



ENTRUST

ORCとEntrustによるフェ デレーショングレードの安 全なクラウドサービス



ORCのPIVotal ID™は米国政府が使用するフェデレーションIDソリューションであり、強化された暗号化に支えられたクラウドベースのIDaaS (Identity-as-a-Service) が、強力なセキュリティと幅広い相互運用性をいかに提供するかを示しています。

機密データのクラウドへの移行を検討している多くの企業にとって、セキュリティの問題は依然として重大な懸念事項です。しかし、Operational Research Consultants Inc. (ORC) という1つの企業は、米国連邦政府のようにセキュリティに重点を置く組織にとっても、クラウドはオンプレミス展開と同程度に、またはそれ以上に安全であることを証明しています。

ORC - フェデレーションID管理における先駆者

ORCは、請負業者やサプライヤーとの安全なやり取りをサポートするために、海軍取得公開鍵基盤を立ち上げた1990年代半ばから、米国政府の信頼できるパートナーです。米国政府による情報保証の重視が今後20年間で高まるにつれ、ORCはセキュリティソリューションに関して頼りになるパートナーとして、米国政府に準拠したID管理ソリューションの提供を承認された最初の企業の1つになりました。

現在、ORCは300万を超えるIDを管理し、米国政府とビジネス取引を行っている様々な従業員、請負業者、関係者、退役軍人、市民に1,000万を超える連邦準拠のデジタル証明書を発行しています。

安全で相互運用可能な本人確認と認証の必要性

2004年8月、ブッシュ政権は国土安全保障大統領指令 (HSPD-12) を発行し、連邦の施設と資源を保護するために、安全で信頼できる本人確認に関する政府全体の基準を設定しました。このイニシアチブは、政府職員に単にIDバッジを発行するのではなく、安全な個人資格情報を発行するために必要なプロセス、その発行プロセスと資格情報を検証する方法、資格情報のライフサイクル全体にわたるリスクおよび質の管理に重点を置いています。

個人識別検証 (PIV) プログラムはこのプロセスを実施し、FIPS (連邦情報処理標準) 201はPIVスマートカードのインターフェイスとデータ要素を指定します。PIVカードのデータ要素の中には、1つまたは複数の非対称秘密暗号化鍵があります。部署および機関は、準拠した公開鍵基盤 (PKI) を使用して、ユーザーにデジタル証明書を発行する必要があります。PIVイニシアチブでは、発行された資格情報間のフェデレーション相互運用性をサポートすると同時に、特定の企業・政府間、市民・政府間、市民・企業間の取引をサポートする他の高保証の資格情報も生成しました。これには、次のような様々なPIV-I (相互運用可能PIV) やPIVバリエーションが含まれます: 交通機関職員ID資格情報 (TWIC®)、救急隊員認証資格情報 (FRAC)、商業ID検証 (CIV)、外部認定当局 (ECA) PIV-I。これらは様々な規制要件に対応し、グローバルに拡張できるように構築されています。証明書発行のプロセスとポリシー、重要なルートに提供される保護、そのPKIでの認証局鍵の発行は、システムの全体的な保証レベルにおける重要な要素です。

課題: 認証、相互運用性、信頼

従来のオンプレミスID管理システムは、簡単にクラウドに拡張することはできません。ORCは、クラウドベースのID管理が連邦政府全体で信頼されるためには、セキュリティが重要な差別化要因であることを認識し、高保証の暗号化がNISTのセキュリティ要件を満たす唯一の方法であることがわかっていました。PKIに関しては、これは、ルートおよび発行認証局鍵を生成し、高保証のFIPS認定ハードウェアで保護する必要があることを意味しました。その理由は単に強力なセキュリティを超えるものです。これらの鍵の1つが侵害された場合の運用上の影響は、PKIで発行されたすべての証明書を取消し、すべての資格情報を再発行する必要があるためです。

ORCはまた、Federal Bridge、PIV / PIV-I、DoD、FISMAなどの複数の認証および認定要件と複数レベルで相互認証をサポートする必要性に直面したため、柔軟な範囲の保証レベルおよびポリシーをサポートできるソリューションを必要としました。このソリューションは実証済みであり、幅広い相互運用性を保証するオープンシステム標準に基づく必要もありました。ORCは最終的に、クラウド環境で暗号化サービスに高可用性と信頼性を提供することの重要性を認識しました。

ソリューション: ORC PIVOTAL ID™とENTRUST

連邦政府のクラウドサービスに高レベルの保証を提供するために、ORCはPIVotal ID™と呼ばれる一連のソリューションを提供しています。PIVotal ID™には、連邦政府全体で信頼され、グローバルなフェデレーションが可能な強力なID資格情報を発行する認証・認定管理サービスが含まれています。これには、高保証のEntrust nShield®ハードウェアセキュリティモジュール (HSM) に基づいたPKIからのデジタル証明書の発行が含まれます。ORCは、米国連邦政府機関（一般市民、軍）、その従業員、グローバルな契約コミュニティ、取引パートナー、退役軍人、米国政府や規制業界のいずれかの部分とビジネスを行う必要がある市民のために、安全な取引を可能にする数百万の準拠した資格情報を発行・管理しています。PIVotal ID™には以下が含まれます。

- 個人識別検証 (PIV)
- 非連邦発行体相互運用可能PIV (NFI PIV-I)
- 外部認証局 (ECA)
- 電子サービスアクセス証明書 (ACES)

- TWIC 証明書作成局
- PIVotal Commercial™ (PIV-CIV)
- PIVotal Validation™

ORCは、Entrust nShield HSMが、優れた保護機能と暗号化加速機能に加えて、安全なクラウドサービスインフラストラクチャ内のルート鍵とすべての従属鍵を保護・管理するための柔軟性と拡張性を提供することを評価しました。

強固な暗号化のための費用効果の高いソリューション

Entrust nShield HSMは、暗号化とデジタル署名に使用される秘密鍵を保護・管理する強化された改ざん防止プラットフォーム上に構築されており、ID管理、ウェブサービス、データベース暗号化、トークン化、PKIサービス、強力な認証など、事実上すべてのアプリケーションをサポートします。nShield HSMは、ソフトウェアベースの暗号化によって提供されるセキュリティが不十分であるとみなされるシステムに対して、適切なレベルの物理的および論理的制御を確立するための最も費用効果の高い方法を提供します。

ENTRUST NSHIELD HSMにより、企業は以下のことが可能になります。

- 仮想化環境とクラウド環境で、比類のない運用上の柔軟性、高可用性、拡張性を実現する。
- 法規制の遵守と、バックアップやリモート管理などの日常の主要な管理タスクのコストを削減する。
- 簡素化されたHSM登録、効率的な鍵プロビジョニング、十分に強靱なハードウェア機能により、高保証のビジネス継続性を実現する。
- 改ざん防止ハードウェア内の暗号化鍵および操作を保護することで、重要なアプリケーションのセキュリティを強化する。
- 役割ベースの多要素認証や柔軟なクォーラムベースの認証などの強固な管理ポリシーを通して、業務の厳格な分割と二重制御を確立します。

ORCについて

ORCはWidePoint企業で、米国連邦政府の信頼できるパートナーであり、政府および企業の顧客に情報セキュリティソリューションを提供します。このソリューションは完全に準拠した信頼性の高い情報の交換および保証を確実にします。ORCのソリューションは企業・政府間、政府・政府間、市民・政府間の情報保証および認証サービスのエリートプロバイダーとして、レガシーシステムと相互運用可能であり、市場のすべての主要なソフトウェアアプリケーションとシームレスに統合できます。ORCは、Entrust nShield HSMを利用して、フェデレーショングレードのセキュリティで保護されたクラウドID管理サービスを提供します。

ENTRUSTについて

Entrust は、信頼性の高い本人認証、決済、データ保護を可能にすることにより、世界の動きを安全に維持します。今日、人々はこれまで以上に、国境を越えた移動、買い物、電子政府サービスへのアクセス、企業ネットワークへのログインといったさまざまな場面で、シームレスで安全なユーザー体験を求めています。Entrust は、これらすべてのインタラクションに対応した、他では見られない広範なデジタルセキュリティおよび資格情報発行用ソリューションを提供しています。2,500名以上の従業員とグローバルパートナーのネットワークを備え、150か国以上における顧客から支持されているため、世界における多くの委託組織から信頼を得ていることは不思議ではありません。

詳細は下記URLをご覧ください。
entrust.com/ja/HSM

