ECU へのデジタルな予防接種

ネットワーク接続を備えた車両の IT セキュリティの確立は、ECU 製造現場から既に始まっています

セキュアなデータ交換に必要な暗号鍵マテリアルを安全かつ要件に沿って ECU に導入するにはどのようにすればよいのでしょうか？中央鍵管理バックエンドと分散型プロダクションキーサーバーで構成された統合ソリューションは、その答えとなります。

車両の制御ユニットは、サイバー攻撃に対する防御という点では文字通り重要な役割を果たします（暗号鍵を使用するだけでは、ECU が自らを認証し、電気システム内のデータ交換を外部の世界と同様に承認するだけに過ぎません）。ただし、ここで特に課題となるのは、さまざまな車両プラットフォーム向けの ECU はそれぞれ、OEM メーカー固有の鍵マテリアルと証明書を事前に実装しておく必要があるということです（ECU 製造メーカーが ECU を製造する際に供給されていれば理想的です）。

OEM メーカーの鍵マテリアルのセキュアな配布

この場合、中央バックエンドとしての標準的な鍵管理ソリューション（KMS）と、製造施設に設置された KMS と通信するための分散型プロダクションキーサーバー（PKS）を結合すると、効果的なソリューションが実現します。これは OEM メーカーにとって大きなメリットがあります。なぜなら、OEM メーカー固有の ECU に自社の鍵マテリアルを書き込むプロセスを、ECU サプライヤの既存の生産インフラで完全に行えるようになるからです。

このソリューションではまず、個々の自動車メーカーによって提供される鍵マテリアルを含んだデータパケットが KMS に送信されます。鍵マテリアルは中央に保存され、必要に応じて各製造現場にセキュアにデータ転送され、すぐに使用できる状態でプロダクションキーサーバーに保存されます（図 1）。

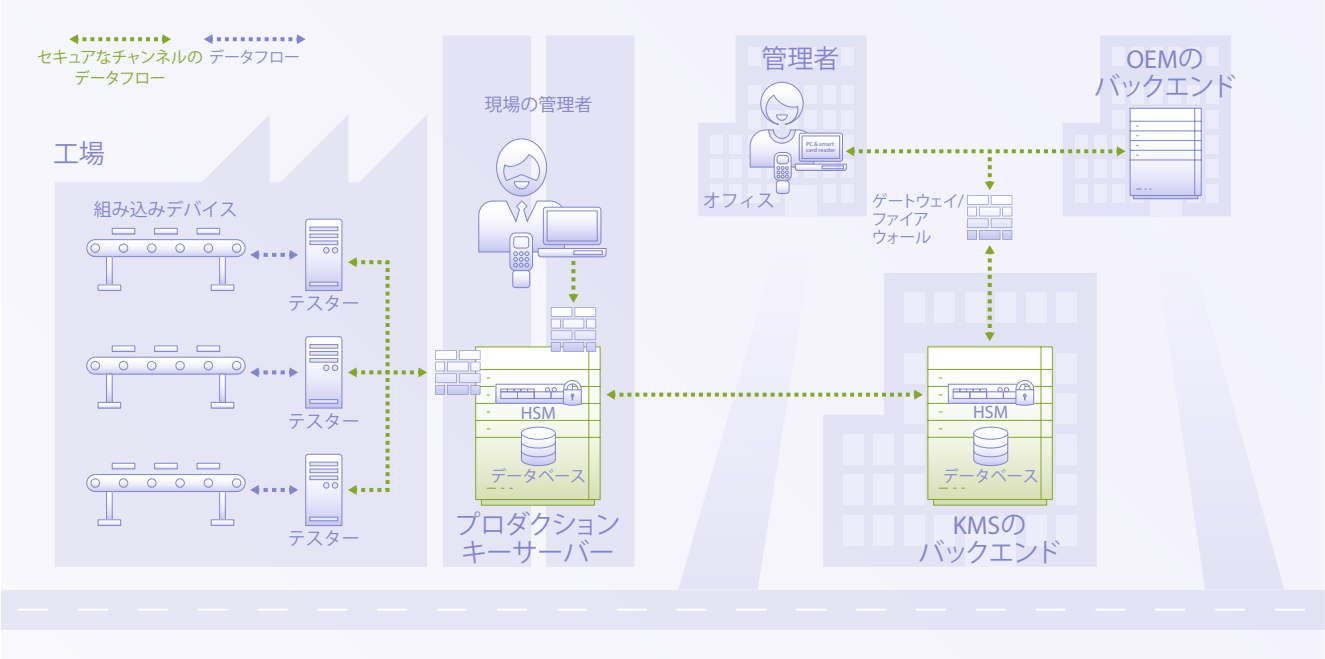

図 1：KMS（鍵管理ソリューション）とプロダクションキーサーバーによる鍵配布および書き込みの統合

生産ライン検査システム（EOL）経由の鍵の書き込み

鍵マテリアルは、接続された生産ライン検査システムによって、ECU の製造時に現場で書き込まれます。これらの鍵マテリアルは次に、プラントのプロダクションキーサーバーから個々の鍵パッケージを読み出し、それを「デジタル予防接種」のように、製造時点で個々の ECU に「注入」します。それと同時に、PKS はどの暗号鍵がどの ECU に書き込まれたかを記録します。最後に、PKS は要求に応じて、製造現場から中央 KMS バックエンド経由で OEM メーカーに検証ファイルを返送します。これにより、自動車メーカーは ECU に鍵マテリアルが正しく書き込まれたことを確認することができます。

このソリューションでは、セキュリティと可用性を共に高く維持できます。

常時接続をしないセキュアなストレージ

このソリューションの特別なメリットは、セキュリティと可用性を共に高く維持できるという点にあります。プロダクションキーサーバーは、堅牢で強力なハードウェアセキュリティモジュール（HSM）とサーバー自体のセキュリティソフトウェアの両方によって不正アクセスから保護されています。また、PKS は、データの同期化やアップデートを行う場合、および暗号データに十分なバッファを作成する場合にのみバックエンドと接続します。これは、PKS がインターネットへの常時接続に依存していないことを意味し、潜在的なオンライン攻撃に対して高い耐性があることを示しています。

ユーザーは、必要に応じて KMS バックエンドとの接続頻度を自由に決定することができます。ストックがあらかじめ指定された最小数を下回っている場合は、新しい鍵がサーバーから自動的に要求されます。これによって、生産時に ECU に書き込むうえで十分な鍵マテリアルが常に使用可能となり、潜在的なコスト要因であるネットワーク接続の中断による生産停止を防止することができます。プロダクションキーサーバーは常時動作します。

世界中の ECU 製造現場で使用

ほぼすべての車載 IT セキュリティ機能の基礎は、ECU データに暗号鍵をセキュアかつ正確に割り当てることです。KMS-PKS 統合ソリューションを使用すれば、セキュアな鍵管理から、セキュアなストレージ、鍵マテリアルの ECU への書き込み、記録および検証に至るまで、複雑な暗号マテリアルの配布メカニズムを OEM メーカーが適切に制御できるようになります。このプロセスが世界中の多くの自動車メーカーの ECU 製造に使用されているのはそのためなのです。■

執筆者

Christian Wecker、ESCRYPT PKS 製品マネージャ
Michael Lueke、ESCRYPT KMS シニアプログラムマネージャ