THALES

> Thales nShield Edge

KEY BENEFITS

> Protects cryptographic keys in secure hardware

> Supports laptops and virtual machines

> Provides dual control access for valuable keys

> Enables secure backup of keys

> Shares management with other nShield HSMs

> Provides practical solution for offline CAs

> Protects keys for registration authorities

> Controls key use for code signing

> Facilitates remote nShield HSM operations

> Simplifies HSM application development

> Readily integrates with third-party applications

> Delivers FIPS compliance

USB-attached hardware security module for offline CAs, code signing, and HSM management

nShield Edge is a portable hardware security module for use in offline certification authorities (CAs) and registration authorities (RAs), code signing, and remote HSM operations. It combines a full-featured HSM with a smart card reader in one device, offering secure backup and dual control access of an organization's high-value keys with low transaction volumes. Its USB connectivity makes it especially suitable for use with laptops and virtual machines. nShield Edge's security boundary is tamper-resistant against physical attacks and validated up to FIPS 140-2 Level 3.

www.thalesgroup.com/iss

>> Thales nShield Edge

Protects keys in secure hardware

nShield Edge enables enterprises to add hardware protection to critical applications, such as offline CAs, registration authorities, and code signing. Using standard cryptographic interfaces including, nShield Edge integrates readily with Microsoft Certificate Services (PKI), Entrust Authority Security Manager, RSA Certificate Manager, Microsoft Authenticode, and many other applications.

Supports laptops and virtual machines

nShield Edge is a USB-attached HSM that easily integrates with laptops. About the size of a double CD case, it is highly portable and draws its power from the USB connection.

nShield Edge provides an ideal solution where virtual machines need to access a local HSM, as in the case of offline CAs or development environments.

Provides dual control access for valuable keys

Unlike USB crypto tokens, nShield Edge can require a quorum of trusted individuals to be present to authorize a signature or decrypt sensitive information. This ensures that no single individual can circumvent policies and defraud the system, or simply walk out of the door with a copy of the key. nShield Edge verifies the identity of the individuals through smart cards with passphrases, which need to be inserted into the integrated smart card reader.

Shares management with other nShield HSMs

nShield Edge can be managed in the same Security World as nShield Solo and nShield Connect to reduce the total cost of ownership in large HSM deployments because staff don't have to be trained on different management systems.

Provides practical solution for offline CAs

To protect the offline CAs from being compromised, machines hosting the CAs are often locked away in vaults, so laptops have become a natural choice due to their size. Because many offline CAs have a life span of 10 or 20 years, it has also become industry best practice to run CAs in virtual machines, which can be run independently of the hardware. Many virtualization techniques are able to connect from a guest system to a USB-attached piece of hardware.

A USB-connected, small, and highly portable HSM, nShield Edge is ideally suited for offline CAs running in virtual machines or on laptops.

Protects keys for registration authorities

nShield Edge is equally suited for protecting infrastructure and agent keys in registration authorities, which are often located close to the end-users, for example in local HR offices, where the cards can be personalized. nShield Edge enables the RA agent to fulfill all tasks without compromising key security. For critical operations, nShield Edge can require a quorum of two or more people to be present to authorize a transaction.

Controls key use for code signing

nShield Edge can enforce a quorum of authorized people to approve code with two-factor authentication credentials. Even if one of the credentials is lost or stolen, the code signing key is not compromised or lost. nShield Edge also supports a secure backup that enables an organization to securely recover the key in an emergency.

Facilitates remote nShield HSM operations

Using the optional Remote Operator, nShield Edge's portability makes it ideal for security personnel who need to remotely operate other nShield HSMs. Its USB connection makes it the natural choice for use with administrative laptops.

Simplifies HSM application development

nShield Edge is perfectly suited for application developers who want to develop and test HSM integrations into their application, especially if the developer is using a laptop. Its size makes it the ideal personal HSM to be used by developers at their desk. Developers can also run the application inside a virtual machine for testing.

For more information, please see
www.thalesgroup.com/iss

Thales - Information Systems Security