escrypt
SECURITY. TRUST. SUCCESS.

CycurLIB

組み込みシステム用の暗号ライブラリ

概要

暗号化プロトコルと暗号化アルゴリズムは、IT セキュリティアプリケーションにセキュリティ機能の基盤を提供します。たとえば、セキュアフラッシュ、機能のアクティベーション、セキュアブートには、デジタル署名検証などの暗号化アルゴリズムが必要です。暗号ライブラリは、あらゆる組み込みセキュリティソリューションの基盤として使用されます。

CycurLIB には、一般的な暗号化機能が効率よく実装されており、ASPICE（LEVEL 2）および ISO 26262 準拠のプロセス（ASIL D）で開発されています。

CycurLIB は、自動車業界、医療装置や機械製造などの量産品で広く使用されています。

CycurLIB は、厳しい性能制約を満たしつつ、コードのサイズに応じて最適化された暗号化アルゴリズムを提供します。

CycurLIB では、署名を検証してデータの真正性と完全性を判定することで、製品の安全性を容易に向上できます。CycurLIB は、顧客のニーズに応じて細かな設定が可能です（AUTOSAR に準拠した設定ツールを使用します）。

ESCRYPT 2020/01

escrypt
SECURITY. TRUST. SUCCESS.

詳細

全般

- MISRA-C:2012 と ANSI-C 標準に基づいた実装
- コードのサイズに応じて最適化されている一方で、厳しい性能制約をクリア
- HIS ソースコードメトリクス準拠のコンポーネント
- ASPICE（LEVEL 2）準拠の開発プロセス
- ISO 26262 準拠の開発プロセス（ASIL D）
- AUTOSAR 対応
  - AUTOSAR 準拠の設定ツール
  - AUTOSAR 準拠のメモリマッピング
- 製品への統合が容易
- 直感的な API
- モジュール構造のため、ソフトウェアを直接適合可能
- 詳しい解説付き

利用可能な暗号アルゴリズム

- AES
  - 鍵サイズ :128 ビット、192 ビット、256 ビット
  - 暗号利用モード : CBC、GCM
- ハッシュアルゴリズム
  - SHA-2（SHA-224、SHA-256、SHA-384、SHA-512）
  - SM3
- メッセージ認証コード
  - HMAC-SHA2、HMAC-SM3
  - CMAC-AES
  - SipHash
- 楕円曲線
  - 署名の生成と検証
    - ECDSA（決定的および非決定的）：NIST P-224、P256、P-384
    - Ed 25519
    - SM2 Digital Signature Algorithm（SM2 デジタル署名アルゴリズム）
  - 鍵の交換と生成
    - ECDH：NIST P-224、P-384
    - Curve 25519
    - SM2 鍵交換
  - 非対称暗号化
    - ECIES
    - SM2 暗号化
- RSA
  - モジュラス : 1024 ビット、2048 ビット、3072 ビット、4096 ビット
  - サポートされている RSA 署名方式 : PKCS#1 RSASSA-PSS、PKCS#1 RSASSA-V1.5
- 証明書
  - X.509 パーサーおよびチェーン検証
- RNG および KDF
  - 乱数の生成 : HMAC-DRBG
  - 鍵導出関数 : NIST SP800-56A rev1 に準拠した KDF2、KDF
- 中国系アルゴリズム
  - SM2、SM3、SM4（中国国家規格に準拠した楕円曲線暗号、ハッシュ関数、およびブロック暗号）

サポートされているプラットフォーム

- C99 準拠のコンパイラを備えたすべてのプラットフォーム（8 ～ 64 ビット）

機能＆利点

- 既存製品へのシームレスな統合
- 一般的な暗号アルゴリズムと証明書の標準をすべてサポート
- 最高の品質基準を満たす実装
- 低フットプリント
- モジュール化された構成
- すべてのプラットフォームで動作可能

継続的な機能強化と調整

- 拡張／変更 : 市場の動向とお客様の要件に基づいた機能拡張

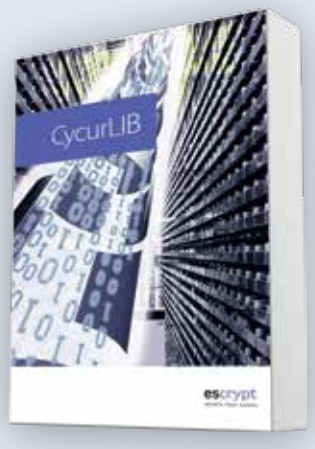
カスタマイズ

- 拡張および変更に関する不明点については、当社までお問い合わせください。

予告

- CycurLIB コンポーネント : AUTOSAR CryptoDriver

2020年リリース: ISO 26262（ASIL D）に準拠



イータス株式会社　ESCRYPT 事業部
TEL：045-222-0900（代表）
E-mail：sales.jp@etas.com