フィンランドはnShield HSMを用いて、デジタルIDとEAC e-パスポートの整合性を保護

Entrust nShield®ハードウェア・セキュリティ・モジュール（HSM）は、デジタル証明書で保護された指紋により、フィンランドのe-パスポートの真正性を保証しています。

世界で最も電子化が進んでいる国の1つであるフィンランドは、効率的なIDおよびアクセス管理を利用したオンライン行政サービスの提供において、長期にわたってリーダーの役割を果たしてきました。国内の人口登録センター（Population Register Centre、以下PRC）が代表的な事例です。PRCはEntrust nShield HSMで保護された国の公開鍵基盤（PKI）と認証局（CA）を運用し、市民証明書と呼ばれる固有の検証可能なデジタルIDをすべての住民に対して発行しています。住民はその市民証明書を使用して、安全なオンライン行政サービスに効率的かつ費用効果的にアクセスすることができます。このため、デジタルIDの発行に関する最新の欧州（EU）指令に準拠した新しいe-パスポートを同様の技術を使用して発行するように国から求められたとき、当センターはその経験から、プロセスの完全性を保証するために何を使用すべきかは分かっていました。それはEntrustです。

> **PRCは、PKIの導入によるオンライン行政サービスの提供、またデジタル証明書の発行と使用に関する経験が豊富です。Entrust nShield HSMは、秘密鍵を保護するための優れたソリューションであると考えています。**
>
> – Jan Partanen氏、フィンランド人口登録センター

詳細をチェック：ENTRUST.COM/ja/HSM

フィンランド人口登録センター

フィンランド人口登録センターの開発マネージャーであるJan Partanen氏は、次のように語っています。「EUの新しいe-パスポートは、耐タンパ性のデジタル証明書によって保護されているため、世界で最も安全です。ただし、このシステムは、国々がデジタル証明書の真正性を保証する署名鍵を確実に保護している場合にのみ機能します。フィンランドではEntrust nShield HSMがCA、PKI、デジタルID発行の署名鍵を保護しているため、フィンランドのe-パスポートとオンライン行政サービスの整合性を確保できると私たちは確信しています」

セキュリティとプライバシーの確保

すべての人の指紋は固有のものです。EUはこのシンプルな事実を利用して、本人だけがパスポートを使用して旅行できるように保証しています。どのような方法なのでしょうか。EAC（Extended Access Control）標準に基づくEUの第二世代のe-パスポートでは、政府は、なりすましがさらに困難になる強力な生体認証（通常は指紋または虹彩認識）を活用することができます。EAC e-パスポートは、パスポートの有効性を確保しながら、パスポート所有者のプライバシーを保護します。新しいe-パスポートプロセスが完全に実装されると、偽のEUパスポートを使用して別人になりすまして旅行することは事実上不可能になります。EACスキームでは、EU加盟国は指紋データを機械可読渡航文書（MRTD）に追加する必要があります。

e-パスポート、PKI、デジタルIDの保護に使用されるかどうかに関係なく、デジタル証明書は信頼性の高いCAが固有の署名鍵を使用して発行するため安全です。ただし、署名鍵の危殆化や盗難によって、一見有効なデジタル証明書が発行される可能性もあります。HSMは、ソフトウェアよりも格段に安全な耐タンパ性の環境を提供するため、EUはHSMを使用してe-パスポートのCA署名鍵を生成、保存、保護することを義務付けています。

成功の歴史

歴史的に、フィンランド政府はHSMを使用して国内のCAおよびPKIを保護してきました。そのため、当センターはHSMを使用してe-パスポートの整合性を保護することを当初から考えていました。HSMは安全でトラブルがないことが実証済みで、証明書を発行するために国内のCAにシームレスに組み込まれています。HSMは、連邦情報処理基準（FIPS）140-2レベル3の認定を受けており、これは政府および企業の暗号化ソリューションとして最も広く採用されているセキュリティベンチマークであり、EUの EAC e-パスポート基準として義務付けられています。また、Entrustプロフェッショナルサービスチームがe-パスポートと鍵管理に関する専門知識を提供し、PRCが効率的で費用対効果の高いe-パスポート発行プロセスを確立するためのサポートをしたことも、同様に重要です。

「当センターは、PKIの導入によるオンライン行政サービスの提供、またデジタル証明書の発行と使用に関する経験が豊富です。HSMは、署名鍵を保護するための優れたソリューションであると思います。もちろん、鍵管理も重要です。Entrustプロフェッショナルサービスチームは、鍵管理に関する優れた専門知識とともに、信頼できるソリューションの提供実績があります。私たちはe-パスポートを保護するために、Entrustプロフェッショナルサービスチームと Entrust nShield HSMをためらうことなく選択しました」とPartanen氏は述べています。

フィンランド人口登録センター

> **Entrust nShield HSMを導入することにより、当センターの署名鍵がハードウェアモジュールのセキュリティ保護対象から外れることは絶対ないため、悪用されることは決してありません。HSMとデジタル証明書は複雑に思えるかもしれませんが、これらを使用した結果はシンプルです。これらはフィンランドのe-パスポート、CA、PKI、オンライン行政サービスの整合性を保証してくれます。**
>
> – Jan Partanen氏、フィンランド人口登録センター

E-パスポートのプロセス

PRCはEntrustプロフェッショナルサービスチームと協力して、EU基準に準拠し、市民のプライバシーを保護する新しいe-パスポート発行プロセスを開発および実装しました。新しいe-パスポートには、デジタル証明書とパスポート所有者の指紋が埋め込まれたチップが含まれています。フィンランドのルートCAは、Entrust nShield HSM内で安全に生成かつ保護されている署名鍵を用いて、各証明書を発行しています。署名鍵はHSMのセキュリティ保護の対象から外れることがないため、悪用されることは決してありません。国境を越える際には、パスポートリーダーでパスポート所有者のIDを確認することができます。デジタル証明書によって認証されたデバイスのみがパスポートを読み取ることができ、パスポート所有者のプライバシーを保護しながら、パスポートの有効性を確保することができます。

費用対効果と高可用性

PRCは、1台のサーバのみに動作するHSMではなく、ネットワークに接続されたEntrust nShield Connect HSMをe-パスポートプロセスで使用することにしました。HSMをネットワーク化することで、PRCには2つの重要な利点がありました。1つは、nShield HSMは複数のサーバをサポートするため、PRCはe-パスポートPKIサーバごとにHSMを1台ずつ購入する必要がなく、ハードウェアコストを削減できたことです。もう1つのメリットは、HSMが高い可用性とスケーラビリティを効率的にサポートしているため、自動フェイルオーバーによりHSM間のシームレスな切り替えが可能になったことでした。

「Entrust nShield HSMは、1つのデバイスが複数のサーバとアプリケーションを同時にサポートできるため、コストと可用性といった明確なメリットをもたらしました。また、デバイスを内部操作から保護するための管理業務の分離など、当センターがHSMに期待するセキュリティ機能をすべて提供してくれます」とPartanen氏は説明します。

プロセスおよび市民の保護

フィンランドがデジタル証明書によって保護された指紋を含むe-パスポートを発行しています。このため、Partanen氏は証明書の盗難および漏洩の恐れはHSMの価値を支える推進力となっていることを指摘しています。同氏は次のように述べています。「e-パスポートの場合、署名鍵の乗っ取りによって、犯罪者や

フィンランド人口登録センター

Entrust導入のメリット

- IDの電子認証が可能
- e-パスポートの整合性と市民のプライバシーを保護
- パスポートの不正取得、偽造、悪用を防止
- 安全なオンライン行政サービスの提供

組織のプロファイル

1969年に設立されたフィンランド人口登録センターは、フィンランド国内の人口情報や市民や建築物の識別情報を管理しています。オンラインサービスなどの高品質のIDソリューションにより、フィンランド市民に対するサービス提供を専門に行っています。

PRCの詳細については、www.vrk.fiおよびwww.fineid.fiをご覧ください。

テロリストが偽造パスポートを発行する可能性があります。あるいは、鍵を使用してe-パスポート自体のロックを解除されると、市民のプライバシーが取り返しの付かないほどの損害を受けるおそれがあります。

Entrust nShield HSMを導入することにより、当センターの署名鍵がハードウェアモジュールのセキュリティ保護対象から外れることは絶対ないため、悪用されることは決してありません。HSMとデジタル証明書は複雑に思えるかもしれませんが、これらを使用した結果はシンプルです。これらはフィンランドのe-パスポート、CA、PKI、オンライン行政サービスの整合性を保証してくれます」

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

ENTRUST

お問い合わせ：
HSMinfo@entrust.com