



ENTRUST

Nexus GO Signingと Entrust Securityで、安全性の 高いデジタル署名を実現



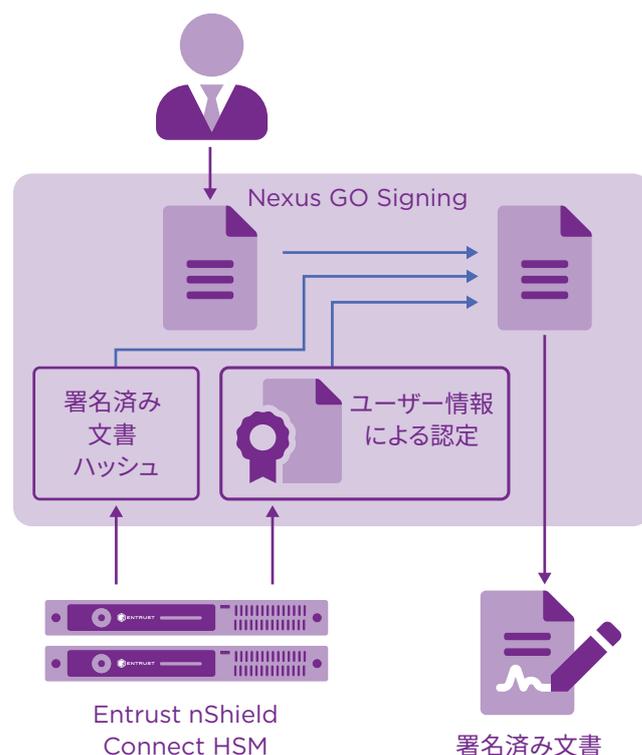
EntrustとNexusが安全性の高いデジタル署名サービスを提供

ハイライト

- 契約書、同意書、その他の重要文書を改ざんから保護
- 文書の信頼できる情報源を保証
- 署名者の信頼できるアイデンティティを確立
- ETSI、eIDAS規則、国家標準化機関の要件に準拠
- 契約書やその他の文書の紙のコピーに基づいて、手動プロセスをデジタル化かつ自動化

問題: 文書への署名に使用される手動プロセスでは、エラーが発生しやすい

デジタル文書は強力なツールですが、簡単に内容を書き換えることができ、情報源を確立することが困難です。契約を含むプロセスなど、文書への署名に使用されるプロセスの多くは、セキュリティ上の理由から依然として手動で行われているのが現状です。



➤ Nexus GO SigningとEntrust で、 安全性の高いデジタル署名を実現

課題: 安全性を損なうことなく、デジタル 文書への署名を実施する

文書への署名は、署名の資格情報が改ざんされることなく、署名者として正しい個人に安全に結び付けられる必要があります。多様な署名の案件に適用できるように、eIDAS、ETSIなどの規則や国が定める要件に準拠するソリューションが必要です。

ソリューション: ハードウェアセキュリ ティモジュール (HSM) を使用した信頼でき る文書署名

Nexus GO Signingは、PAdES、XAdES、eIDAS規則の仕様に従い、PDFやXML文書で高度なデジタル署名を生成します。署名は、文書の内容と署名済みハッシュ値、およびユーザーデータを含む証明書を結び付けることで、署名者を署名の資格情報に関連付けます。

ユーザーは強力な2要素認証を使用して、署名の手順に同意します。その結果、PAdES、XAdES、eIDAS規則に準拠し、編集できないようにロックされ、署名と署名証明書が挿入された文書が作成されます。複数のユーザーが同一の文書に署名できます。

nShieldのHSMとNexus GO Signing を併せて使用する理由は？

Entrust nShield Connect HSMは、Nexus GO Signing およびNexusのCA 認証局)と統合し、包括的、論理的、物理的に鍵を保護します。また、これらを組み合わせることで、セキュリティポリシーを実施するための監査可能な方法を提供します。

HSMは、署名の資格情報の整合性を維持するために使用されます。署名に使用される暗号化鍵を処理すると同時に、ユーザーを署名鍵に関連付ける証明書を発行する際の信頼の基点となります。

HSMで署名の資格情報と証明書の発行を処理することにより、重要な鍵を損なう可能性がある攻撃に対して、ソリューションの抵抗力が大幅に強化されます。HSMは、暗号化された重要なデータを保護することが実証済みで監査可能な唯一の方法です。

Entrust nShield Connect HSMを使用することで、Nexusサービスの利用者は以下が可能になります。

- 厳重なアクセス制御メカニズムを用いて慎重に設計された暗号境界内で鍵を保護し、鍵が許可された目的にのみ使用されるようにする
- RSAやECCアルゴリズムを含む、要求の多いワンタイムアプリケーションをサポートする、優れたパフォーマンスを提供する

➤ Nexus GO SigningとEntrust で、 安全性の高いデジタル署名を実現

Entrust nShield Connect HSMは、安全な暗号化処理、鍵の保護・管理を実行できるよう、強化された改ざん防止環境を提供します。nShield HSMを使用することで、以下が可能になります。

- 暗号鍵を保管・管理するために厳重に制御された改ざん防止環境を提供
- セキュリティ機能を管理タスクから分離し、鍵の使用ポリシーを適用
- 業界標準のAPI (PKCS#11、OpenSSL、JCE、CAPI、CNG、WebサービスAPIとnShield Webサービスオプションパックを組み合わせたもの) を使用するアプリケーションを備えたインターフェース

Entrust HSM

Entrust nShield HSMは、最高の性能と安全性を備え、簡単に統合できるHSMソリューションの1つであり、規制コンプライアンス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。

Nexus Group

スウェーデンの企業であるNexus Groupは、急成長している革新的なアイデンティティ・セキュリティ企業です。物理的世界とデジタル世界の人々や物に対して信頼できるアイデンティティを提供することで、社会を保護します。そのテクノロジーの大部分はNexus Smart IDソリューションに統合されており、標準化された使いやすいモジュールを提供します。そのモジュールを使用することで、組織は、物理的IDおよびデジタルIDの発行と管理、物理的アクセスおよびデジタルアクセスの管理、電子署名の実施、公開鍵基盤 (PKI) 証明書の発行と管理が可能になります。Smart IDソリューションは一般的に、企業ID、市民ID、IoT (モノのインターネット) セキュリティに使用されます。Nexusは、ヨーロッパ、インド、米国にある17のオフィスとグローバルパートナーネットワークに従業員300人を擁しています。

詳細

技術仕様の詳細については、
entrust.com/ja/HSMまたは
www.nexusgroup.com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

