



eIDASをビジネス機会に

nShield HSMでトラストサービスを構築



ENTRUST

SECURING A WORLD IN MOTION



概要

欧州連合 (EU) の電子識別およびトラストサービス (eIDAS) 規則は、EU全体の組織に重要な機会をもたらします。eIDAS規則により、政府機関や企業はより迅速で簡単かつ安全に国境を越えた電子商取引を運用できるようになります。また、eIDAS規則によりトラストサービスプロバイダー (TSP) は、ソリューションの需要を拡大するためのビジネス環境を確立することができます。

このようなメリットを実現するためには、信頼できるサービスとアイデンティティの確立が根本的に求められます。Entrust nShield®ハードウェア・セキュリティ・モジュール (HSM) は、信頼できるデジタルトランザクションを可能にする、必要不可欠なセキュリティサービスをお届けします。TSPはnShield HSMを使用することで、強力な信頼の基点に基づいてサービスの提供を拡大すると同時に、セキュリティを強化しながら、国境を越えて法的拘束力のあるトランザクションを行うことができます。

もたらされる機会

EUのeIDAS規則は、EU内でトラストサービスを提供する組織に魅力的な機会をもたらします。この規則は、安全な電子商取引を推進し、最終的にヨーロッパのデジタル経済を発展させられるよう、EU全体における基準を確立する目的で制定されました。EUは同規則を通じて、法的拘束力のある国境を越えた取引、契約、サービスを可能にする、電子商取引の枠組みを確立することとなりました。

組織はこの共通基準を採用することで、従来の紙ベースへの依存を減らし、デジタルトランザクションがもたらす次のようなメリットをさらに活用できるようになります。

- より迅速なワークフローと対応
- ユーザの利便性の向上
- より強力なセキュリティ
- コスト削減
- 運用効率の向上

特に、eIDAS規則は次のような組織に多くのメリットをもたらします。

- 企業：eIDAS規則により、より多くのトランザクションが可能になり、国境を越えた事業拡大を容易に実現可能。
- 政府機関：当規則の下で、より多くのサービスの提供、利便性や価値の向上、より多くのユーザへの対応、コスト削減が可能。
- TSP：eIDAS規則に準拠したトラストサービスを提供することにより、市場およびサービスの拡大や、急成長する市場で収益を上げることが可能。



eIDAS規則

eIDAS規則は「企業、市民、公的機関の間で安全かつシームレスな電子的相互作用を可能にする、予測可能な規制環境を提供する指標」となります。

参照: ec.europa.eu/digital-single-market/en/trust-services-and-eid

トラストサービスの要件

国境と組織を越えたデジタルトランザクションに対する信頼を確立するには、信頼性、可視性、監査可能性、そして制御性を保証する、信頼できるシステムが必要です。eIDAS規則は、以下を含むトラストサービスに関する枠組みをもたらします。

- 文書の署名・封印や、Webサイトの識別のための証明書の発行
- デジタル署名されたタイムスタンプの提供
- 署名されたデータの長期保存
- 電子配信サービスの提供
- 署名と封印の検証と確認

eIDAS規則に準拠するために、トラストサービスは認証取得済みのHSMを使用する必要があります。コモンクライテリアEAL 4+に認定されていることが望ましいものの、EU諸国の一部ではFIPS 140-2認証も受け入れられています。さらに、「適格レベル」での署名に使用されるクライアント鍵を保持する場合、デバイスは、署名者による鍵の「唯一の制御」に対する特定要件を満たすよう、適格署名生成デバイス(QSCD)として認証される必要があります。どちらの場合も、署名プロセスの基盤となる暗号鍵が安全なデバイスで適切に保護されている場合にのみ実行される、強力な暗号化が必要となります。適格署名の場合は、認証された署名者による鍵の唯一の制御を保証するために、ユーザ署名鍵の保護を強化する必要があります。それにより、最終的にシステム全体のセキュリティは、暗号鍵を保護する信頼の基点と同様に強固なものとなります。



ソリューション

Entrust nShield HSM

ソリューションのご紹介

セキュリティを万全に機能させるためには、監査可能な方法によって暗号化された重要なデータを保護する、専用の認定済みHSMを使用する必要があります。Entrust nShield HSMは、デジタル署名と暗号化を実行するための強力な暗号鍵を生成します。また、ソフトウェアベースの暗号鍵の管理に対する強度が認識されているため、HSMの使用は増加傾向にあり、eIDAS標準の採用が拡大し続けるにつれて、その傾向はさらに加速すると予想されます。

nShield HSMはコモンクライテリアEAL4+認定を取得し、QSCDとして認識されており、eIDAS規則への準拠をサポートします。nShield HSMを使用することにより、認証された耐タンパ性ハードウェア内で暗号化を行い、署名鍵を生成・管理することができます。

パートナーシップを通じた顧客価値の最大化

デジタル証明書、タイムスタンプ、デジタル署名を発行するTSPは、eIDASに準拠したソリューションの一部としてnShield HSMを使用することができます。Entrustは、多くのTSPと技術パートナーシップを結んでおり、このようなパートナーシップを通じて、eIDASエコシステム向けの統合nShield HSMソリューションを提供しています。

nShield HSMを採用することにより、TSPはeIDAS規則に準拠し、提供するサービスのセキュリティを大幅に向上させることができます。また、統合された完全なソリューションを提供することにより、TSPは次のことが可能になります。

- 規則に準拠した高価値のトラストサービスを確立
- eIDAS規則に関連した成長市場を活用
- Entrustのグローバルなブランド認知度を通じて市場での認知度を向上
- 変化し続ける市場要件にTSPが適応できるよう、セキュリティ業界のリーダー企業と提携



nShield HSM

Entrust nShield HSMは、安全な暗号化処理と、鍵の保護および管理を実行できるよう、強化された耐タンパ環境を提供します。

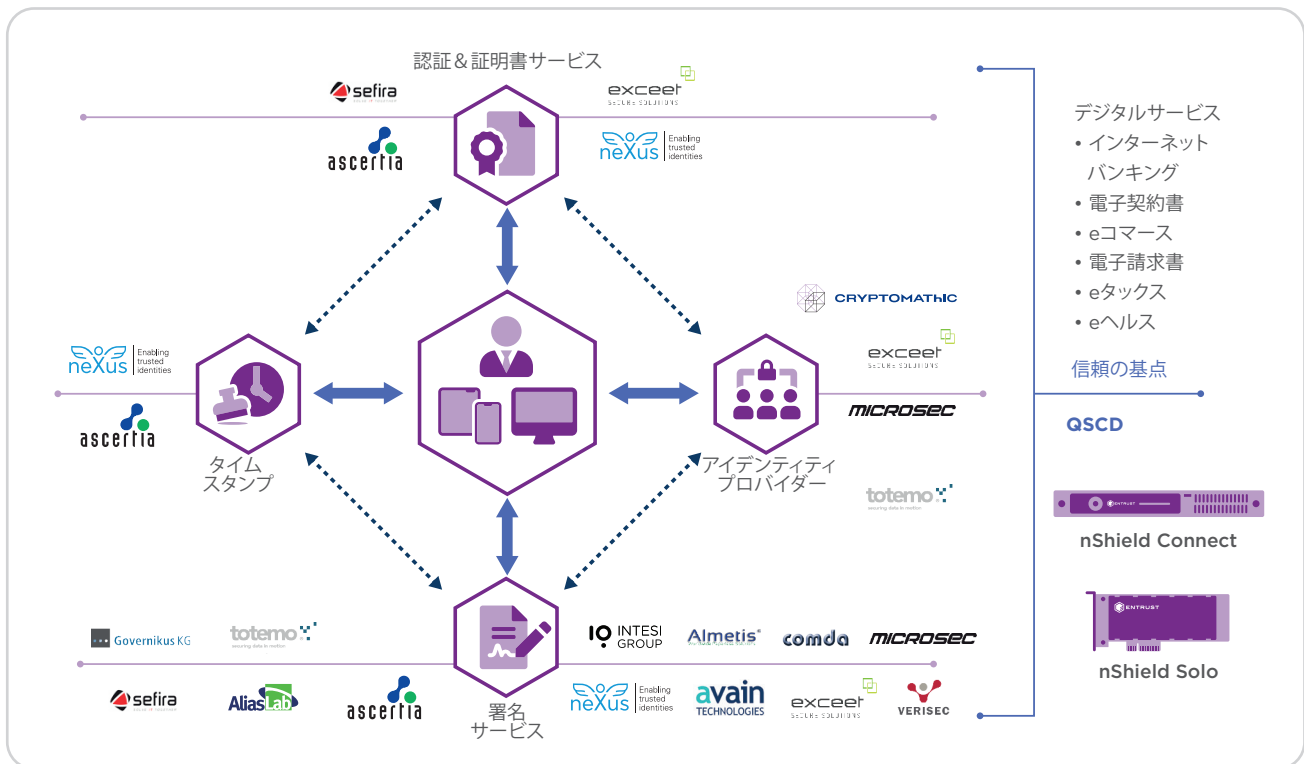


図1: Entrustは、幅広いソリューションおよびサービスプロバイダーとパートナーシップを確立しています。

現在、Entrustのパートナー企業は、4つの重要な分野でセキュリティを強化しています。

- 認証および証明書サービス
- アイデンティティプロバイダー
- 署名サービス
- タイムスタンプ

ユーザにもたらすメリット

nShield HSMは、パートナー企業の統合ソリューションと組み合わせることで、政府機関や企業に数多くの魅力的なメリットをもたらします。

- 国境を越えて法的拘束力のあるビジネスランザクションを実行
- リスクとコストを最小限に抑えながら、サービスのデジタル化を拡大
- 実証済みの統合ソリューションの導入時間を最小化

結論

eIDAS規則がもたらす機会を最大限に生かすために、企業、政府機関、TSPは、信頼できる安全なデジタルサービスを確立する必要があります。Entrust nShield HSMを採用することで、安全なデジタルトランザクションの基盤となる暗号鍵を強力に保護することができます。



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

