Empowering Tomorrow's Automotive Software
www.etas.com

車載 HSM 向け セキュリティ スタック ESCRYPT CycurHSM

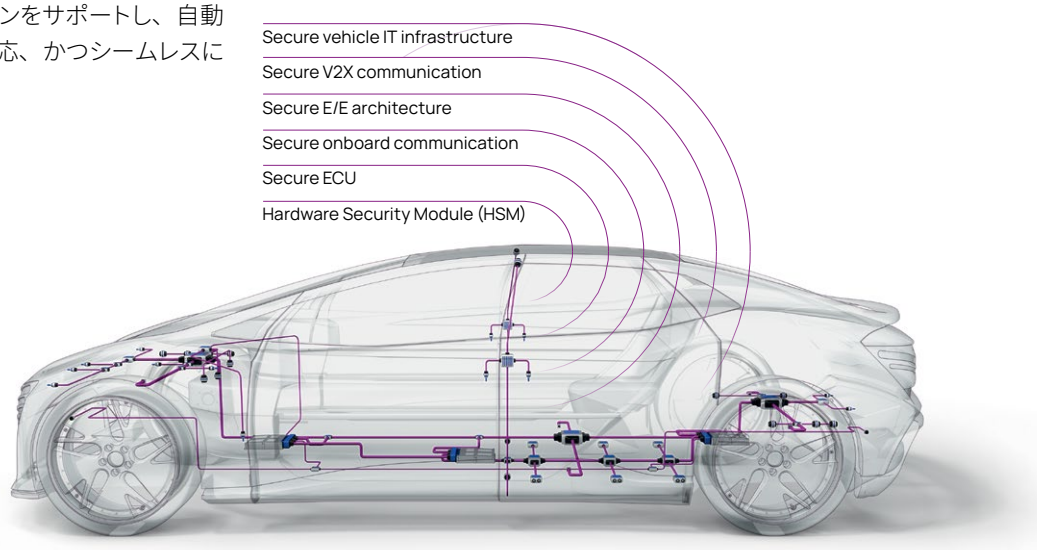
概要

ECU レベルのセキュリティを確保する場合、ソフトウェアのみのセキュリティ ソリューションでは、システムの整合性を十分には保護できません。組み込みシステムを攻撃から確実に守り、ソフトウェアの整合性を保護するには、ハードウェアセキュリティモジュール (HSM) が不可欠です。HSM はデータの機密性を確保して、システムの整合性と信頼性を維持します。

ESCRYPT CycurHSM は、HSM が組み込まれた車載マイクロコントローラ用のアプリケーションをサポートする、完全なセキュリティソフトウェアスタックであり、複数の半導体メーカーによる幅広い車載 HSM に対応しています。ESCRYPT CycurHSM は、モジュール式の柔軟な HSM ファームウェアであり、オープンで標準化されたインターフェース (AUTOSAR、SHE+ など) を介して、あらゆるセキュリティアプリケーションをサポートし、自動車メーカー独自のセキュリティ要件にも対応、かつシームレスに統合します。

ESCRYPT CycurHSM は、世界中の 自動車メーカーやサプライヤーとの何百ものプロジェクトに実装され、すでに数百万台の車両に搭載されている、実績あるソリューションです。また、高度に最適化された HSM ソフトウェアが最高レベルの ECU セキュリティを保証します。

ESCRYPT CycurHSM は、世界初の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」において最も厳格な CAL4（サイバーセキュリティ保証レベル 4）の認証を受けています。



サポートする機能

ETAS の ESCRYPT CycurHSM は、幅広い機能を提供します。

暗号や証明書
- 非対称暗号化アルゴリズム
  - RSA
  - ECDSA、ECBD、ECDH、ECDHE、EdDSA
- 標準の暗号サービス
  - 対称暗号化（AES など）
  - MAC の生成と検証（CMAC、HMAC など）
  - 乱数生成（TRNG、PRNG）
  - ハッシュアルゴリズム
  - 鍵導出
- 証明書サポート（認証、解析）
- 中国のアルゴリズム
- 鍵交換プロトコル（Diffie-Hellman）

フィールドリターン分析と HSM デバッグ
- フェールセーフ HSM アップデート
- HSM 制御のセキュアアクセス (チャレンジレスポンス プロトコル)
- HSM デバッグ
- HSM ダンプ
- セキュアなホストフラッシング
- セキュアロギング

HSM コアの一般機能
- バンクスワップ SOTA サポート
- コンポーネント保護（SHE+ サポート）
- フラッシュの耐久性を拡張するための EEPROM エミュレーション
- HSM ライフサイクルモード
- HSM RAM モード
- メモリロック解除（フラッシュパスワード保護）
- マルチコアのサポート
- ランタイム操作の検出
- セキュアブート、トラステッドブート、認証ブート、その他のブートモード
- データと鍵の安全な保管
- 多数の鍵（› 100）を持つシステムのサポート
- 署名に基づくトラストアンカー
- プリエンプティブな並列ジョブ処理

OEM 向けの機能
- OEM 特有のプロトコルや機能に対応する、OEM 別の構成サービス

カスタマイズ可能
本製品にご興味がある場合、特定の用途でご利用を検討中の場合は、ぜひお問い合わせください。

ESCRYPT CycurHSM は、お客様固有のニーズに合わせた構成が可能な、柔軟性の高いセキュリティファームウェアです。

ESCRYPT CycurHSM のアドバンテージ

- **使いやすさ**
  AUTOSAR 対応、AUTOSAR 非対応の自動車アプリケーションにシームレスに統合可能
- **迅速さ**
  リアルタイムオペレーティングシステムに基づく設計により、HSM のリアルタイム特性を実現
- **信頼性**
  オープンソースソフトウェアを使わずにコーディング
- **包括性**
  全 OEM の幅広い要件を満たすために必要なセキュリティ機能をすべてカプセル化
- **将来性**
  最新の基準や新しいサイバーセキュリティ規制に準拠（ISO/SAE 21434）
- **最高品質**
  最高水準の品質基準を満たし（ASPICE、ISO 26262 ASIL D）、セーフティクリティカルなアプリケーションに対応
- **セキュリティ**
  高性能な暗号化が求められるお客様独自のアプリケーションに応じた、強力で多様なハードウェア / ソフトウェア協調デザインプラットフォームを提供
- **柔軟性**
  OEM 特有の暗号要件に対応可能な Variant Configuration を用意し、HSM Firmware を Binary File で提供

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/CycurHSM

ETAS/COM-JP/03-2023