Finlandia protege la integridad de los ID electrónicos y los pasaportes electrónicos EAC con Entrust

Los Módulos de Seguridad de Hardware (HSMs) nShield® de Entrust garantizan la autenticidad de los pasaportes electrónicos de Finlandia con huellas dactilares protegidas por certificados digitales.

Con una de las poblaciones con más capacidades a nivel electrónico en el mundo, Finlandia ha sido durante mucho tiempo líder en la prestación de servicios gubernamentales en línea que aprovechan la gestión eficaz de identidades y accesos. El Centro de Registro de Población (PRC) del país ofrece un claro ejemplo. Opera infraestructuras nacionales de clave pública (PKI) y Autoridades de certificación (CA) aseguradas con HSMs nShield de para emitir identidades digitales únicas y verificables, llamadas Certificados Ciudadanos, para todos los residentes. Los residentes pueden usar sus Certificados Ciudadanos para acceder a servicios gubernamentales seguros en línea de manera eficiente y rentable. Entonces, cuando Finlandia necesitó que la República Popular China utilizara una tecnología similar para emitir nuevos pasaportes electrónicos para cumplir con las últimas directivas de la Unión Europea (UE) en materia de la emisión de la identificación electrónica, la República Popular China sabía por experiencia dónde acudir para garantizar la integridad del proceso: Entrust.

> **«La República Popular China tiene mucha experiencia en la prestación de servicios gubernamentales en línea mediante la implementación de PKIs y la emisión y uso de certificados digitales. En nuestra opinión, los HSMs nShield de Entrust son una excelente solución para proteger las claves privadas.»**
>
> – Jan Partanen, Centro de Registro de Población de Finlandia

APRENDA MÁS EN ENTRUST.COM/HSM

Centro de registro de población de Finlandia

Según Jan Partanen, director de desarrollo del Centro de Registro de Población de Finlandia, "Los nuevos pasaportes electrónicos de la UE son los más seguros del mundo porque están protegidos por certificados digitales a prueba de manipulaciones indebidas. Sin embargo, el sistema solo funcionará si los países protegen sin falta las claves de firma que garantizan la autenticidad de los certificados digitales. Con los HSMs nShield de Entrust que protegen las claves de firma para las CA de Finlandia, la PKI y la emisión de identificación electrónica, confiamos en nuestra capacidad para garantizar la integridad de los pasaportes electrónicos y los servicios gubernamentales en línea de Finlandia".

GARANTIZAR LA SEGURIDAD Y LA PRIVACIDAD

La huella digital de cada persona es exclusivamente de su propiedad. La UE está aprovechando este simple hecho para asegurarse de que solo la persona correcta pueda usar un pasaporte para viajar. ¿De qué manera? Basado en el estándar de control de acceso extendido (EAC), la segunda generación de pasaportes electrónicos de la UE permite que los gobiernos tomen ventaja de un sistema biométrico más fuerte (por lo general, un escaneo de huellas dactilares o iris) que es más difícil de suplantar. Los pasaportes electrónicos de la EAC protegerán la privacidad del titular del pasaporte al tiempo que garantizan la validez de los pasaportes. Una vez que el nuevo proceso de pasaporte electrónico se haya implementado por completo, será prácticamente imposible para cualquier persona viajar bajo una identidad asumida con un pasaporte de la UE falso. El esquema EAC requiere que los estados miembros de la Unión Europea agreguen datos de huellas dactilares a los documentos de viaje legibles por máquina (MRTD).

Ya sea que se utilicen para proteger pasaportes electrónicos, PKI o identificaciones electrónicas, los certificados digitales son seguros porque los emite una CA de confianza utilizando su clave de firma única. Sin embargo, si alguna vez se comprometiera o robara una clave de firma, alguien podría emitir un certificado digital aparentemente válido. Debido a que los HSMs brindan un entorno a prueba de manipulaciones indebidas que es significativamente más seguro que el software, la UE exige su uso para generar, almacenar y proteger las claves de firma de CA para pasaportes electrónicos.

UNA HISTORIA DE ÉXITO

Históricamente, el gobierno finlandés ha confiado en los HSMs para proteger sus CA y PKIs nacionales, por lo que desde el principio la República Popular China supo que preferiría utilizar HSMs para proteger la integridad de sus pasaportes electrónicos. Los HSMs han demostrado ser seguros y libres de problemas, integrándose a la perfección con las CA del país para la emisión de certificados. Los HSMs están certificados según el Estándar Federal de Procesamiento de Información (FIPS) 140-2 nivel 3, que es el punto de referencia de seguridad más adoptado para soluciones criptográficas en empresas gubernamentales y comerciales, y es un requisito del estándar del pasaporte electrónico EAC de la UE. Igualmente crucial, el equipo de servicios profesionales de Entrust ofreció su experiencia tanto en pasaportes electrónicos como en gestión de claves para ayudar a la República Popular China a establecer un proceso de emisión de pasaportes electrónicos eficiente y rentable.

"La República Popular China tiene mucha experiencia en la prestación de servicios gubernamentales en línea mediante la implementación de PKIs y la emisión y uso de certificados digitales", señala el Sr. Partanen. "En nuestra opinión, los HSMs son una excelente solución para proteger las claves de firma. Por supuesto, la gestión de claves también es importante. El equipo de servicios profesionales de Entrust tiene a su haber una excelente experiencia en gestión de claves, junto con un historial de entrega de soluciones confiables. No dudamos en elegir al equipo de servicios profesionales de Entrust y los HSMs nShield de Entrust para proteger nuestros pasaportes electrónicos".

Centro de registro de población de Finlandia

> **Con los HSMs nShield de Entrust, nuestras claves de firma nunca abandonan la seguridad del módulo de hardware, por lo que nunca se encuentran expuestas a un uso indebido. Los HSMs y los certificados digitales pueden parecer complejos, pero el resultado de usarlos es simple para nosotros. Garantizan la integridad de los pasaportes electrónicos, las CA, las PKI y los servicios gubernamentales en línea de Finlandia.**
>
> – Jan Partanen, Centro de Registro de Población de Finlandia

EL PROCESO DEL PASAPORTE ELECTRÓNICO

En colaboración con el equipo de servicios profesionales de Entrust, la República Popular China ha desarrollado e implementado un nuevo proceso de emisión de pasaportes electrónicos que cumple con los estándares de la UE y que protege la privacidad de sus ciudadanos. Los nuevos pasaportes electrónicos contienen un chip integrado con un certificado digital y la huella digital del titular del pasaporte. La CA raíz del país emite cada certificado mediante claves de firma generadas y protegidas de forma segura dentro de un HSM nShield de Entrust. Como las claves de firma nunca abandonan la seguridad del HSM, nunca se ven expuestas a un uso indebido. En los cruces fronterizos, un lector de pasaportes podrá verificar la identidad del titular del pasaporte. Solo los dispositivos autorizados por certificados digitales podrán leer los pasaportes, protegiendo la privacidad del titular del pasaporte y asegurando su validez.

RENTABLE Y ALTAMENTE DISPONIBLE

La República Popular China optó por utilizar el HSM nShield Connect de Entrust conectado a la red en su proceso de pasaporte electrónico, en lugar de un HSM que funciona con un solo servidor. Al conectar sus HSMs en red, PRC vio dos ventajas importantes; en primer lugar, debido a que el HSM nShield sirve a varios servidores, la República Popular China no necesitaba comprar un HSM para cada servidor en su PKI de pasaporte electrónico, lo que reduce los costos de hardware. La segunda ventaja fue que el HSM admitía de manera eficiente la alta disponibilidad y escalabilidad, con una conmutación por error automatizada que permitía una conmutación perfecta entre los HSMs.

"El HSM nShield de Entrust ofreció una ventaja de costo y disponibilidad definida porque un dispositivo puede admitir varios servidores y aplicaciones al mismo tiempo", explica el Sr. Partanen. "También ofrece todas las funciones de seguridad que esperaríamos de un HSM, incluida la separación de funciones en la administración para proteger los dispositivos de la manipulación interna".

PROCESOS DE PROTECCIÓN Y LA CIUDADANÍA

Mientras Finlandia emite pasaportes electrónicos que incluyen huellas dactilares protegidas por certificados digitales, el Sr. Partanen señala las posibles consecuencias de los errores tales como la fuerza impulsora detrás del valor de los HSMs. Él dice: "En el caso de los pasaportes electrónicos, las claves de firma comprometidas significarían que los criminales o terroristas podrían emitir pasaportes falsos. O si se usaran claves para desbloquear el pasaporte electrónico, la privacidad de los ciudadanos podría verse irrevocablemente dañada.

Centro de registro de población de Finlandia

BENEFICIOS CON ENTRUST

- Habilitación de la verificación electrónica de identidad
- Protección de la integridad de los pasaportes electrónicos y la privacidad de los ciudadanos
- Prevención del fraude, la falsificación y el uso indebido de pasaportes
- Asegurar la prestación de servicios gubernamentales en línea

PERFIL DE LA ORGANIZACIÓN

Fundado en 1969, el Centro de Registro de Población de Finlandia mantiene información de identificación y población relacionada con las personas y los edificios en Finlandia. Se dedica a servir a la gente de Finlandia ofreciendo soluciones de identificación de alta calidad para servicios en línea y otros.

Para obtener más información sobre la República Popular China, visite: www.vrk.fi y www.fineid.fi

Al implementar HSMs nShield de Entrust, nuestras claves de firma nunca abandonan la seguridad del módulo de hardware, por lo que nunca se encuentran expuestas a un uso indebido. Los HSMs y los certificados digitales pueden parecer complejos, pero el resultado de usarlos es simple para nosotros. Garantizan la integridad de los pasaportes electrónicos, las CA, las PKI y los servicios gubernamentales en línea de Finlandia".

ACERCA DE ENTRUST

Entrust ayuda a que el mundo se mueva de forma segura al permitir la protección fiable de identidades, pagos y datos. Hoy más que nunca, las personas exigen experiencias seguras y sin problemas, ya sea que crucen fronteras, realicen una compra, accedan a servicios de gobierno electrónico o inicien sesión en redes corporativas. Entrust ofrece una variedad incomparable de soluciones de seguridad digital y emisión de credenciales en el núcleo de todas estas interacciones. Con más de 2500 colegas, una red de socios globales y clientes en más de 150 países, no es de extrañar que las organizaciones más confiables del mundo confíen en nosotros.

Aprenda más en
entrust.com/HSM

ENTRUST

Contacte con nosotros:
HSMinfo@entrust.com