
プレスリリース

ETAS と Infineon、AURIX マイクロコントローラに実装する ESCRYP T C ycurHSM が NIST の CAVP 認証を取得

- 暗号アルゴリズムの実装品質を検証し、適正な動作を保証
- 要件の厳しい車載アプリケーションに最適

ドイツ、シュトゥットガルトおよびミュンヘン、**2023年11月20日** - ソフトウェアデファインドビークル (SDV) 向けソリューションのリーディングプロバイダーである ETAS GmbH と Infineon Technologies 社 (FSE : IFX / OTCQX : IFNNY) は、このたび暗号アルゴリズムスイートの認証を取得しました。この認証は米国立標準技術研究所 (NIST) の Cryptographic Algorithm Verification Program (CAVP) により検証され、当該スイートの ESCRYP T C ycurHSM における使用を認めたものです。自動車用組み込みセキュリティソフトウェアスタックの C ycurHSM は、Infineon の第2世代 AURIX™ TC3xx ハードウェアセキュリティモジュール (HSM) に実装されています。

CAVP テストプロトコルは国際的に認知された事実上の業界標準であり、米国の暗号標準およびガイドラインの策定を担う連邦政府機関 NIST の規定に準じて暗号アルゴリズムの品質を検証し、適正な動作を保証するために用いられています。この CAVP 認証取得に加え、実装した暗号スイートには独自の検証を実施して、米国連邦政府の暗号ソフトウェア標準である連邦情報処理規格 (FIPS) の認証に必要な要件を満たしていることも確認済みです。

「この CAVP 認証取得により、ETAS と Infineon はお客様にクラス最高のセキュリティソリューションを提供できることが、あらためて立証されました」と、ETAS の Onboard Security Operational Unit の Concept and Delivery Lead を務める Mark Elkins は述べています。「CAVP 認証があれば、世界中の OEM にとって追加のアルゴリズム検証の負担が軽くなり、車両には最先端のセキュリティ製

品だけが搭載されるようになります。」

「CAVP 認証を取得したことで、これまで以上に Infineon の MCU 製品と、当社のパートナーエコシステム内で開発されるソフトウェアソリューションを、お客様に信頼していただくことができます」と、Infineon Technologies、Software, Partnership & Ecosystem Management の Senior Director、Thomas Schneid は語っています。「AURIX には豊富なラインアップが揃っています。絶えず進化する市場において、これこそが厳しい要件に応える最高の車載アプリケーションであるとアピールできるのは、ETAS のようなソリューションプロバイダとのパートナーシップのおかげです。」

自動車用組み込みセキュリティソフトウェアスタックの ESCRYPT CyscurHSM は、セキュリティのためのトラストアンカーを、ハードウェアセキュリティモジュールを用いて車両のマイクロコントローラ (MCU) に実装します。複雑な OEM のセキュリティ要件を満たしやすくし、ドメインコントローラを含むあらゆる車載エレクトロニクス制御ユニット (ECU) に搭載できます。ESCRYPT CyscurHSM はすべての AUTOSAR スタックやブートローダにスムーズに統合可能で、非 AUTOSAR システムにも有効です。

Infineon の第 2 世代 AURIX TC3xx HSM は、AURIX TC3xx MCU ファミリーの全バリエーション向けに用意されているため、ESCRYPT CyscurHSM の CAVP 検証は AURIX TC3xx ファミリー全体に適用されます。したがって、AURIX TC3xx HSM は CAVP 検証済み暗号アルゴリズムの実装に完全対応しています。

ETAS について

1994 年に設立された ETAS GmbH は、ボッシュ・グループの完全子会社であり、欧州、北米、南米、アジアの 12 カ国に海外営業拠点を展開しています。ETAS のポートフォリオには、ソフトウェアデファインドビークルを実現するための車載用ベーシックソフトウェア、ミドルウェア、開発ツール、クラウドベースのサービス、サイバーセキュリティソリューションおよびエンドツーエンドのエンジニアリング/コンサルティングサービスが含まれます。弊社の製品ソリューションとサービスにより、自動車メーカーやサプライヤーは、自社の独自性を活かした車両ソフトウェアを効率よく開発、運用、保護することができます。

さらに詳しい情報は www.etas.com を参照してください。

Infineon について

インフィニオン テクノロジーズは、パワーシステムと IoT における半導体分野のグローバルリーダーであり、製品とソリューションを通じて、脱炭素化とデジタル化を推進しています。全世界で約 58,600 人の従業員を擁し、2023 年会計度 (2022 年 10 月～2023 年 9 月) の売上高は約 163 億ユーロです。ドイツではフランクフルト証券取引所 (銘柄コード : IFX)、米国では店頭取引市場の OTCQX (銘柄コード : IFNNY) に上場しています。

図 :



(テーマ画像 : ハードウェアセキュリティモジュールセキュリティ) ©ETAS



(画像 : Mark Elkins, ETAS) © ETAS



(画像 : Thomas Schneid, Infineon) © Infineon