ECU 量産時のセキュリティ

Security in ECU Production

執筆者

Norbert Bißmeyer
ESCRYPT GmbH
（ドイツ、ボーフム）

セキュリティエンジニア ESCRYPT 社は ETAS GmbH の 100%子会社です。組み込みシステム向けのセキュリティソリューションを提供しています。

プロダクションキーサーバーによるセキュアな鍵管理

暗号化はインターネットに接続している組み込みシステムを攻撃や不正アクセスから保護します。しかし、鍵の可用性とセキュアなインジェクション（投入）を保証することは、特にグローバルな量産チェーンでは難しい問題です。ECU 量産について最大限のセキュリティを確保するために、ESCRYPT は新たにプロダクションキーサーバー（PKS）を提供しています。簡単に実装できて拡張性に優れたこのソリューションは、ESCRYPT の鍵管理ソリューション（KMS）を補完し、極秘の暗号データをシステムのライフサイクル全体にわたって確実に保護します。

組み込みシステムが担う機能は増加の一途をたどっています。その最たる例として、自動車には多くの ECU が使用されていて、そのソフトウェアが増大するパワートレイン、安全、利便性の機能をうまく連携させています。これまでは、自動車の IT システムは孤立化し、それぞれ独立していました。今こそ、外のデジタル世界との接続性を確保して、Car-to-X 通信、つまり無線通信によるファームウェア更新（Firmware-over-the-Air、FOTA）のセキュリティとサービスの可能性を生かすときです。

システムを外部に開放すると、いろいろなチャンスが広がりますが、同時に新たなセキュリティリスクも抱えることになります。自動車の組み込みシステムの保護を確実に行えないと、それらが過失や故意により改ざんされる可能性が生まれてしまいます。デジタルデータの交換は、必ず暗号鍵と証明書による適切な認証に基づいて許可されなければなりません。しかし、量産時にこれらの鍵と証明書を提供して実装し、さらに保護対象製品の耐用期間全体にわたって管理することは、特に拠点が世界中に分散している製造・サプライチェーンや多種多様なサプライヤ構造で成り立っている自動車産業などのような事業分野では非常に困難です。

分散型または集中型の鍵プロビジョニング

今日まで、アプローチには暗号データ（鍵や証明書など）のプロビジョニングの分散と中央の拠点からの管理が並行して用いられてきましたが、どちらのソリューションも完璧ではありません。製造現場ごとに切り離されて実施される分散型ソリューションには、実装が容易なうえ、上位の IT システムとは無関係に管理できるという長所があります。しかも、鍵の可用性が高く、現地のインターネット接続の品質に左右されることはありません。しかし、分散型ソリューションではセキュリティやメンテナンスのためのオーバーヘッドが大きくなります。また、メーカーのプラントで生成される鍵とサプライヤにより生成される鍵がそれぞれ使用されている場合、鍵生成や配布の概要を把握することは特に困難です。一方、集中型ソリューションは鍵管理とセキュリティの面では有利ですが、インターネットの接続障害が発生した場合や転送速度が最適に及ばない場合は、鍵のインジェクション（投入）を行うときの待ち時間が長くなり、遅延や製造休止時間さえ発生してしまう可能性があります。

解決策：分散型のサーバーと集中型のバックエンド

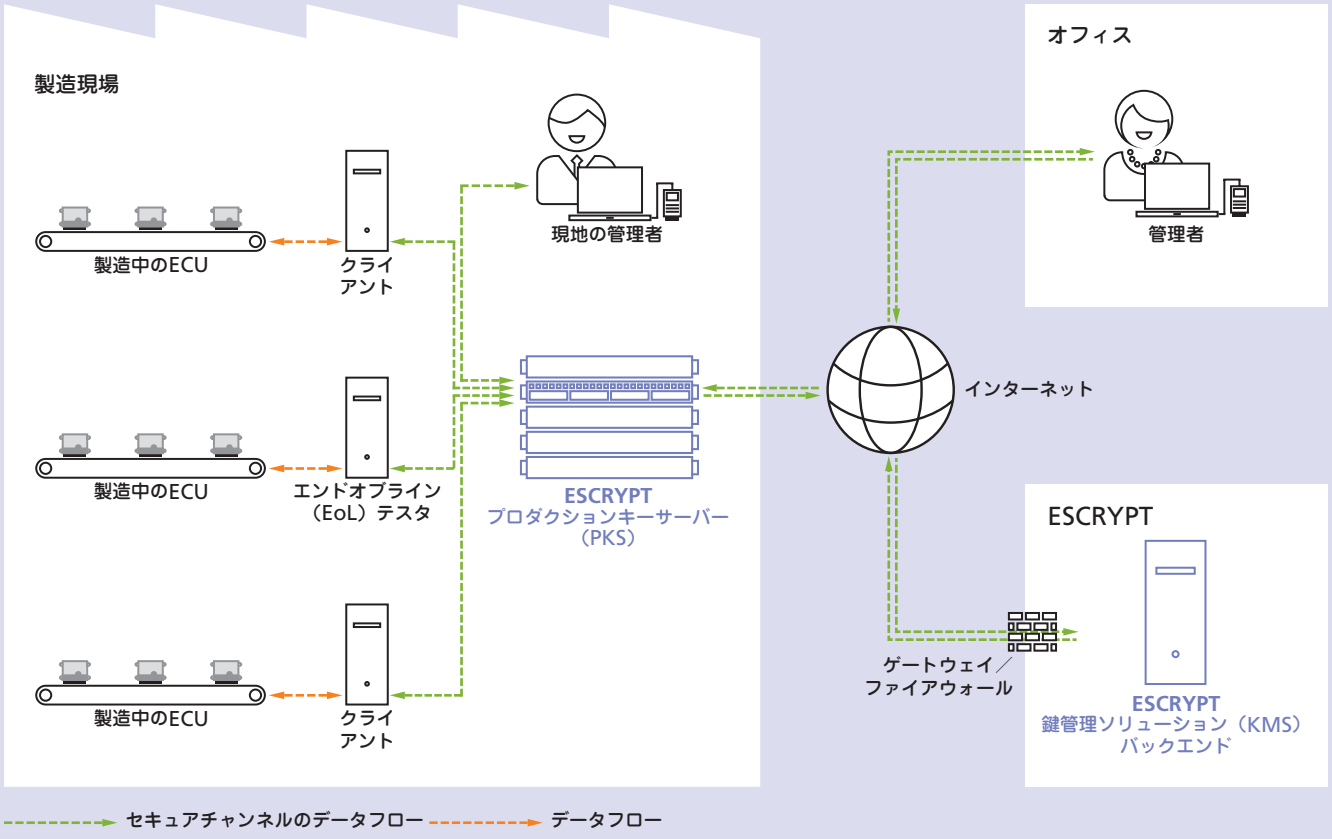
ESCRYPT は、集中型のバックエンド（鍵管理ソリューション（KMS））と、各プラント内のプロダクションキーサーバー（PKS）で行われる分散型キーインジェクションを組み合わせた第 3 のアプローチを採用しています。このアプローチでは、最大可用性と低遅延が実現できるだけでなく、産業用途に最適な高性能のハードウェアセキュリティモジュール（HSM）と適切なセキュリティソフトウェアが各 PKS を不正アクセスから保護するので、暗号データを最適に保護することができます。しかも、このアプローチでは PKS はバックエンドと（データ同期化と更新実行のために）頻繁に通信しないので、インターネット接続からの独立性を最大限保つことができます。この通信の頻度は調整可能です。

PKS はサーバーラック用に標準化されたモジュールであり、独自の電源接続、ギガビットイーサネットインターフェース、HSM を備え、ESCRYPT ソフトウェアがプレインストールされています。一度設定するだけで、すぐに使えます。メンテナンスと管理は KMS バックエンドを通じてオンラインで行うことができます。必要に応じて、証明書の期限切れ、鍵を使った認証、データベースのログ溢れ、あるいはローカルバッファ内の暗号データの不足などといったクリティカルなイベントを、PKS から、たとえばメールで自動的にレポートすることができます。

PKS が世界中の製造現場に分散している場合、鍵割り当ての管理と監視、および PKS の運用と設定は、集中型の KMS バックエンドで行われます。量産時に他のソースからの暗号データを使用する場合は、そのデータを KMS バックエンドに手動でインポートできます。またこれ以外の方法として、認証を通じて KMS に直接接続できる他社製のバックエンドを使用して適切な暗号化されたデータをやりとりすることも可能です。PKS と KMS バックエンドは指定された間隔で同期するので、ECU メーカーは、暗号データ用に十分なバッファを作成することにより、KMS にアクセスするときのインターネット接続の安定性に影響を与えることはほとんどありません。

このフレキシブルなアーキテクチャにより、メーカーは鍵管理に対する自らの運用管理を維持することも、あるいは ESCRYPT に鍵管理を実行させることもできます。どちらの場合も、KMS と分散型サーバーの接続が強力な基礎となり、その上で複雑な暗号化動作を PKS ハードウェアが高速で確実に実行できます。また、複数の PKS をクラスタ化して使用することもできます。重要な点は、クラスタ化された PKS が、適正水準のセキュリティの確保が肝要な量産環境において、最大限の保護を実現し、知的財産窃盗に対しても最大限の防護を行うことです。機密データ（認定された取引先用の暗号鍵など）は HSM に格納されていて、それらを取得するためには KMS 上のあらかじめ決められたルーチンと認証を経由しなければならないようになっているので、たとえ PKS ハードウェアがすべて盗まれても、データにアクセスされることは絶対にありません。しかも、HSM はシステムにインストールされている暗号データ用の金庫としての役割を果たし、システム起動時に追加の暗号化とセキュリティチェックを通じて、データを保護します。これらすべてに加えて、ファイアウォール、暗号化、改ざん防止ソフトウェア、および HSM ベースのセキュリティ処理が、サーバー、バックエンド、およびプロセスに関与している他のすべての受信者とのデータ交換におけ

プロダクションキーサーバー（PKS）
鍵／証明書のインジェクション



る各ステップを保護します。

全体論的なセキュリティソリューションが必要

セキュリティに関するこれらの予防措置と非常に高度なアーキテクチャにより、自動車産業における典型的な使用事例（マイクロコントローラのセキュアブート、診断インターフェースのロック、セキュアハードウェアエクステンション（SHE）鍵やトランスポートレイヤセキュリティ（TLS）証明書のインジェクションなど）は、将来増えてくるコネクテッドカーでもセキュリティを確保することができます。また、この方法は、将来のCar-to-X（車とモノ）通信の保護や、試験者自身の認証が要求されるECUの最終テストにも応用できます。こうして実現されるセキュリティは、組み込みセキュリティに関するESCRYPTの全体論的アプローチにより、自動車のライフサイクル全体にわたって維持できます。PKSはECU量産時の暗号データの管理とインジェクションのセキュリティを確保しますが、組み込みシステムは自動車のライフサイクル全体にわたって過失や故意の改ざんが行われないように保護されなければなりません。ESCRYPTは、自動車廃棄後に鍵と証明書を確実に削除するなど、自動車のライフサイクルの全段階に適したセキュリティソリューションと必要な専門知識を有しています。

ECUのセキュアで分散した製造現場を実現するためのフレキシブルなソリューションアーキテクチャが、最大限の可用性、短い待ち時間、そして使用される暗号データの最適な保護をお約束します。