cpl.thalesgroup.com

THALES
Building a future we can all trust

タレスが、インドネシアの大手フィンテックサービス企業のPCIコンプライアンスを支援

概要

インドネシアのある大手フィンテックサービス企業は、顧客と安全にデータを交換するために、PCI-DSS（Payment Card Industry Data Security Standard）に準拠するデータ保護ソリューションを必要としていました。

組織

インドネシアの大手フィンテックサービス企業は、調査分析ソフトウェアの開発分野で24年の経験を持ちます。資本市場と金融市場での専門知識とソフトウェア開発を組み合わせた製品を提供し、個人投資家やセクター専門家などの幅広いユーザーに対応しています。

同社は、請求書決済アグリゲーター、電子決済プラットフォーム、オンライン決済ソリューションの3つの事業を運営しています。

ビジネスニーズ

同社は、eコマース、銀行、保険の各分野の顧客と安全にデータを交換するために、PCI-DSSに準拠するデータ保護ソリューションを必要としています。監査人は、データを保護するためにPCI-DSSの暗号化および鍵管理要件を満たすよう、FIPS（連邦情報処理標準）140-2検証を義務付けています。

大手フィンテック企業であるためには、各種の認定基準および金融サービスのコンプライアンスに準拠していることが重要です。コンプライアンスに対応できないと、セキュリティインシデントにつながり、その結果データ侵害が発生して高額な罰金が科せられ、ブランドの評判が落ち、ビジネス全体がリスクにさらされる可能性があります。

何よりも重要なのは、顧客のニーズが、より多くのパートナーがサービスを利用し、分析のため機密財務データを処理するようになったとしても、それに応じて拡張し拡大できるソリューションにあることです。

PCI-DSSに準拠していない場合の潜在的な責任

PCI Security Standards Councilによると、準拠していない企業は次の結果に直面する可能性があります。

- 売上の減少
- 新しい決済カードの再発行費用
- 不正行為による損失
- 訴訟費用、和解と判決
- 決済カードを受け入れる機能の終了
- 失業（CISO、CIO、CEO、および従属的な専門職の地位）
- 廃業

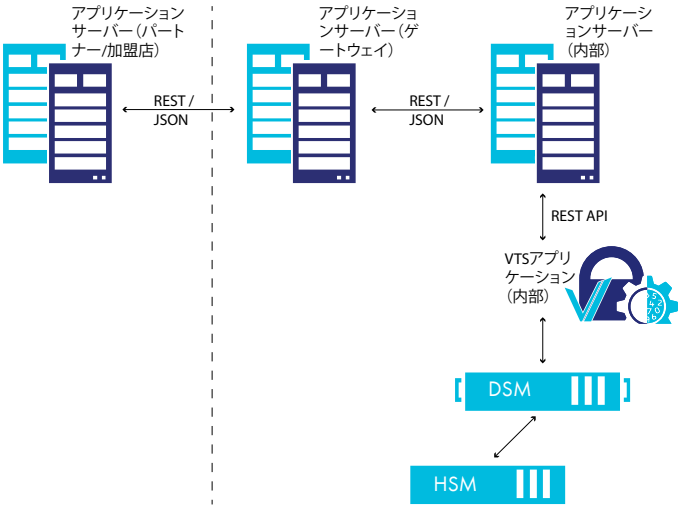
さらに、Ponemon Instituteの2019年「情報漏えい時に発生するコストに関する調査」レポートによると、レコード1件の情報漏えいにつき平均150ドルのコストがかかっています。

ソリューション

フェーズ1の要件は、アプリケーション内データの暗号化サービスを提供するソリューションを展開することです。タレスは、アプリケーションでRest APIを使用して暗号化サービスを呼び出せるCipherTrust Token Server（CTS）の使用を提案します。

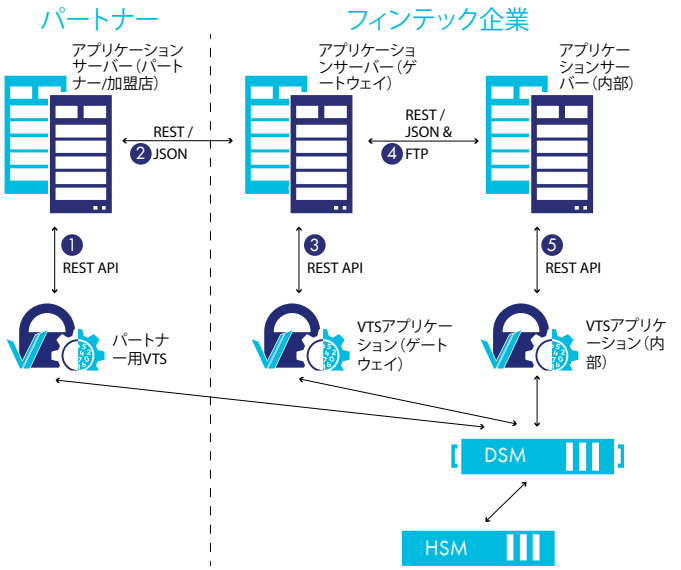
暗号化に使用される鍵は、タレスのCipherTrust Data Security Manager（DSM）内で安全に管理および保護されます。

監査人の要件の一部としてソリューションをFIPS 140-2 Level 3で検証する必要があるため、同社は既存のThales Luna General Purpose Hardware Security Module（GP HSM）をDSMの信頼の基点（Root of Trust）として使用しています。



上図はフェーズ1の展開を示しています

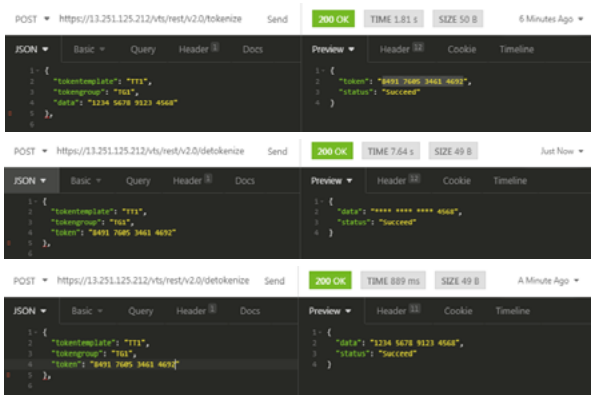
提案した完全なソリューションには、ゲートウェイサーバーから内部サーバーにFTP経由で送信する前に、非構造化データを暗号化する機能があります。



上図はトークン化の全体的なアーキテクチャを示しています

1. トークン化段階: パートナーはデータを送信する前にトークン化します。
2. ゲートウェイサーバーへ: パートナーはトークン化したデータをフィンテック企業のゲートウェイサーバーへ送信します。
3. トークン化解除: フィンテック企業のゲートウェイサーバーは内部処理のためデータを復号化します。
4. 内部サーバーへ: 処理されたデータは、内部サーバーに送信する前に暗号化されます。
5. データ分析段階: 内部サーバーは、分析、処理、保管のためメッセージを復号化します。

*すべての「Vormetric」および「Keysecure」は、2020年9月から「CipherTrust」に名称が変わります。



上図はさまざまなトークン化段階を示しています

コンプライアンス要件の準拠

フィンテック企業にとってコンプライアンスを維持することは、顧客との信頼を構築し維持するための重要なビジネスニーズです。コンプライアンスは、1回限りの年次イベントではありません。コンプライアンスの維持および保持は継続的な課題として扱い、PCIのベストプラクティスに従って規制要件を満たす必要があります。

タレス Data Security Managerの利用

タレス Data Security Manager（DSM）は、すべてのタレス Data Security Platform製品を一元管理する共通環境です。DSMは、ポリシー制御および暗号鍵の安全な管理と保管を提供し、Webベースのコンソール、CLI、SOAP、REST APIを備えています。

トークン化ソリューションの活用

タレス Data Security Managerには、金融サービスを支援するトークン化ソリューションがあります。これはデータ侵害の増加や不正行為事例の増加に対処するための、次に求められるソリューションです。トークン化は、機密データを非機密データに置き換えて、盗まれた場合でも使用不能にすることでデータ自体を保護します。トークン化によって、データは認識不能なトークン形式になりますが、元のデータのフォーマットは保持されます。

金融サービスにおけるマネーロンダリング防止イニシアチブでは、個人を特定できる情報（PII）のプライバシーとセキュリティを維持しながらデータを分析することが必要とされます。

トークン化されたデータは、データベーススキーマを壊すことなく、元のデータの代わりに使用できるため、既存のアプリケーションやシステムを変更したくない組織にとって大きなメリットになります。

タレスのData Security Platformは、シンプルでワンストップの保存データセキュリティソリューションです。

HSMについて

ハードウェアセキュリティモジュール

タレスは、今日の市場で最高レベルのパフォーマンスを備えた、最も安全で統合が容易な、業界をリードするハードウェアセキュリティモジュール（HSM）の製品ファミリーを提供しています。HSMはトラストアンカー（信頼の要）として機能し、データとデジタルアイデンティティを暗号化するマスター鍵を、高保証のFIPS 140-2 Level 3検証済み、耐タンパ性のアプライアンスで保護します。タレスは、次のタイプの専用HSMを提供しています。

汎用HSM

Luna HSMはいくつかのフォームファクタで提供されており、ネットワーク接続型アプライアンス、組み込みPCIモジュール、ポータブルUSBアプライアンスがあります。このHSMは、広範なアプリケーションに簡単に統合でき、一般的な暗号処理の高速化、暗号鍵のライフサイクル保護を実現し、暗号化インフラストラクチャ全体の信頼の基点として機能します。Crypto Command Centerを使用して、オンプレミス、仮想、ハイブリッドクラウド環境の複数のLuna HSM暗号化リソースを一元的に監視および管理することができます。

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。

> cpl.thalesgroup.com <

お問い合わせ先 – cpl.ipsales@thalesgroup.com すべてのオフィスの所在地と連絡先情報につきましては 、cpl.thalesgroup.com/ja/contact-usをご覧ください。