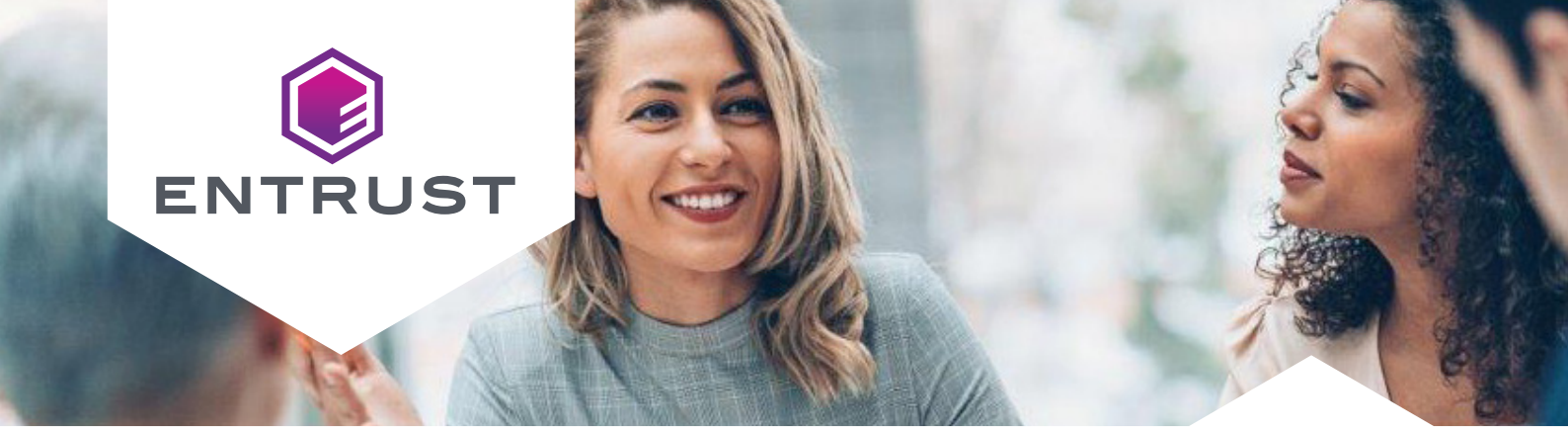


MicrosoftとEntrustは、IoT（モノのインターネット）のセキュリティと信頼を強化します

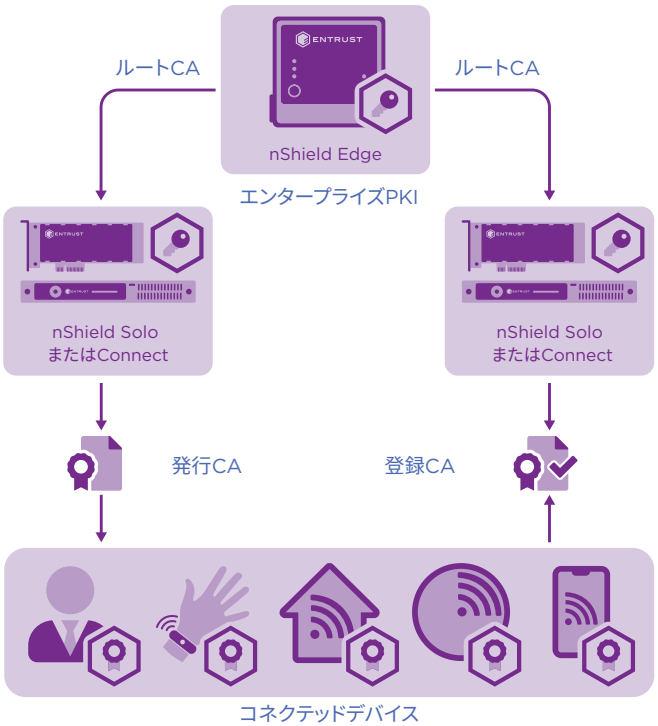
デバイス登録サービスとハードウェアセキュリティモジュールにより、IoTデバイスの安全な登録が可能になります

ハイライト

- ネットワークデバイス証明書の整合性を向上させる
- デバイス登録をサポートするために、既存のPKIの使用を可能にする
- 鍵の安全な保管と管理を提供する
- FIPS140-2レベル3検証済み鍵保護を提供する
- データセキュリティ規制の遵守を促進する

問題：ID確認と認証にデジタル証明書を使用するインターネット接続ネットワークデバイスの数が増加していることも、証明書の登録をサポートする必要がある。

より多くのデバイスがインターネットやエンタープライズネットワークに接続されるにつれて、その識別と認証は非常に重要になります。承認されていないデバイスは、マルウェアをクローズドドメインに導入するためのベクトルを作成し、重大なリスクをもたらす可能性があります。公開鍵基盤（PKI）は、ID確認と認証のためのデバイス資格情報を発行および管理するために使用されますが、信頼できる登録プロセスも実施する必要があります。



Entrust nShield HSMは、エンタープライズPKIルートおよび発行CA鍵だけでなく、証明書の整合性と検証のためにデバイス証明書をCA信頼の基点にバインドするために使用される秘密鍵も保護します。

詳細をチェック：ENTRUST.COM/ja/HSM

MicrosoftとEntrustは、IoT（モノのインターネット）のセキュリティと信頼を強化します

課題：増加するコネクテッドデバイスが、信頼できるドメインベースの資格情報を使用して、証明書を安全に登録できるようにする。

デバイス証明書の発行は、増加する承認されたデバイスが制限されたドメインに接続する安全なネットワーク環境を確立するための最初のステップにすぎません。デバイス接続を検証および制御するには、認証局（CA）による証明書を登録する必要があります。登録プロセスを支える暗鍵を保護および管理することは、システム全体の信頼の基盤を提供するために不可欠です。

ソリューション：MicrosoftとEntrustを一緒に使用すると、コネクテッドデバイス証明書の安全な登録が可能になります。

Microsoft Active Directory証明書サービス（AD CS）の機能の1つとして、ネットワークデバイス登録サービス（NDES）は、コネクテッドデバイスと証明書登録用の登録局（RA）間の通信を定義するSimple Certificate Enrollment Protocol（SCEP）を実装します。Microsoft IntuneやSystem Configuration Managerなどのクラウドベースのオンプレミスソリューションは、NDESを使用して、デバイスをプロビジョニングおよび登録します。NDESは、Windows Serverに接続されているデバイスのデジタルIDを、対応する秘密鍵にバインドすることにより、その登録と検証を可能にします。このサービスは、CAを信頼の基点として使用して、証明書の登録ならびに証明書の真正性および整合性の検証を可能にします。

ファイルにローカルに保存されている鍵を使用してサーバ上で発行プロセスが実行されると、鍵が攻撃を受け、複製、変更、置換に対して脆弱になる可能性があります。Entrust nShieldハードウェアセキュリティモジュール（HSM）は、秘密のNDES鍵を保護することにより、証明書登録プロセスの保証レベルを向上させます。Entrust nShield®HSMは、Microsoft標準の暗号化アプリケーションプログラミングインターフェイス（CAPI）を使用して、Microsoft NDESと統合します。

Entrust HSMをMicrosoft NDESと併せて使用する理由は？

増加するモノのインターネット（IoT）をサポートするために、より多くのコネクテッドデバイスが展開されるにつれて、PKIは、ドメイン全体で発行される証明書のセキュリティを支えるルートCA秘密鍵を保護するだけでなく、これらの増加する証明書の登録も保護することが期待されます。組織のPKIは、秘密鍵を保護するためにHSMを使用せず、証明書を登録および検証するメカニズムを採用していないため、混乱に対して脆弱であり、深刻な結果を招く可能性があります。HSMは、セキュリティが重要な鍵を盗難や誤用から保護し、ライフサイクル全体の管理を可能にする強化された環境を提供し、高可用性のために複数のHSMを使用して、フェイルオーバーをサポートします。Entrust nShield HSMを使用して証明書の発行をIDチェックと承認にバインドし、証明書の登録と検証を制御することは、CAのセキュリティ侵害から学んだ重要な教訓に基づいています。

MicrosoftとEntrustは、IoT（モノのインターネット）のセキュリティと信頼を強化します

FIPS140-2レベル3、Entrust nShield HSMを含む厳格なセキュリティ標準の認定を受けています。

- ルートCAと登録鍵を安全で改ざん防止環境に保存する
- スマートカードベースのポリシーと2要素認証を使用して、管理者アクセスを管理する
- 公共部門、金融サービス、企業の規制要件に準拠する

Entrust HSM

Entrust nShield HSMは、Windows Server 2003 のリリース以降ADCSをサポートしており、幅広いグローバルな顧客ベースに展開されています。NDESのサポートは、このサービスの拡張です。複数のアプリケーションとPKIにおける資格情報の管理を簡素化し、Hyper-Vを含む仮想化環境で動作できます。Entrust nShield HSMは、組織がペイメントカード業界データセキュリティ基準（PCI DSS）などの監査およびコンプライアンス要件を満たすのに役立ち、次のバリエーションで利用できます。

- nShield Edge：オフラインルートCA用のポータブルUSB接続HSM
- nShield Solo+ / Solo XC：サーバ用の組み込み PCI Express高性能HSM
- nShield Connect+ / Connect XC：データセンター用のネットワーク接続された高性能HSM

Microsoft

マイクロソフトは、ビジネスリソースの共有方法、およびIDとアクセス制御の管理方法を変革しました。Microsoft AD CSおよびNDESに基づくシステムは、公開鍵証明書を作成および管理するためのカスタマイズされたサービスを提供して、人とデバイスの間に信頼できるビジネス環境を確立します。Microsoft NDES：

- デバイス証明書をRAにプロビジョニングして登録する
- ドメインベースの資格情報を使用して登録を保護する
- 証明書の検証と失効サービスを可能にする

www.microsoft.com

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

お問い合わせ：
HSMinfo@entrust.com