト取得
md5	MD5ダイジェスト初期化、計算、取得
md5_hmac_init	MD5-HMACコンテキスト初期化
md5_hmac_update	MD5-HMACダイジェスト計算
md5_hmac_final	MD5-HMACダイジェスト取得
《SHA1》	
sha1_init	SHA1コンテキスト初期化
sha1_update	SHA1ダイジェスト計算
sha1_final	SHA1ダイジェスト取得
sha1	SHA1ダイジェスト初期化、計算、取得
sha1_hmac_init	SHA1-HMACコンテキスト初期化
sha1_hmac_update	SHA1-HMACダイジェスト計算
sha1_hmac_final	SHA1-HMACダイジェスト取得
《SHA256》	
sha256_init	SHA256コンテキスト初期化
sha256_update	SHA256ダイジェスト計算
sha256_final	SHA256ダイジェスト取得
sha256	SHA256ダイジェスト初期化、計算、取得
sha256_hmac_init	SHA256-HMACコンテキスト初期化
sha256_hmac_update	SHA256-HMACダイジェスト計算
sha256_hmac_final	SHA256-HMACダイジェスト取得

《SHA384》	
ctsha384_init	SHA384コンテキスト初期化
ctsha384_update	SHA384ダイジェスト計算
ctsha384_final	SHA384ダイジェスト取得
ctsha384	SHA384ダイジェスト初期化、計算、取得
ctsha384_hmac_init	SHA384-HMACコンテキスト初期化
ctsha384_hmac_update	SHA384-HMACダイジェスト計算
ctsha384_hmac_final	SHA384-HMACダイジェスト取得
《SHA512》	
ctsha512_init	SHA512コンテキスト初期化
ctsha512_update	SHA512ダイジェスト計算
ctsha512_final	SHA512ダイジェスト取得
ctsha512	SHA512ダイジェスト初期化、計算、取得
ctsha512_hmac_init	SHA512-HMACコンテキスト初期化
ctsha512_hmac_update	SHA512-HMACダイジェスト計算
ctsha512_hmac_final	SHA512-HMACダイジェスト取得
《AES-GCM》	
aesgcm_set_key	鍵からAES-GCM用キースケジュールを作成
aesgcm_enc_init	AES-GCMコンテキスト初期化
aesgcm_enc_update	AES-GCMエンコード、ダイジェスト計算
aesgcm_enc_final	AES-GCMダイジェスト取得
aesgcm_enc	AES-GCMエンコード
aesgcm_dec	AES-GCMデコード
《ChaCha20-Poly1305》	
chacha20_aead_setkey	ChaCha20-Poly1305キー設定
chacha20_aead_encrypt_init	ChaCha20-Poly1305コンテキスト初期化
chacha20_aead_encrypt_update	ChaCha20-Poly1305計算
chacha20_aead_encrypt_final	ChaCha20-Poly1305MAC取得
chacha20_aead_setkey	ChaCha20-Poly1305復号
《DH》	
dh_ini	DHコンテキスト初期化
dh_generate_key	DH秘密鍵計算
dh_gir	DH共通鍵計算
《DSA》	
dsa_check_p	DSA署名チェック
ecdsa_check_p	ECDSA署名チェック
《ECC》	
ecdh_calc_pubkey	ECDH公開鍵計算
ecdh_gen_hey	ECDH共通鍵計算

【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DMG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