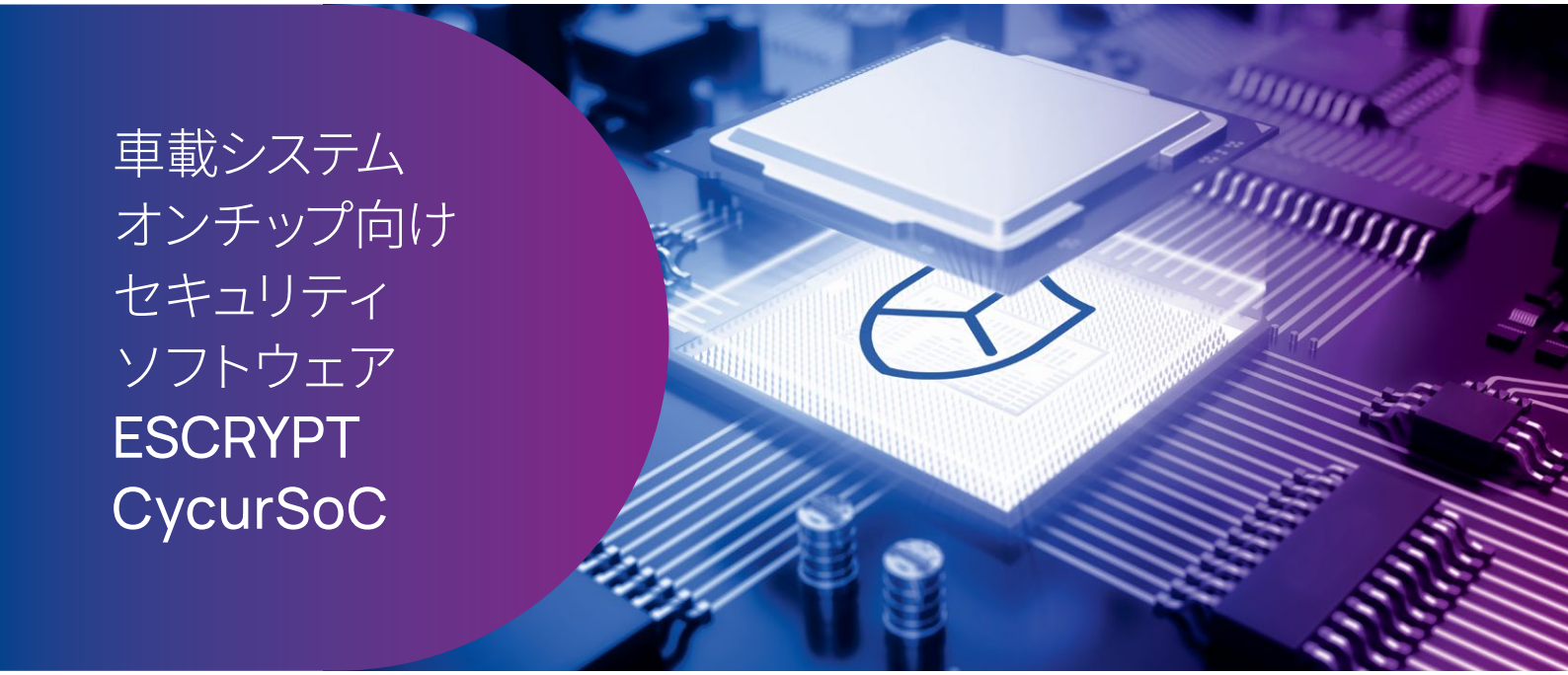
Empowering Tomorrow's Automotive Software
www.etas.com

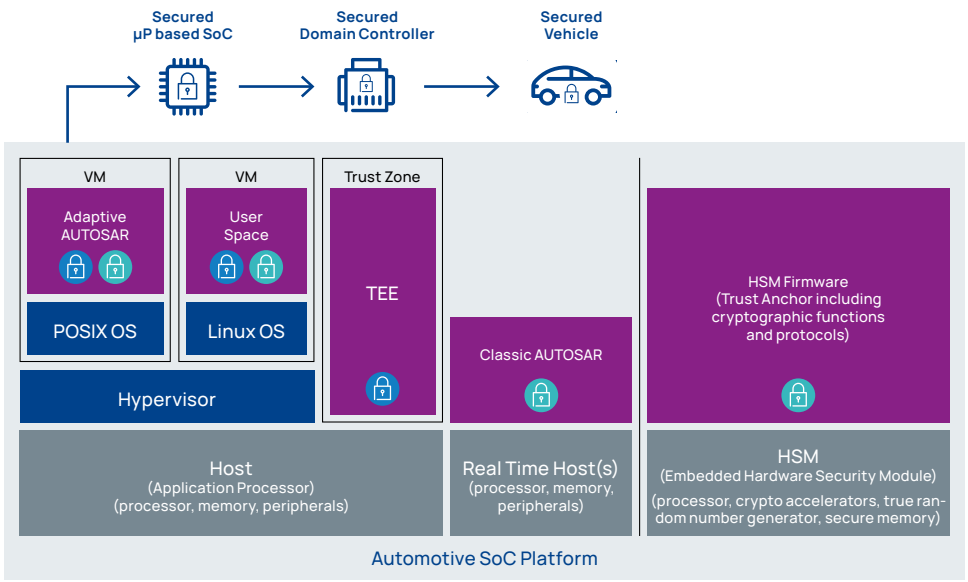
車載システム オンチップ向け セキュリティ ソフトウェア ESCRYPT CycurSoC



ソフトウェアデファインドビークル（SDV）の安全性と信頼性を実現

電動化や自動運転、先進運転支援システム（ADAS）、インフォテインメントシステムにより、強力な車載コンピューティングプラットフォームの出現が加速しています。これらのプラットフォームの中枢コンポーネントは、マイクロプロセッサベースのシステムオンチップ（SoC）です。
SoC プラットフォームにより、車載 E/E アーキテクチャは従来の分散型 ECU からさらに集中型のドメインアーキテクチャへと進化しました。
高度な E/E アーキテクチャは、カスタマーエクスペリエンスの向上と自動化の促進につながる強力なソフトウェア機能をサポートします。ただし、このようなメリットには、サイバーセキュリティの脆弱性や脅威への対処が伴います。

ESCRYPT CycurSoC は、将来まで見据えた SoC ベースの車載 ECU 向け組み込みサイバーセキュリティソフトウェアソリューションです。車載セキュリティのさまざまなユースケースに対応して設計されており、HSM コアやその他の SoC CPU コアを利用する各種 SoC アーキテクチャ向けのセキュリティビルディングブロック一式を提供します。
ESCRYPT CycurSoC は、使用可能なシステムリソースへの影響を最小限に抑えるように最適化されています。標準化されたオープンインターフェース（SHE+、AUTOSAR Classic、AUTOSAR Adaptive など）をサポートし、仮想マシンや各種ホスト環境を含むさまざまな組み込みテクノロジーソリューションと柔軟に統合が可能です。



HSM & TEE バリアント

- **ESCRYPT CycurSoC-HSM** は、マイクロプロセッサ（µP）ベースの SoC プラットフォーム向けの、HSM コアファームウェアバリアントです。
- **ESCRYPT CycurSoC-TEE** は、HSM コアを持たない可能性のあるµP ベースの SoC プラットフォームの Trusted Execution Environment（TEE）ソフトウェア バリアントです。
- プラットフォームとセキュリティのユースケースに応じて、両方のバリアントを個別に提供することも、相互に補完することもできます。
- どちらのバリアントもルートオブトラストとして機能し、SoC リソースを効率的に利用して、セキュリティの完全性、堅牢性、およびゼロトラストの概念を維持します。

ESCRYPT CycurSoC-HSM Security Components

ESCRYPT CycurSoC-TEE Security Components

ESCRYPT CycurSoC – マイクロプロセッサベースの SoC ソリューションをサポート

- HSM コアまたは TEE ホストでのセキュア領域の生成に不可欠なセキュリティ機能を実装
- アプリケーションに暗号化プロトコルとアルゴリズムを提供
- システムアーキテクチャ全体へのスムーズな統合を確保しつつ、自動車メーカーの複雑なセキュリティ要件に効果的に適合
- データと機能の整合性を保持して信頼性、安全性、データ保護を実現
- 自動車メーカーやチップの要件を抽象化し、すべての要件に準拠しながらコスト削減も実現するセキュリティソリューションを提供

暗号機能

- CMAC、HMAC
- ハッシュアルゴリズム
- 鍵導出
- TRNG & PRNG
- デジタル署名アルゴリズム：ECDSA、EdDSA、RSA
- 対称、非対称暗号化
- 認証付き暗号化、復号化
- SHE+ に対応
- 鍵交換アルゴリズム：ECDH、ECDHE、ECBD
- 鍵ラッピング、送信
- 鍵カプセル化メカニズム（KEM）
- 証明書チェーンの保証
- 証明書処理
  - 解析
  - 署名依頼
  - 失効、CRL 処理
  - チェーン検証

HSM とホストコア

- データと鍵を外部フラッシュへセキュアに保管
- セキュアアクセス
- SoC 上の異なるコア間で信頼できるチャネルを確立
- 多数の鍵で E/E アーキテクチャをサポート
- マルチコア CPU のサポート
- 仮想化のサポート
- マルチ CPU ユースケースの対応
- HSM ライフサイクルモード
- 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のサポート
- 署名に基づくトラストアンカー
- 実行時改ざん検知

トラストゾーン

- TEE オペレーティング システムとの統合
- トラストゾーンと SoC 上の他のコアとの間に信頼できるチャネルを確立
- 信頼性のあるアプリケーション（TA）領域と非セキュアな領域をサポートする自動車グレードのセキュリティ機能

ESCRYPT CycurSoC のアドバンテージ

- **ユーザーフレンドリー**
  車載 ECU にシームレスに統合可能
- **迅速**
  POSIX やリアルタイム OS と簡単に統合可能
- **包括的**
  自動車メーカーの車載セキュリティ要件を満たすために必要なすべてのセキュリティ機能をカプセル化
- **品質と信頼性**
  高品質基準（ASPICE、ISO/SAE 21434 CSMS、ISO 26262 ASIL B）に準拠
- **セキュア**
  高性能な暗号化が要求されるユーザー固有の用途向けにハードウェア / ソフトウェア協調設計の強力なプラットフォームを提供
- **柔軟性**
  お客様の特定のニーズを満たす構成が可能

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/CycurSoC

ETAS/COM-JP/03-2023