



**ENTRUST**

SECURITY  
IDENTIFICATION

## **Finnland schützt die Integrität elektronischer IDs und Reisepässe mit Produkten von Entrust**

Die nShield®-Hardware-Sicherheitsmodule (HSM) von Entrust gewährleisten die Authentizität finnischer elektronischer Reisepässe anhand von durch digitale Zertifikate gesicherten Fingerabdrücken.

Weltweit gehören die Finnen zu den Nationalitäten, die besonders häufig elektronische Geräte und Dienste nutzen. Lange Zeit war Finnland Vorreiter bei der Bereitstellung von staatlichen Online-Diensten, die effektives Identitäts- und Zugriffsmanagement nutzen. Das Population Register Centre (PRC) des Landes ist ein treffendes Beispiel. Es betreibt eine Public Key Infrastructure (PKI) und Zertifizierungsstellen (CAs), die mit nShield HSM von Entrust gesichert sind und eindeutige und prüfbare digitale Identitäten, Bürgerzertifikate genannt, an alle Einwohner ausstellen. Die Einwohner können ihre Bürgerzertifikate nutzen, um online effizient und kostengünstig auf sichere Regierungsdienste zuzugreifen. Das finnische PCR benötigte nun ähnliche Technologie, um neue elektronische Reisepässe auszustellen, die den neusten Richtlinien der Europäischen Union (EU) zur Ausstellung elektronischer Dokumente entsprechen. Aufgrund seiner bisherigen Erfahrungen wusste das PCR, an wen es sich wenden musste, um die Integrität des Prozesses zu gewährleisten – an Entrust.



**Das PCR ist sehr erfahren in der Bereitstellung von Online-Regierungsdiensten mithilfe von PKI sowie der Ausstellung und Verwendung von digitalen Zertifikaten. Unserer Ansicht nach sind nShield HSM von Entrust eine ausgezeichnete Lösung zum Schutz von Signierschlüsseln.**



– Jan Partanen, Population Register Centre of Finland



# Das finnische Population Register Centre

Laut Jan Partanen, dem Development Manager des Population Register Centre of Finland, sind die neuen elektronischen Reisepässe der EU die sichersten der Welt, denn sie sind durch manipulationssichere digitale Zertifikate geschützt. „Das System funktioniert jedoch nur, wenn die einzelnen Länder ausnahmslos die Signierschlüssel sichern, die die Authentizität der digitalen Zertifikate garantieren. Da die nShield HSM von Entrust die Signierschlüssel für Zertifizierungsstellen, PKI und Ausstellung elektronischer IDs in Finnland sicher schützen, sind wir überzeugt, dass wir die Integrität der finnischen elektronischen Reisepässe und staatlichen Online-Dienste garantieren können.“

## GEWÄHRLEISTUNG VON SICHERHEIT UND DATENSCHUTZ

Jeder Mensch hat individuelle Fingerabdrücke. Die EU nutzt diese simple Tatsache, um sicherzustellen, dass ein bestimmter Reisepass nur von der jeweiligen berechtigten Person verwendet werden kann. Wie funktioniert das? Die zweite Generation elektronischer Reisepässe der EU ermöglicht es Regierungen, auf Grundlage des Standardverfahrens Extended Access Control (EAC) schwer zu imitierende biometrische Daten (in der Regel einen Fingerabdruck oder einen Iris-Scan) zu nutzen. Die Gültigkeit von elektronischen Reisepässen, die mit EAC gesichert sind, ist gewährleistet und die Daten des Passinhabers sind geschützt. Sobald das neue Verfahren für elektronische Reisepässe vollständig implementiert wurde, ist es nahezu unmöglich, unter einer missbräuchlich verwendeten Identität mit einem gefälschten Pass zu reisen. Das EAC-Verfahren verlangt von den Mitgliedsstaaten der Europäischen Union, Fingerabdruckdaten in maschinenlesbare Reisedokumente (MRTDs) einzufügen.

Digitale Zertifikate sichern elektronische Reisepässe, IDs oder PKI jederzeit verlässlich, denn sie werden von einer vertrauenswürdigen Zertifizierungsstelle mithilfe eines eindeutigen Signierschlüssels ausgestellt. Wenn ein Signierschlüssel jedoch kompromittiert oder gestohlen würde, könnte damit ein scheinbar gültiges digitales Zertifikat ausgestellt werden.

HSM stellen eine manipulations sichere Umgebung bereit, die deutlich sicherer ist als Software. Daher ist deren Nutzung von der EU vorgeschrieben, um die Signierschlüssel für elektronische Reisepässe zu erstellen, zu speichern und zu schützen.

## EINE ERFOLGSGESCHICHTE

Schon immer hatte die finnische Regierung beim Schutz ihrer nationalen Zertifizierungsstellen und PKI auf HSM gesetzt. Daher waren sie sich von Anfang an sicher, dass sie HSM für den Schutz der Integrität von elektronischen Reisepässen nutzen wollten. HSM haben sich als sicher und störungsfrei erwiesen und können nahtlos in die finnischen Zertifizierungsstellen für die Ausgabe von Zertifikaten integriert werden. HSM sind gemäß dem Federal Information Processing Standard (FIPS) 140-2 Level 3 zertifiziert. Hierbei handelt es sich um den am weitesten verbreiteten Sicherheitsmaßstab für kryptographische Lösungen von Regierungen und Wirtschaftsunternehmen, der laut des EAC-Verfahrens der EU für elektronische Reisepässe vorgeschrieben ist. Des Weiteren war entscheidend, dass das Professional Services Team von Entrust das PCR mit seinem Fachwissen zu elektronischen Reisepässen und Schlüsselverwaltung bei der Bereitstellung eines effizienten - und kostengünstigen - Verfahrens zur Ausstellung von Reisepässen unterstützt.

„Das PCR ist sehr erfahren in der Bereitstellung von staatlichen Online-Diensten mithilfe von PKI sowie der Ausstellung und Verwendung von digitalen Zertifikaten“, stellt Partanen fest. „Unserer Ansicht nach sind HSM eine ausgezeichnete Lösung zum Schutz von Signierschlüsseln. Selbstverständlich ist auch die Schlüsselverwaltung wichtig. Das Professional Services Team von Entrust kann ausgezeichnete Fachkenntnisse auf dem Gebiet der Schlüsselverwaltung sowie eine Erfolgsbilanz bei der Bereitstellung von Vertrauensdiensten vorweisen. Wir haben bei der Entscheidung für das Professional Team von Entrust und die nShield HSM von Entrust für die Sicherung unserer Reisepässe keine Sekunde gezögert.“



# Das finnische Population Register Centre

« Die nShield HSM sorgen dafür, dass unsere Signierschlüssel die sicheren Grenzen des Hardwaremoduls zu keiner Zeit verlassen, sodass ein Missbrauch unmöglich ist. HSM und digitale Zertifikate mögen komplex erscheinen, aber für uns sind sie letztendlich einfach zu verwenden. Sie gewährleisten die Integrität elektronischer Reisepässe, Zertifizierungsstellen, PKI und staatlicher Online-Dienstleistungen in Finnland. »

– Jan Partanen, Population Register Centre of Finland

## DAS VERFAHREN

Das PCR hat in Zusammenarbeit mit dem Professional Services Team von Entrust ein neues Verfahren zur Ausstellung von elektronischen Reisepässen entwickelt, das die EU-Normen erfüllt und die Daten der Bürger schützt. Die neuen elektronischen Reisepässe enthalten einen Chip, in den ein digitales Zertifikat und der Fingerabdruck des Reisepassinhabers eingebettet sind. Die finnische Root-Zertifizierungsstelle stellt die einzelnen Zertifikate anhand von Signierschlüsseln aus, die sicher in einem nShield HSM von Entrust erstellt und geschützt werden. Da die Signierschlüssel die sichere Umgebung des HSM nie verlassen, besteht zu keiner Zeit die Gefahr, dass diese missbräuchlich verwendet werden. An Grenzübergängen kann die Identität des Passinhabers mit einem Passlesegerät überprüft werden. Die Reisepässe können nur von Geräten gelesen werden, die durch digitale Zertifikate autorisiert sind. Dadurch sind die Daten des Passinhabers geschützt, und es ist garantiert, dass es sich um einen gültigen Reisepass handelt.

## KOSTENGÜNSTIG UND STETS VERFÜGBAR

Das PCR hatte sich entschieden, für ihr Verfahren zur Ausstellung von elektronischen Reisepässen nicht auf ein HSM mit einem einzigen Server, sondern auf nShield-Connect-HSM von Entrust zu setzen, die an ein Netzwerk angeschlossen sind. PCR sah in der Vernetzung ihrer HSM zwei große Vorteile: Erstens bedient

das nShield HSM mehrere Server. Daher benötigte PCR nicht für jeden Server seiner PKI für elektronische Reisepässe ein HSM und konnte so die Hardware-Kosten senken. Zweitens ist das HSM stets verfügbar und äußerst skalierbar, denn automatischer Failover ermöglicht ein schnelles Wechseln zwischen HSM.

„Die nShield HSM boten hinsichtlich der Kosten und Verfügbarkeit einen deutlichen Vorteil, da ein Gerät gleichzeitig mehrere Server und Anwendungen unterstützen kann“, erklärt Partanen. „Außerdem verfügt es über alle Sicherheitsfunktionen, die wir von einem HSM erwarten. Dazu gehört auch die Aufgabentrennung bei der Administration, die Geräte vor interner Manipulation schützt.“

## SCHUTZ VON PROZESSEN UND BÜRGERN

Finnland stellt elektronische Reisepässe aus, die durch digitale Zertifikate geschützte Fingerabdrücke enthalten. Sollte hierbei ein Fehler passieren, könnte das schwerwiegende Folgen haben. Das macht HSM laut Jan Partanen umso wertvoller sind. Er sagt: „Kompromittierte Signierschlüssel würden bedeuten, dass Kriminelle oder Terroristen gefälschte elektronische Reisepässe ausstellen könnten. Auch könnten die Schlüssel verwendet werden, um den elektronischen Reisepass selbst zu entsperren. Damit wäre der Schutz der Daten der Bürger unwiederbringlich dahin.“



# Das finnische Population Register Centre

## VORTEILE VON ENTRUST

- Elektronische Überprüfung der Identität
- Schutz der Integrität elektronischer Reisepässe und der Daten der Bürger
- Verhinderung von Betrug, Fälschung und Missbrauch von Reisepässen
- Sichere Bereitstellung von staatlichen Online-Dienstleistungen

## UNTERNEHMENSPROFIL

Das finnische Population Register Centre wurde 1969 gegründet und pflegt Bevölkerungsdaten und Daten zur Identifizierung der Einwohner und Gebäude in Finnland. Es stellt den finnischen Bürgern Ausweislösungen für Online-Dienste und sonstige Dienste bereit.

Weitere Informationen zum PCR finden Sie auf [www.vrk.fi](http://www.vrk.fi) und [www.fineid.fi](http://www.fineid.fi).

Die nShield HSM sorgen dafür, dass unsere Signierschlüssel die sicheren Grenzen des Hardwaremoduls zu keiner Zeit verlassen, sodass ein Missbrauch unmöglich ist. HSM und digitale Zertifikate mögen komplex erscheinen, aber für uns sind sie letztendlich einfach zu verwenden. Sie gewährleisten die Integrität elektronischer Reisepässe, Zertifizierungsstellen, PKI und staatlicher Online-Dienstleistungen in Finnland.“

## ÜBER ENTRUST

Entrust ermöglicht vertrauenswürdige Identitäten und Zahlungen sowie verlässlichen Datenschutz und hält damit die Welt sicher in Bewegung. Ein nahtloses und sicheres Umfeld ist heute mehr denn je unerlässlich, sei es bei Grenzüberritten, beim Einkaufen, beim Zugriff auf E-Government-Dienste oder beim Einloggen in Unternehmensnetzwerke. Entrust bietet für genau diese Interaktionen eine unübertroffene Bandbreite an Lösungen für digitale Sicherheit und die Ausstellung von Berechtigungsnachweisen. Mit 2.500 Mitarbeitern und einem weltweiten Partnernetzwerk ist Entrust für Kunden in über 150 Ländern tätig, die sich bei ihren sensibelsten Operationen auf uns verlassen.



Weitere Informationen auf  
[entrust.com/HSM](http://entrust.com/HSM)



**ENTRUST**