

Identify3D、タレスのクラウドベースのHSMをサービスソリューションとして自社のセキュリティサービスを拡張

デジタルマニファクチャリングの大手ソフトウェアプロバイダーは、顧客IPのセキュリティと製造の品質を確保するために、Thales Data Protection on Demand (DPoD) を選択しました。

組織

カリフォルニア州サンフランシスコを拠点とするIdentify3Dは、デジタルマニファクチャリングにおける不正な配布、改変、複製、生産を防止し、すべての段階で知的財産保護、製造再現性、トレーサビリティを提供しています。同社は、生産基準と製造ルール(機械、消耗品、主要な設定パラメータ)を、生産を行う前の承認と認証が必要な設計に結合することにより、設計の元の品質を維持できるようにしています。

ビジネスニーズ

デジタルマニファクチャリングは増加傾向にあり、サプライチェーンプロセス全体を通して、あらゆる段階でデータを保護する必要があります。しかし、この比較的新しい分野でのセキュリティプロバイダーはほとんどが新興企業です。Identify3Dには、経験豊富なスタッフという大きな差別化要因があり、ビジネスプロセスの不可欠な部分としてセキュリティに重点を置いています。Identify3Dのチームは、セキュリティの世界、特にハードウェアセキュリティモジュール(HSM)に精通しています。

自分たちが担う役割を十分に理解しており、セキュリティを軽視しません。顧客の知的財産を保護することは、この重要な要件に基づいています。Identify3Dは、セキュリティ意識が極めて高い航空宇宙および防衛組織、自動車および医療機器を含む多様な業界のさまざまな製造施設にわたり、世界中に顧客を抱えているため、セキュリティが極めて重要となっています。

最高戦略責任者のステファン・トーマス氏は「セキュリティはすべてにおいて不可欠です。当社の業界の他の企業では、顧客から要求された時にのみセキュリティを追加していますが、当社はそのような方法を取りません。セキュリティから始めます」と述べています。

シニアフィールドアプリケーションエンジニアのダグ・ピーターソン氏は、タレスのHSMをこれまでのプロジェクトで長年使用しており、非常に精通しています。タレスのHSMソリューションは、強力な暗号化と実績のある信頼性をIdentify3Dに提供しています。タレスのDPoDを利用する前、Identify3Dは、自社の鍵を保護するための信頼の基点として、また顧客施設のオンプレミスで、すでにHSMを使用していましたが、HSMアズ・ア・サービスソリューションの提供に向けて拡張したいと考えていました。



信頼の基点に加え、Identify3DはオープンソースのEJBCA認証局を必要としていました。タレスの暗号の俊敏性により、同社は楕円曲線で可能になる小さい鍵サイズを使用することで、業務の迅速化と改善を実現できます。

Identify3Dは、次のユースケースに対する使いやすいクラウドベースのHSMソリューションを探していました。

- 自社の鍵を保持するための認証局
- 顧客の鍵を保持するためのクラウドでの管理コンポーネント



また、同社はオンプレミスの代替案とクラウドベースのオプションも検討しました。評価対象となった他のソリューションは、鍵数へのアクセス制限や鍵ごとの料金請求によって高コストになるため、あまり感銘を受けませんでした。同社の印象に残ったのは、タレスが提供する99.95%のSLAと、成功を収めるためにチームと連携して要件を満たすというタレスの意欲でした。同社は、他の選択肢からは同じ対応力を得られないと確信しました。

ソリューション

Identify3Dは、シンプルなオンラインマーケットプレイスを通じて幅広いCloud HSMと鍵管理サービスを提供するクラウドベースのプラットフォーム、DPoDを選択しました。Cloud HSMサービスには以下が含まれます。

- Luna Cloud HSM—独自のHSMオンデマンドサービスを使用して、アプリケーションや統合要件に対応するように、認定された鍵保管庫(key vault)をセットアップします。
- Luna Cloud HSM for Private Key Protection—認証局に属する秘密鍵を保護して、PKIの信頼の階層構造を確立します。
- Luna Cloud HSM for Digital Signing—ソフトウェアパッケージ、ファームウェアパッケージ、電子文書にデジタル署名し、送信者の真正性を保証します。
- Luna Cloud HSM for Oracle TDE—Oracle TDEデータ暗号鍵がCloud HSMサービス内にあるマスター鍵で暗号化されていることを保証し、最適なパフォーマンスとスケーラビリティを実現します。

Identify3Dは、Cloud HSMサービスを使用して、認定された鍵保管庫(key vault)をセットアップし、鍵を保護および管理しています。

評価

同チームは、Data Protection On Demandの30日間無料トライアルから始めました。クラウド内の鍵ストアおよび認証局(CA)として、DPoDを検証しました。製品をテストしたところ、DPoDがより使いやすくフリクションレスで、顧客環境への統合が容易であることに気づきました。タレスは同チームと緊密に連携し、評価プロセスを経てDPoDにいくつかの重要な改善を行いました。Identify3Dは市場で差別化を図り、暗号の俊敏性の高いソリューションでサービスを向上させており、量子対応ソリューションを含むさらなるユースケースを検討しています。

ピーターソン氏は、「タレスは当社の考えに耳を傾け、強化を図りました。当方が必要としているものに取り組むタレスの意欲は大きなセールスポイントであり、評価対象としていた他のベンダーには類を見ないものでした」と述べています。

評価期間中、タレスはDPoDを強化し、各パーティションに格納できる鍵の数を10から100に増やし、RSA 4096キーのサポートを追加しました。これは、Identify3Dにとって重要な機能であり、決定において不可欠な要素でした。

暗号化の導入と管理、鍵の管理、HSMのホスティングを、オンデマンドでクラウドから行うことには、次のような多くのメリットがあります。

- 先行投資が不要
- クラウドに依存しない
- 5分足らずで稼働
- OpEx(運用費)のみ従量課金
- SLA On Demand - 99.95%の稼働率
- 自動フェイルオーバーを装備
- 鍵のバックアップが自動
- 鍵と暗号化操作のメトリックとレポート
- 柔軟な、自動スケーリング
- 低いTCO
- 比類のない安心

メリット





DPoDの価格体系も選ぶ動機になりました。他のクラウドベースのHSMプロバイダーは、かなりの初期費用を請求し、多くの場合が法外な価格です。Thales DPoDにより、Identify3Dは他のベンダーのソリューションよりも大幅に低いコストで、クラウド内で鍵を移動、保管、管理できるようになりました。また、チームが指摘していたのは、他のベンダーはタレスと同様のサービスを提供していても、アクセスの制限、管理できる鍵数の制御、鍵ごとの料金請求など、より多くの制限があり、すぐに非常に高額になる可能性があるということです。

DPoDのHSMおよび鍵管理サービスは、顧客の要件の変化に応じて自動的にスケールアップおよびスケールダウンします。これもまた、Identify3Dにとって注目に値するメリットでした。

ピーターソン氏は、「多くのクラウドプロバイダーはビジネス上の意思決定を行う際に、顧客として囲い込むことに焦点を合わせ、その後さらに追加のサービスを購入させようとします。タレスは最初からパートナーシップとしてこの件に取り組んでくれました。タレスのソリューションでは、スケーリング、アップグレード、鍵の移動、新たなファームウェア機能の追加、遠隔サポートが容易に行えます」と述べています。

タレスのクラウドプロテクション&ライセンシングについて

今日、企業は重大な決定を下すにあたり、クラウド、データ、ソフトウェアに依存しています。そのため、世界中で高い支持を得ているブランドや大企業は、タレスの製品やサービスを採用することで、クラウドやデータセンターから、デバイスやネットワーク全体に至るまで、データが作成、共有、保存されている場所を問わず、非常に機密性の高い情報やソフトウェアを保護し、セキュアなアクセスを実現しています。当社のソリューションにより、組織は安全にクラウドに移行し、コンプライアンスに自信を持ち、毎日数百万人ものユーザーが使用するデバイスやサービスのソフトウェアからより多くの価値を生み出すことができます。

> cpl.thalesgroup.com <    

お問い合わせ先 - cpl.jsales@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。