High-scalability keystore

Handle millions of keys concurrently with high performance

HIGHLIGHTS

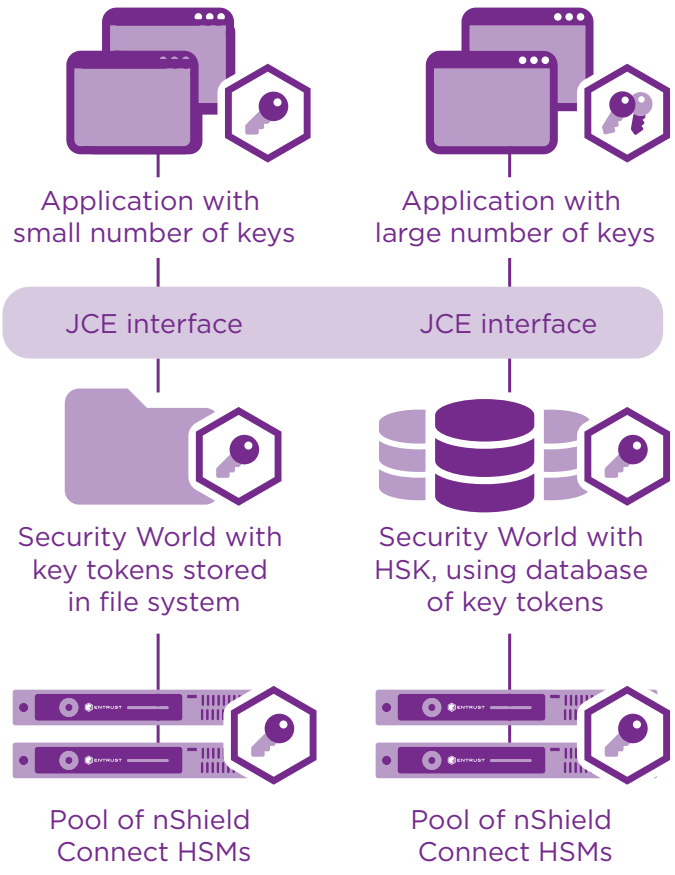
- A high-performance, highly-scalable solution for specific Entrust nShield® HSM use cases
- Supports very large numbers of concurrently active cryptographic keys
- Avoids operating system bottlenecks
- Supports RSA key generation, Certificate Signing Request (CSR) generation, digital signature creation and verification, data encryption and decryption.
- Automatic synchronisation between multiple calling computers
- Customisable extensible solution to fit your needs

Some hardware security module (HSM) use-cases need to handle very large numbers of cryptographic keys concurrently. This can cause bottlenecks in the file system of the computers connected to the HSMs. The high-scalability keystore (HSK) supports very large numbers of keys with high performance.

Key features

The HSK solution provides the following features:

- Scalable to millions of RSA keys
- Performance remains essentially unchanged as the number of keys increases



LEARN MORE AT ENTRUST.COM/HSM

High-scalability keystore

How it works

Entrust nShield HSMs provide high-performance transaction throughput, supporting thousands of transactions per second. (Performance depends on the HSM model and the specific cryptographic operation. See the data sheets for specific nShield models for the latest details on HSM performance.)

Entrust's flexible and secure Security World architecture stores cryptographic keys external to the HSM, as "tokens". The keys within the "tokens" are strongly protected under HSM master keys, using encryption, usage constraints, access controls, and authentication security. This combines very strong security with benefits of scalability, load-balancing, failover, easy expansion or contraction of the number of HSMs in a pool, swapping HSMs into and out of the pool, and easy backup of key tokens without the need for additional backup devices.

The standard Security World architecture stores these "tokens" in the file systems of the calling computers (with synchronisation support), using a single file per token. This approach suits most use cases which typically have a limited number of active keys per client computer.

In certain use cases, nShield HSM performance can be constrained by latencies present in the file system of the calling computer's operating system. HSK provides high performance when there are very large numbers of keys by using a database, rather than the file system, to store the key tokens on the client computer.

The Entrust Professional Services (PS) team will help you assess whether the HSK is suitable for your needs. PS consultants will also provide expert developer support to assist you in integrating HSK into your environment, including customizing HSK to suit your specific requirements as needed.

Example use cases

- Corporate email security for large numbers of users
- Enterprise document signing
- Internet of Things (IoT) with large numbers of connected devices
- Mobile apps with a large number of end-users
- eWallet systems for cryptocurrency exchanges

Technical details

- Java Cryptography Extension (JCE) library, using nShield HSMs
- RESTful JSON Web Services option
- Stores nShield HSM key "tokens" in a database rather than in the file system
- Works with popular relational database software, including MSSQL, Oracle and Derby (with additional databases being added)
- Works with a single HSM or multiple HSMs in a load-balanced pool

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com

Entrust is a trademark, registered trademark, and/or service mark of Entrust Corporation in the United States and/or other countries. ©2020 Entrust Corporation. All rights reserved. October 2020 • PLB9600