



ENTRUST

CryptomathicがEntrust nShield HSMを使用して、 認証電子署名を提供



CRYPTOMATHIC

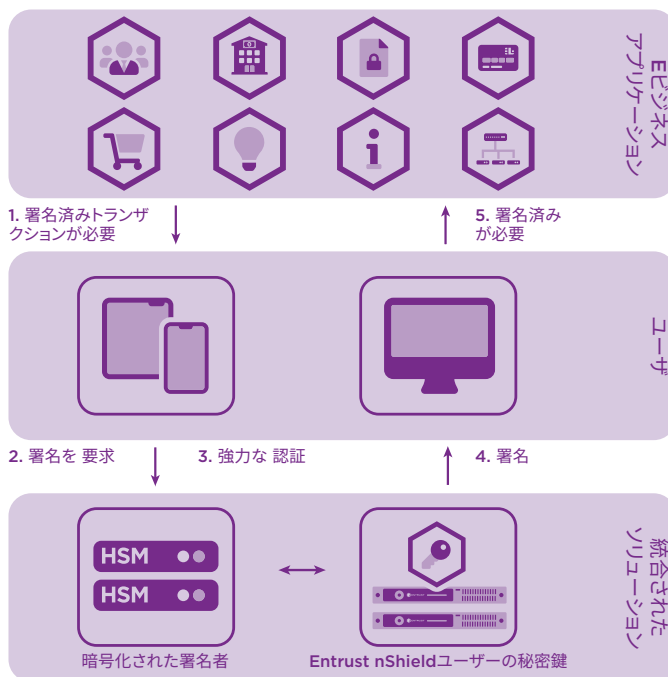
認証電子署名を提供する集中ソリューションで、
顧客のオンライン活動を保護

ハイライト

- いつでも、どこでも、トランザクションとドキュメントに署名
- 汎ヨーロッパの規則に準拠した安全なソリューションを実現
- 「署名する内容の明確な表示」で否認防止をサポート
- 物理的なドキュメントの管理にかかる運用コストを削減
- リモートで適格電子署名を提供

問題：法的拘束力のあるトランザクションやドキュメントにユーザーが物理的な署名を行う必要があるオンラインバンキングサービスでは、完全なデジタルソリューションを実現することはできない。

完全なデジタルサービスをオンラインカスタマーに提供するには、信頼と利便性を提供できることが重要です。現在、オンラインバンキングのトランザクションはほぼすべてのステップがデジタル化されていますが、現行のサービスでは、唯一「エンドユーザーが、コネクテッドデバイスに表示される内容に法的拘束力のある同意を提供する」という作業を実行することができない状態にあります。



Entrust nShield Connect HSMは、オンラインバンキングの顧客に認証電子署名を提供するために、Cryptomathic Signerが使用する秘密鍵を保護・管理します。nShield HSMは、オンプレミスまたはアズ・ア・サービスとして展開することができます。

▶ CryptomathicがEntrust nShield HSM を使用して、認証電子署名を提供

課題：顧客のデジタル活動を完全なものにする、信頼できるデジタル署名体験を提供する。

オンラインサービスを利用する顧客は、ブラウザ操作が中断されることなく、どのデバイスでもすべてを実行できるソリューションを求めています。否認防止をサポートしながら、法的拘束力のあるトランザクションやドキュメントに、いつでもどこにいてもデジタル署名ができるようにするには、信頼性の高いデジタル署名技術が必要です。ヨーロッパでは、電子取引の電子ID及びトラストサービスに関する規則 (eIDAS) が、ビジネスのデジタル変革戦略を実現する強力なプレイヤーになりつつあります。

ソリューション：高保証の認証電子署名と、どこにいても簡単に使用できるゼロフットプリント署名。

デジタル署名は、完全なデジタルサービスを顧客に提供するための次のステップであり、これまでオフラインで行われてきた操作とトランザクションを完全にオンラインで実行できるようにします。この技術革新を推進するため、eIDAS規則には、電子署名がEU内で法的拘束力があるとみなされるよう、企業が順守しなければならない特定の要件が定められています。Cryptomathicの特許技術により、一元管理された安全でユーザーフレンドリーな方法で、エンドユーザーに電子署名ソリューションを提供することができます。また、フットプリントがゼロであるため、エンドユーザーのデバイスにアプリケーションをダウンロードする必要がありません。

Cryptomathic Signerは、CryptomathicのeIDAS規則に準拠した適格署名作成デバイス (QSCD) を組み込んだリモート署名ソリューションです。これにより、銀行やトラストセンターは、法的拘束力のある大規模なデジタル署名サービスをクライアントとエンドユーザーに提供することができます。このソリューションは、ヨーロッパ全体で毎月数百万件の取引を処理する銀行や政府機関に採用されています。「署名する内容を明確に表示する」技術を使用することによって消費者の信頼を構築・強化し、強力なセキュリティとユーザーの利便性を実現します。

Cryptomathic Signerは、Entrust nShield® Connectハードウェアセキュリティモジュール (HSM) と統合して、ユーザーの秘密鍵を保護します。両社は、eバンキングと電子政府で使用される、進化し続ける決済システムとデジタルエコシステムのサポートに関する専門知識を持っており、Cryptomathic Signerはその知識を活用して、既存のWebバンキングサービスとのスムーズな統合を行います。クライアントは、ソフトウェアをインストールしたり、プラグインや追加コンポーネントを使用する必要がありません。ブラウジング機能を備えたあらゆるデバイスから、いつでもどこにいても使用することができます。署名鍵は、オンプレミスまたはアズ・ア・サービスとして展開できるnShield Connect HSMのFIPS 140-2レベル3、およびコモンクライテリアEAL4+に認定された安全なセキュリティ境界内に安全に格納・保護されているため、ユーザーが署名鍵を紛失したり、署名鍵が侵害されたりすることは実際不可能です。

CryptomathicがEntrust nShield HSM を使用して、認証電子署名を提供

Entrust nShield Connectを Cryptomathic Signerと併せて使用する 理由は？

認証HSMの境界外で処理される暗号鍵は、攻撃に対して非常に脆弱であり、侵害につながる可能性があります。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。ユーザーの署名鍵は、可動性を提供するために、トラストセンターの改ざん防止環境に一元的に保存されます。Cryptomathic Signerは、ユーザーのブラウザからnShield Connect HSMへの安全な直接接続を可能にします。オンプレミスまたはアズ・ア・サービスとして展開できるnShield Connect HSMでは、ユーザーの鍵が安全に保管されます。

ユーザーは、既存の2要素認証によって自分自身を認証することで、署名鍵にアクセスし使用することができます。

Entrust nShield Connectは、分散型アプリケーションインスタンスと仮想マシンの共有リソースとして安全な暗号化サービスを提供する、高性能なネットワーク接続型HSMです。このソリューションを使用することにより、ソフトウェアベースの暗号化がリスク管理基準に達しないサーバベースのアプリケーションに対して、適切なレベルの物理的・論理的な制御を実行できます。nShield Connect HSMは、優れた暗号化処理、拡張性、強靭性を提供します。特にモバイルアプリケーション向けの基準が築かれたいま、最新の暗号化アルゴリズムと鍵管理機能を備えた本製品は、将来性のあるソリューションと言えます。HSM内で実行するカスタムコードの開発を可能にするため、顧客の専門的なニーズを満たすために必要不可欠なツールとして機能します。

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にかつきめ細かく制御します。

暗号化

Cryptomathic Signerにより、デスクトップ版とモバイル版のWebブラウザを含む全てのチャンネルで、オンラインサービスを利用する顧客に信頼性の高いデジタル署名サービスを提供することができます。本ソリューションには次のような特徴があります。

- eIDAS規則に準拠した適格電子署名を提供
- 既存の2要素認証展開のセキュリティを活用・強化
- 法執行機関向けの否認防止を適用

www.cryptomathic.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

