

PrimeKeyとタレス、未来の電気自動車と自動運転を推進する輸送機器メーカーにセキュリティソリューションを提供

背景

トラックやバスなどの商用車を製造する大手メーカーは、フリートマネジメント用のオンデマンドセキュリティソリューションを探していました。この革新的な企業は、近い将来の電気トラックと自動運転トラックに必要な基盤を構築し、車両を接続して安全な通信とOTA (Over The Air: 無線) アップデートを実現することを目指していました。また、社内のセキュリティポリシーにより車両にデジタル証明書を搭載する必要があるため、信頼できるPKI環境の導入を検討していました。

将来を見据えた組織として同社は、暗号化の俊敏性を個人ID、ドキュメント署名、V2Xソリューションなどの他のユースケースに拡張できるスケーラブルなセキュリティ投資を求めています。運輸業の、特にデジタル化と自動化の進歩に伴い、同メーカーのセキュリティソリューションは、動的に変化する環境への適応に必要な柔軟性を提供することが不可欠でした。

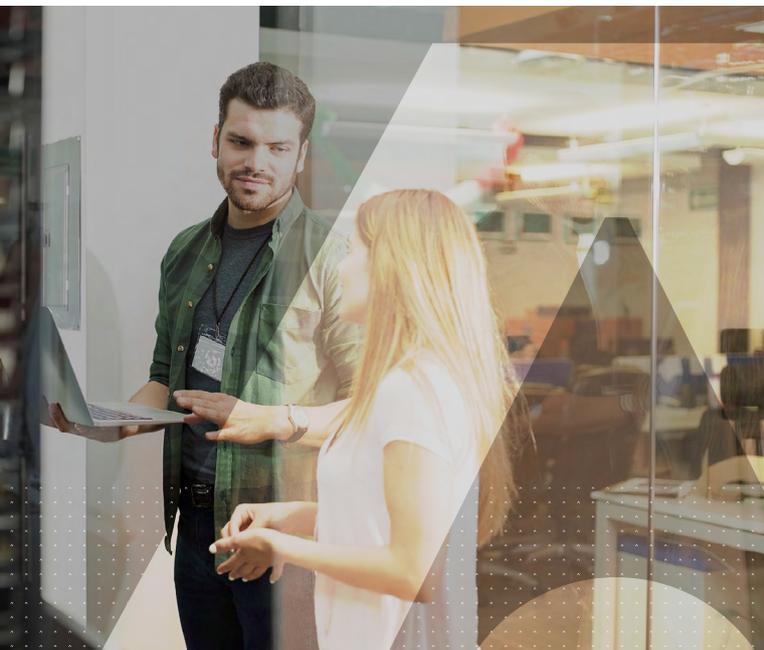
顧客ニーズ

同メーカーは、新世代の電気自動車と自動運転トラックに取り組んでおり、新しい環境をサポートするための証明書ベースのセキュリティソリューションを必要としていました。当初はオンプレミスのPKIソリューション用にHSMを購入することを検討し、サードパーティのホスティングサービスも評価しましたが、迅速に実装でき、先行投資や社内でのハードウェア管理を

必要としないクラウドベースのPKIホスティングおよび証明書ソリューションを望んでいました。

同メーカーはディーゼルエンジンを搭載した車両からバッテリーとソフトウェアを搭載した車両に変更していたため、まったく新しいシステムを実装するという課題を抱えていました。すべての車両に安全なIDを提供できる証明書ベースのソリューションが必要でした。組織のIT部門が、開発部門のPKIの管理とホスティングを担当すれば、開発者はIT部門に証明書を簡単に要求できるようになります。

同メーカーの要件の1つは、PKI展開の最初のユースケースとなる、OTAアップデートを実行できるようにすることでした。テスラ以外のほとんどの車はソフトウェアアップデートのためにディーラーへの持ち込みが必要になりますが、メーカーが望んでいるのは、車両がある現場でアップデートを実行できるようになることです。車両との長距離通信を行うために、車両ごとに安全なIDを用意する必要があります。また、車両で作業する人や、遠隔操作でアップデートを送信する人は、証明書ベースのアクセスを利用する必要があります。これは、GPSやインフォテインメントなどのサードパーティベンダーや車両の機能強化にも当てはまります。すべてが証明書ベースです。メーカーの承認なしに車両に接続することはできません。最終的に、フリート内の各車両にはメーカーが発行したIDが付与されるため、ドライバー、ローダー、整備士などは、証明書ベースのIDなしで乗車することができなくなります。



ソリューション

同メーカーは、認証局としてPrimeKeyのEJBCA Cloudと、PKIの信頼の基点としてThales Data Protection on Demand (DPoD) のLuna Cloud HSMサービスを組み合わせたソリューションを選択しました。IT部門がホストされたPKIを提供するため、エンジニアリングチームは証明書を要求してライフサイクル全体を通じて簡単かつ効果的に証明書を管理できます。

PrimeKeyのクラウドIaaSベースの認証局を利用する後押しになった主な要因は、迅速な市場投入、コスト、および利便性でした。IaaS証明書サービスを提供する他のソリューションも評価しましたが、それらは証明書ごとに価格設定されていました。証明書ごとのモデルでは、各車両や、メカニック、ドライバー、ローダーなどの信頼チェーンに沿って、コストが大幅に増えたり、予算計画の課題が生じたりする可能性があります。比較すると、認証局をクラウドIaaSとして利用する方が、必要な証明書の量を評価したときに理にかなっていました。また、IT部門に証明書を発行させることで、プロセスがより迅速かつ容易になりました。Thales Data Protection on Demand (DPoD)のLuna Cloud HSMを信頼の基点として利用することにより、PKIのセキュリティに疑問の余地はありません。

新しいPKIサービスのメリット

同メーカーは、スマートでエネルギー効率の高い車両フリートを導入する積極的な計画を展開している最中ですが、すでにタレスとPrimeKeyの共同ソリューションによるメリットを経験しています。

- 迅速に実装できる簡素化されたクラウドソリューション
- 予算設定しやすい予測可能なコスト
- 手間のかからない本番環境を保証する強固な技術と高可用性導入
- タレスとPrimeKeyがホストするLuna HSMとPKIサービスは、初期費用やハードウェア管理が不要
- PKIとHSMはどちらもクラウドからオンプレミスソリューションに移行可能であるため、固定されることなく柔軟性を維持
- 統合ソリューションなので、メーカーが複数のベンダーと連携する必要がなく、1つのサプライヤーが実装全体を通じてサポート

次のステップ

同社は、ライフサイクル全体にわたって全車両に必須の安全な証明書を備え、世界140か国にフリートを展開することを計画しています。

PrimeKeyについて

PrimeKeyは、世界をリードするPKIおよび署名ソリューションプロバイダーの1つであり、EJBCA® Enterprise、SignServer Enterprise、PKI Appliance、PrimeKey SEE、Identity Authority Managerなど、多くの革新的な製品を開発してきました。

PrimeKeyは、オープンソースのセキュリティソフトウェアのパイオニアとして、グローバルな企業や組織に、e-ID、e-パスポート、認証、デジタル署名、統合デジタルアイデンティティ、検証などの極めて重要なセキュリティソリューションを実装する機能を提供しています。PrimeKeyの製品は、コモンクライテリアおよびFIPSの認定を取得しており、同社の内部プロセスはISO 9001、14001、および27001の認定を取得しています。同社は、Webtrust/ETSIおよびeIDASの監査を受けた多数の顧客を有しています。

タレスについて

皆様がプライバシー保護を信頼して任せている相手は、そのデータを保護するためにタレスに頼っています。データセキュリティに関しては、組織が直面する決定的な局面は次々と増え続けています。その局面が暗号化戦略の策定、クラウドへの移行、コンプライアンス要件の順守のいずれであっても、デジタルトランスフォーメーションを保護するためにタレスに頼ることができます。

決断の瞬間のための、確実なテクノロジー。