Microsecは、銀行がEntrust nShield HSMを使用し、欧州決済サービス指令（PSD2）に準拠することを支援します

オープンバンキングでは、顧客の承認を得た上で財務情報が安全に共有され、そのメリットには、顧客体験の向上や新しい収益源が含まれます。Microsecは、Entrust nShield®ハードウェアセキュリティモジュール（HSM）を使用して、業界と技術の専門知識に基づいたソリューションを開発しました。これを使用することで、銀行や金融サービス機関はコンプライアンスと競争力を強化することができます。Microsecは、ハンガリーのIT市場のリーダーであり、EU決済サービス指令改訂版2015/2366（PSD2）に準拠する認定証明書を提供する、ヨーロッパ初の認証局（CA）の1つであるe-Szignó認証局を運営しています。

Microsecの主な活動は次のとおりです。

- ハンガリーの企業登録と企業情報システムの維持および開発
- ハンガリー、中央ヨーロッパ、東ヨーロッパにおける幅広い公開鍵インフラストラクチャ（PKI）サービスおよびビジネスソリューション（トレーニング、専門コンサルティングを含む）の提供
- 電子本人確認・認証・トラストサービス（eIDAS）に関するEU規則No910 / 2014に準拠した、認定トラストサービスの提供

ビジネスにおけるチャレンジ

PSD2は、決済サービスと決済サービスプロバイダーを規制するEU指令です。これは、消費者が自身の財務データにアクセスして管理する際の自律性を高め、そのデータを保護する銀行の責任を強化することを目的としたコンプライアンス要件です。また、サードパーティはPSD2に基づき、オープンAPI経由で、顧客の銀行口座に対する新しい革新的な金融サービスを提供することができます。

PSD2は、決済業界に2つの大きな変化をもたらします。これはオンライン取引のセキュリティ要件を強力な顧客認証によって強化することを義務付け、また口座保有者が同意した場合、銀行やその他の金融機関はサードパーティの決済サービスプロバイダーに消費者の銀行口座へのアクセスを許可する必要があります。

PSD2が実施される前は、金融サービスプロバイダーは、顧客に代わって顧客の認証情報を使用して取引を行っていました。これは、顧客に深刻なセキュリティリスクをもたらしました。

Microsec

PSD2の下では、決済サービスプロバイダーは、顧客のIDではなく、プロバイダーのIDを使用して銀行とやり取りする必要があります。この場合、銀行はオープンAPIを公開して、サードパーティの金融サービスプロバイダーが顧客の口座情報にアクセスできるようにする必要があります。銀行はそのために、デジタル証明書を使用してサードパーティの決済サービスプロバイダーと銀行の両方を確認・認証する新しいインフラストラクチャを導入する必要があります。

デジタル認定証明書

PSD2規制技術基準では、決済サービスプロバイダー（PSP）とその公開鍵のIDを安全に証明するデジタル認定証明書を使用することが義務付けられます。認定証明書により、サードパーティプロバイダー（TPP）、銀行などの口座保有型決済サービスプロバイダー（ASPSP）を含むPSPは、PSD2に準拠することができます。この証明書は、コミュニケーションの真正性、機密性、整合性を保証し、また取引やコンテンツに関する法的拘束力のある証拠を提供します。

PSD2デジタル認定証明書は、eIDAS規制に従って作成する必要があります。そのため、トラストサービスプロバイダー（TSP）は信頼性の高いシステムと認定HSMを使用して、証明書発行インフラストラクチャを保護する必要があります。nShield HSMは、オランダのNSCIBスキームの下で、EN 419221-5プロテクションプロファイルに対するコモンクライテリアEAL4 + AVA_VAN.5およびALC_FLR.2に認定されています。このコモンクライテリア認定により、デジタル証明書、タイムスタンプ、またはデジタル署名を発行するeIDAS TSPは、eIDASに準拠するソリューションを実現できます。

認定証明書を発行する認定トラストサービスプロバイダー（QTSP）は、認定証明書に含まれるすべてのデータを検証し、PSPの対面または同等での本人確認の検証を行う必要があります。認定証明書は、各EU加盟国の認定されたトラストサービスプロバイダー（QTSP）のリストを含む、EUトラストリストに基づいて検証する必要があります。

ビジネスチャンス

デジタル認定証明書の使用に関する要件は、Microsecにとってビジネスチャンスであり、新しい収益源をもたらす可能性を示しています。Microsecは、PSD2に準拠した強力な顧客認証ツールを使用して、すでに多くの銀行をサポートしています。PSD2要件により、銀行がオープンAPIを公開し、利用者の口座に決済サービスプロバイダー（TPP）がアクセスできるようになることは、Microsecが銀行およびサードパーティのTPPをコミュニケーションの保護および認証要件への準拠においてサポートできることを意味します。

技術的チャレンジ

この新しい事業分野に参入するにあたって、Microsecは既存の公開鍵認証基盤（PKI）を適応かつ拡大させ、銀行およびTPPをサポートするために必要な要求の増加に対応する必要があります。Microsecは、PSD2に準拠した証明書のための新しい証明書プロファイルを作成し、これをサポートするCAソフトウェアを開発するとともに、新しい証明書タイプの発行と管理の手順および実施方法を指定する必要がありました。また、ウェブサイト認証のための認定証明書の発行という新しいトラストサービスの適合性評価を完了する必要があります。

公開鍵認証基盤（PKI）

進化するビジネスモデルが、オンライン認証やより厳しいデータセキュリティ規制への準拠を必要とする電子的なやり取りにますます依存するようになるにつれて、次世代のビジネスアプリケーションは、高い保証を確保するためにPKIテクノロジーにさらに依存するようになっています。

Microsec

PSD2では、決済サービスプロバイダーは、eIDAS規制で定義されている認定証明書を使用する必要があります。実際には、この証明書は、X.509標準に基づくPKIベースの公開鍵証明書です。eIDAS規制はテクノロジーに中立ですが、PKIは現在、必要なレベルのセキュリティとユーザビリティを提供する唯一のテクノロジーです。

ハードウェアセキュリティモジュール （HSM）

HSMは、強化された改ざん防止ハードウェアデバイスであり、データの暗号化・復号およびデジタル署名・証明書の作成に使用される鍵を生成、保護、管理することにより、暗号化プロセスを保護します。HSMは、FIPS 140-2やコモンクライテリアなどの最高のセキュリティ標準に基づいてテスト、検証、認定されています。HSMにより、組織は次のことが可能になります。

- eIDAS、PSD2、GDPR、PCI DSS、HIPAAなど、サイバーセキュリティに関する新しく設定された規制基準を満たし、それを上回る
- より高いデータの安全性と信頼性を実現する
- 高いサービスレベルとビジネスの機敏性を維持する

eIDAS規制は、TSPが信頼できるシステムを使用することを義務付けており、適用される技術標準では、デジタル証明書の発行に使用される秘密鍵を保護するために、認定HSMの使用が特に求められています。

ソリューション

Microsecは、TPPおよびASPSPの取引に必要なデジタル証明書に必要な新しい特性を組み込んだ認証局ソフトウェアの開発に尽力しました。

MicrosecはEntrust nShield HSMを使用して、デジタル証明書の発行に使用される秘密鍵を保護することで、eIDAS認定証明書を発行する要件を満たし、すべてのEU加盟国でQTSPとして認識される認定ステータスを達成することができました。

Microsecは、地理的に離れた2つのデータセンターにEntrust nShield HSMのかなりの資産をすでに持っていたため、予想される要求の増加に対応する能力と俊敏性を備えていました。

さらに、nShield鍵管理フレームワークであるSecurity Worldは、サービスプロバイダーが適格で信頼性の高いサービスインフラストラクチャを維持するために必要とする、完全な制御、簡単なバックアップ、拡張性、柔軟性を提供します。

Microsecは、次のような必要な手順とプロトコルも実施しました。

- 銀行、決済サービスプロバイダー、またはフィンテック企業が証明書を申請するときに必要なすべての個人情報と組織情報を確認する
- 国内の管轄当局の公的登録簿を参照し、決済サービスプロバイダーがその管轄当局からの必要な承認を受けていることを確認する
- 証明書において世界で一意の参照番号または識別子として機能する、申請組織の一意の承認番号を特定する
- 組織が持つことを許可されている役割を確認する

結果

Microsecは、PSD2準拠のデータの標準形式と管理を指定するETSI TS 119 495に従って、ウェブサイト認証（QWAC）およびeシール（QSealC）用のeIDAS認定証明書を発行します。このサービスは欧州経済領域（EEA）全体で提供されており、Microsecはすでに10のEU加盟国からの申請者にPSD2準拠の証明書を発行しています。

Microsec

ビジネスニーズ

- 銀行とTPPがPSD2規制内で運営するのを支援するサービスを構築する

技術的ニーズ

- PSD2準拠の証明書の発行に必要なソフトウェアとプロセスを開発することにより、既存のインフラストラクチャを使用して新しいビジネスを創出する

ソリューション

- Entrust nShield Solo HSM
- カスタムCAソフトウェアおよびプロセス
- Entrust nShield Security World

結果

- EU全体の新しい規制を適用する新しいサービスを提供するために、迅速かつ簡単に適応された既存のインフラストラクチャは、全体的な収益に追加されます。
- 実証済みで、信頼性が高く、頼れるHSMソリューション
- 規制上の義務の遵守

トラストサービス、対応するソフトウェア開発、コンサルティングは現在、Microsecの収益の3分の2を占めています。PSP向けの新サービスの追加により、今後数年間に国際収益の割合が増加すると予想されます。

Microsecは2007年より、世界的に認められた欧州電気通信標準化機構（ETSI）の正式会員です。ETSIは、将来の経済プロセスの基礎となる可能性のあるITテクノロジーに世界的に適用可能な標準を提供します。Microsecは、電子署名およびインフラストラクチャに関するETSI技術委員会（TC ESI）の仕事に積極的に参加し、PSD2証明書仕様TS 119495の開発に貢献してきました。

Microsecの高水準の製品とサービスは、ISO 9001:2008に基づく品質保証システムと、ISO/IEC 27001:2013に沿ってLloydによって承認された情報セキュリティ管理システムによって支えられています。

Microsecとそのソリューションおよびサービスの詳細については、www.microsec.comをご覧ください。

ENTRUSTについて

Entrustは、信頼性の高い本人認証、決済、データ保護を可能にすることにより、世界の動きを安全に維持します。今日、人々はこれまで以上に、国境を越えた移動、買い物、電子政府サービスへのアクセス、企業ネットワークへのログインといったさまざまな場面で、シームレスで安全なユーザー体験を求めています。Entrustは、これらすべてのインタラクションに対応した、他では見られない広範なデジタルセキュリティおよび資格情報発行用ソリューションを提供しています。2,500名以上の従業員とグローバルパートナーのネットワークを備え、150か国以上における顧客から支持されているため、世界における多くの委託組織から信頼を得ていることは不思議ではありません。

詳細は下記URLをご覧ください。
entrust.com/ja/HSM

ENTRUST

お問い合わせ：
HSMinfo@entrust.com