Finland protects the integrity of electronic IDs and EAC e-passports with Entrust

Entrust nShield® hardware security modules (HSMs) ensure the authenticity of Finland's e-passports with fingerprints secured by digital certificates.

With one of the world's most electronically enabled populations, Finland has long been a leader in delivering online government services that take advantage of effective identity and access management. The country's Population Register Centre (PRC) provides a clear example. It operates national public key infrastructures (PKIs) and Certification Authorities (CAs) secured with Entrust nShield HSMs to issue unique and verifiable digital identities, called Citizen Certificates, to all residents. Residents can use their Citizen Certificates to access secure online government services efficiently and cost effectively. So when Finland needed the PRC to use similar technology to issue new e-passports to comply with the latest European Union (EU) directives on electronic ID issuance, the PRC knew from experience where to turn to ensure the integrity of the process – Entrust.

> **« The PRC is very experienced in delivering online government services through PKI deployment and the issuing and use of digital certificates. In our opinion, Entrust nShield HSMs are an excellent solution to protect private keys. »**
>
> – Jan Partanen, Population Register Centre of Finland

Finland Population Register Centre

According to Jan Partanen, development manager for the Population Register Centre of Finland, "The EU's new e-passports are the most secure in the world because they are protected by tamper-proof digital certificates. However, the system will only work if countries secure – without fail – the signing keys that guarantee the authenticity of the digital certificates. With Entrust nShield HSMs protecting the signing keys for Finland's CAs, PKI, and electronic ID issuance, we are confident in our ability to ensure the integrity of Finland's e-passports and online government services."

ENSURING SECURITY AND PRIVACY

Every person's fingerprint is uniquely their own. The EU is taking advantage of this simple fact to ensure that only the correct person can use a passport to travel. How? Based on the Extended Access Control (EAC) standard, the EU's second generation of e-passports allows governments to leverage a stronger biometric (typically a fingerprint or iris scan) that is more difficult to impersonate. EAC e-passports will protect the passport holder's privacy while ensuring the validity of passports. Once the new e-passport process is fully implemented it will become virtually impossible for anyone to travel under an assumed identity with a fake EU passport. The EAC scheme requires European Union Member States to add fingerprint data to machine-readable travel documents (MRTDs).

Whether they are used to protect e-passports, PKIs, or electronic IDs, digital certificates are secure because they are issued by a trusted CA using its unique signing key. However, if a signing key were ever compromised or stolen, someone could issue a seemingly valid digital certificate. Because HSMs provide a tamper-resistant environment that is significantly more secure than software, the EU mandates their use to generate, store, and protect the CA signing keys for e-passports.

A HISTORY OF SUCCESS

Historically, the Finnish government has relied on HSMs to protect its national CAs and PKIs, so from the beginning the PRC knew that it would prefer to use HSMs to protect the integrity of its e-passports. HSMs have proved to be secure and trouble free, integrating seamlessly with the country's CAs for issuing certificates. HSMs are certified to Federal Information Processing Standard (FIPS) 140-2 level 3, which is the most widely adopted security benchmark for cryptographic solutions in government and commercial enterprises, and is mandated by the EU EAC e-passport standard. Just as crucially, the Entrust professional services team offered expertise in both e-passports and key management to help the PRC establish an efficient – and cost-effective – e-passport issuance process.

"The PRC is very experienced in delivering online government services through PKI deployment and the issuing and use of digital certificates," notes Mr. Partanen. "In our opinion, HSMs are an excellent solution to protect signing keys. Of course, key management is also important. The Entrust professional services team has excellent key management expertise, together with a record of delivering trusted solutions. We did not hesitate in choosing the Entrust professional services team and Entrust nShield HSMs to secure our e-passports."

Finland Population Register Centre

> **With Entrust nShield HSMs, our signing keys never leave the security of the hardware module, so they are never exposed to misuse. HSMs and digital certificates can seem complex, but the result of using them is simple for us. They ensure the integrity of Finland's e-passports, CAs, PKIs, and online government services.**
>
> – Jan Partanen, Population Register Centre of Finland

THE E-PASSPORT PROCESS

Working with the Entrust professional services team, the PRC has developed and implemented a new e-passport issuance process that complies with EU standards and protects the privacy of its citizens. The new e-passports contain a chip embedded with a digital certificate and the passport holder's fingerprint. The country's root CA issues each certificate using signing keys securely generated and protected within an Entrust nShield HSM. As the signing keys never leave the security of the HSM, they are never exposed to misuse. At border crossings, a passport reader will be able to verify the identity of the passport holder. Only devices authorized by digital certificates will be able to read the passports, protecting the passport holder's privacy as well as ensuring the validity of the passport.

COST-EFFECTIVE AND HIGHLY AVAILABLE

The PRC opted to use the network-attached Entrust nShield Connect HSM in its e-passport process rather than an HSM that works with a single server. By networking its HSMs, PRC saw two important advantages; firstly, because the nShield HSM serves multiple servers, the PRC did not need to purchase one HSM for every server in its e-passport PKI, reducing hardware costs. The second advantage was that the HSM efficiently supported high availability and scalability, with automated failover allowing seamless switching between HSMs.

"The Entrust nShield HSM offered a definite cost and availability advantage because one device can support several servers and applications at the same time," explains Mr. Partanen. "It also delivers all the security features we would expect from an HSM, including separation of duties in administration to protect devices from internal manipulation."

PROTECTING PROCESSES AND CITIZENS

As Finland issues e-passports that include fingerprints protected by digital certificates, Mr. Partanen points to the potential consequences of errors as the driving force behind the value of HSMs. He says, "In the case of e-passports, compromised signing keys would mean that criminals or terrorists could issue counterfeit passports. Or if keys were used to unlock the e-passport itself, citizens' privacy could be irrevocably damaged.

Finland Population Register Centre

BENEFITS WITH ENTRUST

- Enabling the electronic verification of identity
- Protecting the integrity of e-passports and the privacy of citizens
- Preventing passport fraud, counterfeiting, and misuse
- Securing the delivery of online government services

ORGANIZATION PROFILE

Founded in 1969, the Population Register Centre of Finland maintains population and identification information relating to the people and buildings in Finland. It is dedicated to serving the people of Finland by delivering high-quality identification solutions for online and other services.

To learn more about the PRC, visit: www.vrk.fi and www.fineid.fi

By deploying Entrust nShield HSMs, our signing keys never leave the security of the hardware module, so they are never exposed to misuse. HSMs and digital certificates can seem complex, but the result of using them is simple for us. They ensure the integrity of Finland's e-passports, CAs, PKIs, and online government services."

ABOUT ENTRUST

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com