Empowering Tomorrow's Automotive Software
www.etas.com

組み込み システム用の 暗号ライブラリ ESCRYPT CycurLIB

概要

IT セキュリティアプリケーションにとって、暗号化プロトコルと暗号化アルゴリズムはセキュリティ機能の根幹を成す重要な要素です。たとえば、セキュアなソフトウェア更新、セキュアブート、暗号化 / 認証された通信、および機能の有効化などが必要となります。

ESCRYPT CycurLIB は、こうしたニーズに応える、暗号アルゴリズムとセキュリティ標準の効率的な実装のための暗号ライブラリを提供します。

組み込みシステム向けに最適化された ESCRYPT CycurLIB は、処理能力やメモリなどのリソースが特に限られた環境で抜群のパフォーマンスを発揮します。

ESCRYPT CycurLIB は、特定のマイクロコントローラ、オペレーティング システム、または外部ライブラリに依存せず、十分な RAM/ROM を備えたどのマイクロコントローラでも使用できます。

ESCRYPT CycurLIB は、耐量子暗号アルゴリズムを含む暗号化アルゴリズムの包括的なセットの他、NIST や中国の暗号標準もサポートしています。

これにより、多様なアプリケーション、特に自動車産業での使用が可能になります。

この暗号化ライブラリは、道路車両サイバーセキュリティの ISO 標準である「ISO/SAE 21434:2021 Road Vehicles – サイバーセキュリティエンジニアリング」に準拠したセキュリティエンジニアリングプロセスを実現します。

ESCRYPT CycurLIB はモジュール式で統合が容易、かつ厳しいパフォーマンスを満たしながらコードサイズを最適化します。署名を検証してデータの真正性と整合性を判定する機能、AUTOSAR に準拠したコンフィグツールを使用することで、簡単に導入して製品の安全を確保することができます。

耐量子暗号 アルゴリズム 対応

実証済み、認証済みのクオリティ

品質は ETAS のビジネス原則に深く根ざしており、すべての製品開発の根幹となる部分です。当社は最高品質の製品のみをお客様に提供することをお約束します。当社の高品質な暗号ライブラリは、さまざまな機関の認証を受けています。

ASPICE

「Automotive Software Process Improvement and Capability dEtermination」（ASPICE）は、広く採用されている業界標準です。主要な自動車メーカーは、これを使用して、電子機器やソフトウェア サプライヤーのプロセスの品質と能力を評価しています。

– ESCRYPT CycurLIB は ASPICE レベル 2 に準拠しています。

ASIL D

自動車のリスク分類 ASIL D は、機能安全 ISO の一部であり、最高レベルのリスク管理を表しています。ASIL D 向けに設計されたコンポーネントは、最も厳しい安全要件を満たしています。

– 暗号化ライブラリは、ISO 準拠の（ASIL D）のプロセスに従って開発されています。

– ESCRYPT CycurLIB は、セーフティクリティカルなアプリケーションに実装可能です。

FIPS と CAVP

米国国立標準技術研究所（NIST）による「連邦情報処理標準（FIPS)」は、暗号化モジュールのセキュリティ要件を規定しています。

NIST の「Cryptographic Algorithm Validation Program（CAVP)」は、暗号アルゴリズムとその個々のコンポーネントの検証テストを提供します。

– FIPS 認定のバリアントが利用可能

– CAVP 検証は近日中にサポート予定

テスト

ESCRYPT CycurLIB は、約 15,000 ユニットで継続的かつ厳密にテストされており、100% の合格率で統合および認定テストが実施されています。
世界中の何百万もの車両やアプリケーションで利用されている実績が、暗号化ライブラリの品質の高さを物語っています。

フリーウェアと ESCRYPT CycurLIB との比較

フリーウェアの暗号ライブラリ	ETAS の暗号ライブラリ
? 十分にテストされているか不明	✓ 厳格にテスト済み
? GPL ライセンスを使用している可能性あり	✓ オープンソース不使用（GPL なし）
× 製品サポートなし	✓ 長期的な製品サポートと保守
× お客様のインシデント対応やサポートなし	✓ お客様のインシデント対応やサポート付き
× 車載システムおよびマイクロコントローラに非対応	✓ 車載システムおよびマイクロコントローラに対応
× 一般的に、セーフティの用途は非対応	✓ セーフティクリティカルなアプリケーション用として実証済み

利用可能な暗号アルゴリズム

カテゴリ	アルゴリズム
対称ブロック暗号	AES SM4
動作モード	CBC CCM CTR GCM
認証暗号化	ChaCha20-Poly1305
対称ストリーム暗号	ChaCha20
デジタル署名	RSASSA-PSS RSASSA-PKCS1-V1_5 ECDSA EdDSA SM2 Digital Signature
耐量子暗号アルゴリズム	CRYSTALS-KYBER CRYSTALS-DILITHIUM
非対称暗号化	SM2 Encryption ECIES ECIES DHAES RSA-OAEP
ハッシュアルゴリズム S	SHA-2 SHA-3 SM3
メッセージ認証コード（MAC）	CMAC HMAC Poly1305 SipHash24
Diffie-Hellman 鍵交換	Curve25519 ECDH FFC DH
MQV 鍵交換	SM2 Key Exchange
鍵導出アルゴリズム	KDF2 / ANSI X9.63 KDF Hash-based KDF according to NIST SP800-56C HKDF according to RFC5869 KDF in CTR mode with AES-CMAC according to NIST SP800-108
キーラップ	NIST AES Key Wrapping
疑似乱数生成	HMAC_DRBG Hash_DRBG
証明書	X.509 parsing and chain validation OCSP response parsing and validation
パスワード認証鍵交換	SPAKE2+

詳細

全般

- MISRA-C:2012 と ANSI-C 標準に基づいた実装
- HIS ソースコードメトリクス準拠のコンポーネント
- 外部ライブラリは不要（OSS は含まれていない）
- 動的メモリ割り当てなし
- 厳しいパフォーマンス制約を満たしながら、コードサイズを最適化
- モジュラー構造のため、ソフトウェアを直接適応可能
- GUI による設定
- ASPICE（レベル 2）準拠の開発プロセス
- ISO 26262 準拠の開発プロセス（ASIL D まで）
- AUTOSAR 準拠
  - AUTOSAR 準拠の設定ツール
  - AUTOSAR 準拠のメモリマッピング
- FIPS 認定バリアントが利用可能
- 詳しい解説付き
- 直感的な API
- 製品への統合が容易
- 特定のマイクロコントローラに依存しない

サポートするプラットフォーム

- ANSI-C 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 ビット～ 64 ビット）

将来的な拡張

- コンポーネント : AUTOSAR CryptoDriver
- 耐量子暗号アルゴリズムの最適化
- EdDSA 拡張機能（Ed448）

ESCRYPT CycurLIB のアドバンテージ

- 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サポート
- 最高の品質基準を満たす実装
- 小フットプリント
- 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
- 高品質なお客様サポート

- **継続的な機能強化と適応**
  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**
  拡張および変更についての詳細は、ETAS までお問い合わせください

ETAS の製品とソリューションに関するお問い合わせ：
info@etas.com

製品の詳細情報：
www.etas.com/CycurLIB

ETAS/COM-JP/03-2023