



ENTRUST

itAgileがEntrustを採用しペーパーレス社会で信頼を構築

itAgile

PRIME Cert TSP

ビジネスチャンス

itAgileは、デジタル文書と署名ソリューションのプロバイダーです。同社がビジネスチャンスとして着目したのは、電子識別及び認証とトラストサービス (eIDAS) 規則に準拠したサービスプロバイダー (TSP) 適格要件を顧客が満たすことができ、顧客のより迅速な市場投入を可能にするような製品を作り出すことで、顧客が適格TSPとなれるようサポートを提供することでした。

eIDAS規則は、欧州連合 (EU) 全体で法的拘束力のある国境を越えたビジネスを可能にする、電子取引のフレームワークを確立するために制定されました。同規則は、電子署名に手書き署名と同等の法的地位が与えられる基準を明確にし、各加盟国内の監督機関が定めるトラストサービスプロバイダー (TSP) に関する規則を見据えています。

「我々は、nShield Soloがシステムの基盤を成すコンポーネントであると確信している。このシステムは効果的に機能していると言えるだろう。Entrust チームおよび同社のnShield HSMとの良好な協働関係を通して、市場投入までの時間を短縮し、コストを回収することが可能となった」

- Gianni Sandrucci氏 (itAgile最高経営責任者)

EUで事業を展開している企業は、同規則に準拠したトラストサービスを利用することで、すべての署名された文書や契約書の有効性がEU全域で保証されるというメリットを得ることができます。特に銀行は、顧客のアイデンティティと契約の有効性を保証するために、eIDAS規則に準拠したシステムの利用を進めています。また、政府が市民向けデジタルサービスを拡大するにつれて、eIDAS規則に準拠したサービスと署名の使用が必要となってきました。

技術的チャレンジ

itAgileのソリューションには、公開鍵基盤 (PKI) のコアコンポーネントである認証局 (CA) が含まれ、これにより、階層型の信頼チェーンを構築します。PKIには、署名者が本人であることを確認するために必要なハードウェア、ソフトウェア、ポリシー、手順、プロセスが含まれます。

CAは、ユーザーアイデンティティの証明に使用されるデジタル証明書を発行し、PKIのセキュリティとサポートしているサービスの土台となります。そのため、CAは高度な標的型攻撃の対象になる可能性があります。CAに対する攻撃のリスクを軽減するために、物理的かつ論理的な制御と、ハードウェア・セキュリティ・モジュール (HSM) などの強化されたメカニズムを使用して、PKIの整合性を確保することが求められます。

「eIDAS TSP要件を満たす認証局を構築することは、非常に困難である。なぜなら、TSP認定を取得するには、360もの要件を満たす必要があるからだ。要件のひとつとして、暗号化ソリューションのセキュリティ基準である、コモンクライテリアEAL4に認定されたHSMを使用する必要がある。しかし、適格なHSMを市場で見つけることは簡単なことではない。さらに、暗号化そのものが、シンプルで簡単なタスクではないのだ」と、itAgileの最高経営責任者であるGianni Sandrucci氏は述べています。

ソリューション

デジタル署名のエキスパートであるitAgileは、EntrustのnShield Solo HSMを採用しました。同HSMは、コモンクライテリアEAL4+認証を取得しており、適格署名作成デバイス (QSCD) として認定されます。TSPは、強力な暗号化を実行するQSCDを使用し、署名のセキュリティを保護する必要があります。

「HSMはプロセスの中核だ。当社では、信頼の基点を提供するために1つ、デジタル証明書や署名の発行・検証といったPKIの運用用に2つ、そして災害復旧用に1つのHSMが必要となる。このアーキテクチャによりルート鍵とCAが分離されるため、二重のセキュリティを確保することができる。1つのHSMで信頼の基点を提供し、別のHSMで証明書を作成する。

当社サービスには非常に高い信頼性が求められるが、信頼性に優れたEntrust nShield® HSMがそれを叶えてくれる。これこそがEntrustを選択した理由の1つだ。EntrustのHSMは信頼性が高く、長年にわたって使用することができる」と、Sandrucci氏は説明します。

効果

itAgileのPrimeCert TSPは、適格TSPとして認定されるために必要なターンキーソリューションを提供します。PrimeCertの利用者は引き続き、eIDAS規則準拠の認証を受ける必要がありますが、PrimeCertが認証取得に必要な包括的サポートをお届けします。そして、そのサポートの重要な1要素となるのがEntrustのnShield Solo HSMです。同HSMは、コモンクライテリアEAL4+だけでなく、FIPS 140-2レベル3の認証も取得しています。

「...当社サービスには非常に高い信頼性が求められるが、信頼性に優れたEntrust HSMがそれを叶えてくれる。これこそがEntrustを選択した理由の1つだ。EntrustのHSMは信頼性が高く、長年にわたって使用することができる」

- Gianni Sandrucci氏 (itAgile最高経営責任者)

Sandrucci氏は次のように話しています。「EUは厳しく規制されている。顧客がペーパーレス化を希望する場合、まず使用するシステムがeIDAS規則に準拠していることをEUに証明する必要がある。Entrust nShield Solo HSMを採用することで当社の製品は、現行のあらゆる規則と、将来施行されるであろう規則に対する要件を満たすことができる」

「我々は、nShield Soloがシステムの基盤を成すコンポーネントであると確信している。このシステムは効果的に機能していると言えるだろう。Entrustチームおよび同社のnShield HSMとの良好な協働関係を通して、市場投入までの時間を短縮し、コストを回収することが可能となった」

ITAGILEについて

itAgileは、イタリアおよびその他の欧州連合 (EU) 地域において、アジャイルデジタル文書ソリューションと署名ソリューションを専門に扱う企業です。2008年に設立された同社は、顧客とパートナーに以下を提供しています。

- ベストオブブリード製品
- 規則と基準に関する徹底した知識
- テクニカルサポート
- 製品を顧客のプロセスに効率的に統合するためのアプリケーション開発

ISO 27001およびISO 9001認証を受けたitAgileは、顧客サービスに焦点を当て、クラウドテクノロジーと革新的なコラボレーションツールを採用した、機敏性の高い組織モデルを取り入れています。

ビジネスニーズ

- デジタル署名を利用する顧客によるeIDAS規則準拠TSPの認証取得と、より迅速な市場投入を可能にする、ターンキーソリューションを構築

技術的ニーズ

- eIDAS規則に準拠した適格TSPのステータスの達成に必要な多数の厳格な技術要件を満たす、複製可能なプロセスを構築 (コモンクライテリアEAL4+認証を受けたHSMによって管理されるCAを含む)

ソリューション

- Entrust nShield Solo HSM

効果

- TSP認定取得を目指すitAgileサービスの利用企業による、より迅速な市場投入を実現

ENTRUSTについて

Entrust は信頼される認証、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 はこうしたインタラクションの要となり、他にはない多様なデジタルセキュリティと認証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

