DATASHEET

暗号セキュリティプラットフォーム – PKIおよび証明書のライフサイクル管理

オールインワン、コンテナベースのPKI仮想アプライアンスによる簡素化、スケーラブル、安全なPKIおよび証明書ライフサイクル管理（CLM）

課題

拡大し続けるPKIの影響力

過去30年間にわたり、公開鍵インフラストラクチャ（PKI）は進化と拡大を続け、クラウドやエッジネットワークからIoT、個人ID、デジタル署名に至るまで、幅広いアプリケーションで重要な役割を果たしています。

ますます複雑化するユースケースに適応するにつれて、PKIの影響力は拡大し続け、デジタルライフの中心的な構成要素となっています。しかし、PKIの規模が拡大し、その利用が複雑化するにつれて、管理するための明確な所有権と責任の欠如という大きな課題が明かになってきました。

このような新しい状況下でPKIを制御する可視性と理解がなければ、組織はこれまでどおりにセキュリティ体制とインフラストラクチャを維持することが難しくなります。

PKIの導入が多様化、拡大し続けると、別の問題が発生します。これまでの解決策では、組織内に別のCAまたは証明書ソースを追加することがよくありましたが、このアプローチでは証明書が広範囲に拡散し、メンテナンス上の大きな問題と膨大な管理負荷が発生してしまいます。

ソリューション

包括的で簡素化されたPKI

Entrust暗号セキュリティプラットフォーム（CSP）は、包括的で高性能なコンテナベースのPKI、CLM、自動化ソリューションを提供します。安全で量子対応のPKIの実行、幅広いアプリケーションへの導入、そしてオンデマンドでの拡張に必要なすべてのコンポーネントを備えています。

コンプライアンスマネージャーを含むパッケージ済みの仮想アプライアンスとして導入され、PKIとCLMを合理化すると同時に、企業およびクラウド環境全体で拡張できる柔軟性が得られます。

完全なPKIには、公開鍵暗号を総合的に確立・管理するソフトウェア、ポリシー、および手順の統合が含まれます。PKIには、以下の要素がすべて含まれています。

- 安全で量子対応のPKIの実行
- 必要な場所、必要な方法で導入可能
- オンデマンドで拡張

暗号セキュリティプラットフォーム – PKIおよびCLM

PKIとCLMコンポーネントの構成要素

認証局

Entrust暗号セキュリティプラットフォームは、組織全体で信頼できるIDを確保するためのデジタル証明書を発行するための、堅牢で拡張性に優れた安全なソリューションを提供します。仮想環境に導入されるこのアプライアンスは、証明書のライフサイクル管理を効率化し、規制要件へのコンプライアンスをサポートし、安全な通信を確保します。

- DevOpsとマイクロサービス向けのCLM自動化により、エンタープライズPKI導入におけるマルチCAサポートを実現
- 2層のCA階層化
- デュアルCA戦略により、Microsoft CAから最新の適応型エンタープライズPKIへのシームレスな移行を実現
- 証明書失効リスト（CRL）とオンライン証明書ステータスプロトコル（OCSP）をサポートし、リアルタイムの証明書検証を実現
- 外部データベースやハードウェアセキュリティモジュール（HSM）との統合により、秘密鍵のセキュリティが強化され、FIPSなどの業界コンプライアンス標準に準拠

証明書ライフサイクル管理の自動化

高度なレポート機能により、プラットフォームのPKIハブは、組織全体のすべてのユーザとマシンのデジタルIDを複数のCAから検出するのに役立ちます。包括的な自動化機能を備え、シンプルで直感的な「単一画面」による管理を提供します。

- ネットワークスキャンとCAデータベースおよびクラウドサービスからの自動インポートによる証明書の検出
- CAベンダーを問わず、証明書ポリシー、発行、更新、失効を一元管理
- エンドポイント全体で証明書をサーバやMDM等へ送信し、鍵の交換や証明書プロファイルを管理する機能
- 証明書のインポートには下記の方法が利用可能
  - 専用のスキャナー
  - RESTful API
  - 手動アップロード
  - 外部CAのデータベース
- 便利な管理コンソール、レポート、通知
- カスタマイズ可能なロールベースのアクセス制御により、規制遵守、権限分散、責任の移譲に役立ちます。認証タグにより、さらにきめ細かなアクセス制御が可能になります。

暗号セキュリティプラットフォームの詳細は、entrust.com/jaをご覧ください。

ENTRUST
SECURING A WORLD IN MOTION

暗号セキュリティプラットフォーム – PKIおよびCLM

Entrust暗号セキュリティプラットフォーム PKIおよびCLMコンポーネント:

- 認証局
- 証明書ライフサイクル管理の自動化
- 登録サービス
- オンライン証明書ステータスプロトコル（OCSP）
- タイムスタンプ
- RESTful API（Entrust CA Gateway）
- 管理コンソール
- 暗号セキュリティプラットフォーム内で利用可能な追加機能: 鍵とシークレットの管理、ハードウェアによる鍵の保護

導入サービス

自動証明書登録および更新用の弊社の登録機関モジュールは、Microsoft Active Directoryの自動登録と、下記の主要な業界プロトコルをサポートしています。

- Intune MDM
- ACMEv2
- Simple Certificate Enrollment Protocol（SCEP）
- EST
- CPMv2

検証局

アプライアンスに組み込まれた検証局（Validation Authority）は、オンライン証明書ステータスプロトコル（OCSP）を介してリアルタイムの証明書検証を提供します。この検証局はサードパーティCAのステータスチェックをサポートし、以下の機能を備えています。

- デジタル証明書のステータスに関する信頼できる情報
- CRLまたはCAデータベースを使用して、1つまたは複数のCAからの情報を処理

タイムスタンプ

デジタルトランザクションとドキュメントの検証可能なRFC3161準拠のタイムスタンプにより、デジタルIDのセキュリティと信頼性を最大限に高めます。

CAゲートウェイ（RESTful API）

EntrustのRESTful APIは、暗号セキュリティプラットフォームとサードパーティCAに対する完全な証明書ライフサイクル管理、レポート、信頼ポリシー、運用管理を可能にする強力なインターフェイスです。

管理コンソール

すべての暗号セキュリティプラットフォームコンポーネントの導入、構成、監視を一元的に行うインターフェイスにより、IT部門の管理タスクを簡素化・効率化します。

暗号セキュリティプラットフォーム – PKIおよびCLM

主な特長

包括的なテクノロジースタック

Entrust暗号セキュリティプラットフォームは、PKIの設定と管理の複雑さを最小限に抑えます。認証局、自動証明書ライフサイクル管理、登録サービス、オンライン証明書ステータスプロトコル（OCSP）、タイムスタンプ、RESTful API、そしてネットワーク接続型HSMをサポートする管理コンソールを含む、包括的なソフトウェアスタックを備えています。

マルチプラットフォームのサポート

このプラットフォームは、VMware、Hyper-V、クラウドプラットフォームプロバイダー（Azure、AWS）、カーネルベース仮想マシン（KVM）など、あらゆる仮想化プラットフォームと互換性があります。これにより、追加の構成や変更なしに、既存のITインフラストラクチャにシームレスに統合できます。

柔軟かつ迅速な導入

オンプレミスでもクラウドでも、このプラットフォームは多様なIT環境への導入に柔軟に対応します。設定と企業のインフラストラクチャへの統合には、最小限のセットアップ時間しかかかりません。

直感的なユーザインターフェイスで管理を簡素化

単一の統合プラットフォームで、証明書管理とポリシー適用を効率化します。直感的なユーザインターフェイスにより、設定と運用が簡素化されます。

高可用性

プラットフォームのクラスタ構成により、メンテナンス中や予期せぬ障害の発生時でもPKIソリューションの運用が維持され、堅牢な耐障害性と事業継続性が確保されます。

安全性

HSMサポート、OCSP、タイムスタンプなどの統合セキュリティ機能により、証明書とデータの安全性が確保されます。

ENTRUST
SECURING A WORLD IN MOTION

entrust.com/ja エントラストジャパン株式会社｜東京都港区台場2-3-1 トレードピアお台場22階

HSMinfo@entrust.com

CSP-PKI & CLM_20260201