ケーススタディ

digicert

ゼロックス、DIGICERT TRUSTCORE SDKを使用してセキュリティとコンプライアンスを強化

概要

企業名: Xerox（ゼロックス）
業種: 製造業
本社: コネチカット州ノーウォーク

主なビジネス要件:

- 複合機のセキュリティ管理の効率化
- サードパーティのアプリ開発や相互運用性に影響を与えない、OpenSSLの安全な代替手段
- FIPS 140-3規格に確実に準拠し、政府機関やその他の高度なセキュリティの遵守

ソリューション:

- DigiCert TrustCore SDK

主な特長:

- SDKライブラリにより、複合機を悪意を持った攻撃者の侵入を保護するため実装された組み込みTPMチップの管理とセキュリティが簡素化される。
- エンジニアは、アプリケーションを再コード化することなく、サポート・セキュリティ・コンプライアンス・ロードマップ管理・知的財産といったメリットを享受しつつ、複数のデバイス環境で安全でないOpenSSLライブラリからアプリケーションを移行することができる。
- FIPS 140-2/3認証を取得したライブラリは、ソフトウェアとハードウェアのセキュリティ標準への準拠を合理化し、維持する。

要件

ゼロックス複合機の業界最高レベルのセキュリティと機能性を確保

複合機のリーディング・プロバイダーであるゼロックスは、複合機内部に最高レベルのセキュリティを実装すると同時に、顧客が電子文書を利用したさまざまなワークフローを構築するために多様な機能を提供するという、一見相反する2つの目的を継続的に達成しなければならない。しかも、それはゼロックスの技術者、顧客、サードパーティのアプリケーション開発者のセキュリティ管理を複雑にしない方法で行う必要があった。

ゼロックスの主席エンジニアであるマーク・ロカス氏は、「私たちは顧客に対し、私たちのデバイスの悪用やデバイスに起因したデータの損失、その他の問題が起きないようにする大きな責任を負っている」と語る。「しかし、顧客に余計な仕事を増やしたり、セキュリティ管理のために技術者を現地で必要とするような状況にはしたくない。電球を交換するために電気技師を呼ぶような例で、電球は10ドルだが、訪問には200ドルかかるのは論外だ。」

必要なレベルのセキュリティを提供するために、ゼロックスの複合機はハードウェアセキュリティモジュール（HSM）として機能するTPM（Trusted Platform Module）2.0チップを内蔵して

「TrustCore SDKは、認証に向けて予測可能なマイルストーンを提供し、他の方法で対処しなければならないかもしれない脆弱性を取り除いてくれます。」

いる。しかし、専門的な暗号の知識がないと管理が複雑である。一方、同社のセキュリティ・スタックの基盤として使われていたOpenSSLは、エクスプロイトに対して脆弱であり、ゼロックスにFIPS 140-2/3のような最新の暗号認証を満たすことができなかった。「政府は、FIPS 140-3に準拠していないデバイスの調達を許可しない。承認されたベンダーのリストに載りたければ、これらの条件を満たさなければならない。」とロカス氏は語る。

しかし、ゼロックスはOpenSSLを単純に破棄して別のプロトコルに切り替えることはできなかった。そのためには大量のコードを書き換える必要があり、同社のエンジニアがそれを実現するのは難しいだろう。さらに、ゼロックスの複合機とやりとりするサードパーティのアプリケーションのほとんどはOpenSSLを使用しており、ゼロックスは、複合機の機能の多くを危険にさらすことなく、開発者が同じことを行うことを当てにすることはできなかった。ゼロックスは、OpenSSLをシームレスに置き換え、同時に最高レベルのセキュリティとデバイスのサポートを提供できるものを必要としていた。

ソリューション

DigiCert TrustCore SDK は、ゼロックスのセキュリティ懸念に対処するための多面的なアプローチを提供

ゼロックスは、DigiCert TrustCore SDKにその解決策を見出した。このSDKは、同社の厳格な基準を満たすように調整された包括的なセキュリティ・スイートである。TrustCore SDKは、多くの要求を実現するための多面的なアプローチを提供し、彼らのエンジニアに、さまざまな環境に対して安全で効率的な実装を行うためのツールを提供した。さらに、TrustCore SDKは、その柔軟でモジュール化されたアーキテクチャにより、ゼロックスのIoTインフラストラクチャの成長に合わせてセキュリティ対策を拡張することを可能にする。

「TrustCore SDKは、認証に向けて予測可能なマイルストーンを提供し、他の方法で対処しなければならないかもしれない脆弱性を取り除いてくれる。また、顧客がセキュリティの負担を負う必要がないため、顧客にとっても私たちにとってもコスト削減となる。また、デジサートとの技術的なパートナーシップは、ロードマップについての会話や、技術標準の方向性についてのサポートも得られる。」とロカス氏は続ける。

OpenSSL に代わり安全な環境を提供

ゼロックスの最大の課題の1つは、既存のセキュリティ・アプリケーションを書き換えることなく、OpenSSLを置き換える方法を見つけ出すことだった。「私たちはソフトウェア・スタックを構築するために大量のオープンソースを使用しており、すべてのオープンソースソフトウェアはOpenSSLテイストで書かれています。しかし、OpenSSLではFIPSの認証はされません。認証されることこそが、ゲームへの切符なのです」とロカス氏は説明する。「そこで、TrustCore SDKがOpenSSLを “偽装 “することで、OpenSSLに依存するすべてのサードパーティアプリケーションが、OpenSSLに依存しないようできないかと考えたのです。」

デジサートは、TrustCore SDKのOpenSSLコネクタをOpenSSLの代替品として構築し、それはロカス氏の期待通りに動作した。OpenSSL コネクタは、最新の規制要件への準拠を保証し、ゼロックスの複合機を通じて送信される文書上のデータを保護し、保存データを保護します。さらに、OpenSSLコネクタにより、ゼロックスは、開発者に新しいライブラリを習得させることなく、OpenSSLベースのサードパーティ開発者アプリケーションのライブラリを維持し、成長させることができる。

「デジサートというFIPS認定を受けるためのパートナーを得た

ことで、オープンソースコミュニティの浮き沈みに対処する必要がなくなり、製品や顧客に影響を与える可能性のある悪用について心配する必要も無くなった」とロカス氏は語る。「移行は従来と同じように行えたので、かなり楽だった。」

TPM鍵の保護とセキュリティを簡素化するAPIの提供

また、TrustCore SDKは、統合済みのAPIを活用することで、複合機を保護するTPM 2.0チップの複雑な管理を抽象化することができる。TrustCore SDKを使用することで、ゼロックスのエンジニアは、TPMの秘密鍵を保護し、ブートシーケンス、ソフトウェアのバージョンチェック、転送中および蓄積中のデータに対するその他の保護をローカルで認証および検証できるようになった。この強化は基本的な保護にとどまらず、各プリンターに高度な暗号化機能と堅牢なデータ完全性対策を導入し、処理されるすべての文書が厳重なセキュリティ下にあることを保証する。

「これらのAPIは、TrustCore SDKが提供する他のセキュリティ・インフラとシームレスに動作するため、開発時間とリソースが軽減される。」とロカス氏。「私たちは、暗号学の博士号を持たずとも、TPM内の秘密鍵を安全に保ち、顧客データを暗号化して保存することができる。当社のデバイスは、TrustCore SDKのおかげで、最近のデジタル環境の課題に対処できるようになった。」

「デジサートというFIPS認定を受けるためのパートナーを得たことで、オープンソースコミュニティの浮き沈みに対処する必要がなくなり、製品や顧客に影響を与える可能性のある悪用について心配する必要もなくなった」

「当社のデバイスは、TrustCore SDKのおかげで、最近のデジタル環境の課題に対処できるようになりました。」

FIPS 140-3準拠への対応を簡単に

さらに、FIPS 140-2/3をはじめとする認証への裏付けにより、ゼロックスはセキュリティの高い政府機関が求めるコンプライアンス・レベルを満たすことができる。「TrustCore SDKのおかげで、コンプライアンス基準を満たし、それを維持するための複雑な機能を、我々の業務のシームレスな側面に変えることができた。」とロカス氏は付け加える。「このレベルの保護とコンプライアンスは、たとえ時間とリソースがあったとしても、社内で構築することは不可能に近かっただろう。」

全体として、TrustCore SDKは、ゼロックスの顧客にセキュリティと俊敏性を提供する能力を加えた。「TrustCore SDKとデジサートとのパートナーシップは、セキュリティとイノベーションのリーダーとしての市場での地位を強化する礎となった。」とロカス氏は結論づける。

DigiCertTrustCore SDKがデバイスのセキュリティとコンプライアンスにどのように革命をもたらし、促進することができるか、当社の営業チーム（ https://www.digicert.com/jp/iot/trust-for-developers）までお問い合わせください。