



ENTRUST

Entrust: デジタルビジネスの変革を可能にする、信頼できるIDソリューション

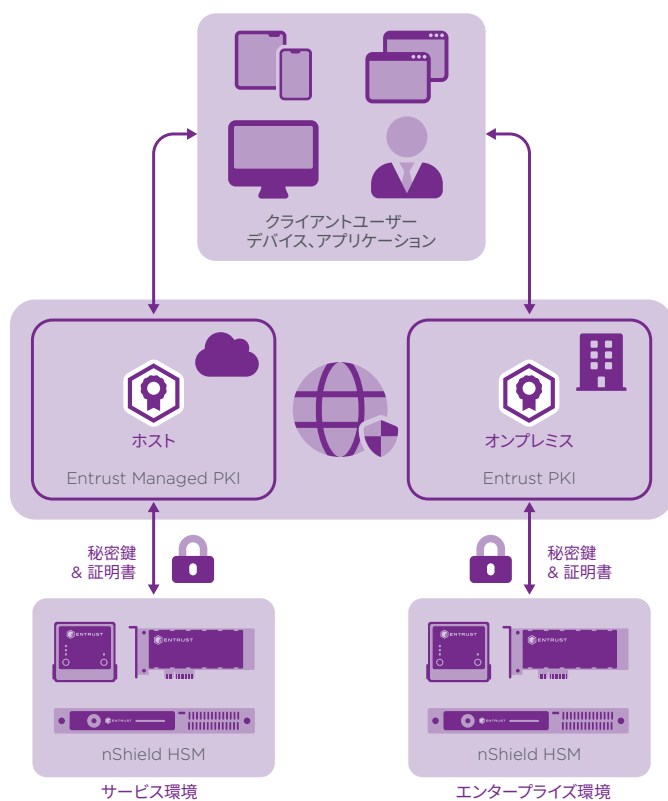
統合ソリューションは、PKI展開のセキュリティを強化します

ハイライト

- エンタープライズアプリケーション全体でユーザーIDを保護する
- オンプレミスおよびホスト型展開のアクセスを制御する
- バックアップ/リカバリを含む証明書のライフサイクルを管理する
- 機密性の高い秘密鍵を保護する信頼の基点を提供する
- FIPSおよびコモンクライテリアの規制コンプライアンスを促進する
- オンプレミス、クラウド、ハイブリッド展開をサポートする

問題: 急速に拡大するエコシステム全体で、信頼できるIDの必要性が高まっている

モノのインターネット (IoT)、モバイルの急増、個人所有デバイスの持ち込み (BYOD) プログラムのデバイス証明書の発行のサポートやIoTネットワークデバイスの登録などの新しい要件の出現により、強力なID管理がこれまで以上に重要になっています。公開鍵基盤 (PKI) ソリューションは、ユーザー、デバイス、アプリケーション、サービスの信頼できるIDを確立して、重要なエンタープライズシステムおよびリソースに安全にアクセスし、安全な環境の重要な要素を提供するのに最適です。



典型的なリモート管理展開で使用されるコンポーネントの概要図

▶ Entrust: デジタルビジネスの変革を可能にする、信頼できるIDソリューション

課題: 認証局 (CA) 鍵の管理を保護する

オンプレミスまたはホストされたPKIによって使用される秘密鍵の強力な保護は、効果的なセキュリティ戦略に不可欠です。PKIの信頼性は、CA階層内の秘密鍵に与えられる保護と関連する検証プロセスに依存します。ソフトウェアに保存および管理されているCA鍵は、セキュリティを損なう可能性のある高度な脅威に対して脆弱である可能性があります。専用のハードウェア鍵管理により、セキュリティが強化され、信頼できるビジネスエコシステムのリスクが低減します。

ソリューション: 強固な信頼の基点を持つ統合ソリューション

Entrust PKIソリューションは、重要なビジネスアプリケーションの証明書ベースのセキュリティを確立および管理します。Entrust Security Managerを使用すると、顧客は独自のデジタル証明書を展開および管理できます。この製品はユーザーを認証し、アクセスを制御し、暗号化アプリケーションを保護します。ハンズオフアプローチを求める顧客に対して、Entrust Managed PKIはホスト型ソリューションを提供します。

Entrust nShield® ハードウェアセキュリティモジュール (HSM) は、Entrust PKI製品と統合して、秘密鍵の機密性と整合性を保護します。オンプレミスまたはホスト型PKIのセキュリティを拡張しようとしている組織は、オンプレミスまたはサービスとしてnShield HSMを使用してEntrustソリューションを展開し、重要な鍵が許可されていない組織に漏洩しないようにすることができます。nShield HSMは、CA秘密鍵を安全に生成、保存、管理します。

nShieldをEntrust Security Manager および Managed PKIと併せて使用する理由は？

ハードウェアルートでの信頼の基点なしでPKIを展開することは可能ですが、認定HSMの暗号化境界外で処理されるCA鍵は、PKI資格情報の発行および証明書失効機能を危険にさらす可能性のある攻撃に対して非常に脆弱です。

HSMの使用は、PKI展開のベストプラクティスと広くみなされており、貴重な暗号化マテリアルを保護するための実証済みの監査可能な方法を提供します。HSMにより、組織は次のことが可能になります。

- 慎重に設計された暗号化境界内でCA鍵を保護し、権限のある組織のみが鍵を使用できるように、職務を強制的に分離した堅牢なアクセス制御メカニズムを採用しています。
- 高度な鍵管理、保管、冗長性機能を使用して可用性を認証し、必要なときに鍵にいつでもアクセスできることを保証する
- 要求が高まるアプリケーションに対応する優れたパフォーマンスを提供する

nShield HSMのEntrust Ready認定は、相互運用性、展開の容易さ、強化されたセキュリティを保証します。

▶ Entrust: デジタルビジネスの変革を可能にする、信頼できるIDソリューション

Entrust nShield HSMは、機密性の高い鍵マテリアルの生成、保護、管理を目的とする高性能の暗号化デバイスです。厳格なセキュリティ基準で認定されたnShield HSMは、以下を行います。

- 鍵を安全で改ざん防止環境に保存する
- 公共部門、金融サービス、企業の規制要件に準拠する
- セキュリティ機能を管理タスクから分離し、セキュリティポリシーを適用
- Support high-performance elliptic curve cryptography (ECC)

Entrustは特定のパフォーマンスと予算のニーズに合わせることができます。

- nShield Edge HSM: 少量のオフラインルートCA構成用のポータブルUSB接続HSM
- nShield Solo +およびSoloXC HSM: サーバーおよびセキュリティアプライアンス用の高性能組み込みPCIe HSM
- nShield Connect +およびConnect XC HSM: 高可用性環境向けの高性能なネットワーク接続HSM
- nShieldアズ・ア・サービス: サブスクリプションベースの高性能オプションにより、柔軟性と費用対効果が向上します

Entrust HSM

Entrust nShield HSMは、最高のパフォーマンスを発揮し、非常に安全で、簡単に統合できるHSMソリューションのひとつであり、規制への準拠を促進すると同時に、企業、金融機関、政府機関に最高レベルのデータセキュリティとアプリケーションセキュリティを提供します。当社独自のSecurity World鍵管理アーキテクチャは、鍵へのアクセスおよび鍵の使用を厳重かつきめ細かく制御します。

詳細

Entrust nShield HSMの詳細については、entrust.com/ja/HSMをご覧ください。アイデンティティ、アクセス、通信、データに関するEntrustのデジタルセキュリティソリューションの詳細については、entrust.com/jaをご覧ください。

Entrust nShield
HSMの詳細はこちら:

HSMinfo@entrust.com
entrust.com/ja/HSM

ENTRUSTについて

Entrust は信頼できる認証、支払い、データ保護を実現することで、動き続ける世界をセキュアにしています。今日、支払いや国際取引、電子政府サービスへのアクセス、そして企業ネットワークへの認証において世界中でより安全で円滑なユーザ体験が求められています。Entrust はこれらの要となる部分において、他に類を見ない幅広いデジタルセキュリティとID発行ソリューションを提供しています。2,500人を超える従業員、グローバルパートナーネットワーク、そして150カ国以上におよぶ顧客に支えられ、世界で最も信頼されている組織から信頼されています。

詳細は下記URLをご覧ください。
entrust.com/ja/HSM

