White Paper

The nShield Security World architecture

Optimizing security and operational efficiency in Entrust nShield HSM environments

ENTRUST

SECURING A WORLD IN MOTION

Contents

EXECUTIVE SUMMARY

Today's security teams continue to contend with expanding IT environments, escalating security threats, and increasingly rigorous compliance mandates, which means their reliance on hardware security modules (HSMs) continues to grow as well. With nShield HSMs and Security World, security teams can gain the flexibility and efficiency they need to scale their HSM operations – while maximizing security. With these offerings, organizations can establish secure, efficient, and uniform control over their HSMs, operational policies, and keys.

INTRODUCTION

The imperative for scaling HSM operations

As security teams seek to address their organization's evolving security requirements and compliance objectives, the use of encryption continues to see rapid growth. Consequently, the use of HSMs continues to proliferate. Delivering high-assurance security to cryptographic systems, HSMs represent a fundamental building block in today's IT environments. HSMs are essential for establishing a trusted layer that enables secure generation, storage, and management of cryptographic keys and materials.

As the number and scope of encryption use cases continues to expand, it's imperative that security teams acquire the ability to scale their HSM operations, while keeping costs and administrative efforts under control. With nShield HSMs and the Security World architecture, organizations can leverage the capabilities they need to scale their implementations, while maximizing cost and operational efficiency as well as security.

nShield HSMs and Security World

Entrust delivers comprehensive and advanced data security solutions, enabling customers to establish strong protections across devices, processes, platforms, and environments. Our solutions feature the following offerings:

nShield HSMs

nShield HSMs are hardened, tamper-resistant devices that protect customers' most sensitive data. nShield HSMs provide a secure environment for generating strong cryptographic keys and performing cryptographic operations, including encryption, decryption, signing, and verification. With nShield HSMs, keys never leave the physical HSM in an unprotected form.

nShield HSMs support a variety of deployment scenarios, featuring these offerings:

- **nShield Connect.** Network-attached HSM appliances that deliver high-performance cryptographic services to applications across the organization.
- **nShield Solo.** Low-profile PCI-Express card modules that deliver cryptographic services to applications hosted on a server or appliance.
- **nShield Edge.** Portable, USB-based desktop devices designed for convenience and economy.

nShield Security World

The Security World architecture supports a specialized key management framework that spans the entire nShield family of general purpose HSMs. This architecture provides a unified administrator and user experience and guaranteed interoperability whether the customer deploys one or hundreds of devices.

Through Security World, customers can easily establish a logical security boundary for managing groups of HSMs. By leveraging this architecture, security teams can realize the following advantages:

- **Enhance security.** With Security World, administrators can leverage high assurance controls for HSM administration, and institute strong, granular controls over the access and usage of application keys. Teams of security administrators can employ powerful separation of duties capabilities by establishing controls that require a specific number of administrators to perform sensitive functions. While keys can be shared across the Security World domain, they never exist outside the HSM in an unencrypted format.
- **Reduce operational costs.** As opposed to other alternatives that require back-up HSMs and manual, labor-intensive HSM cloning efforts, Security World enables simple, automated backups of HSM files. With Security World, teams can back up HSM files using existing file management processes, and they can securely manage keys in the more affordable application layer, rather than the HSM layer.
- **Enhance operational efficiency.** Security World offers organizations a way to centrally and efficiently manage all the nShield HSMs they have in their environment. Whether they're running two or 200 nShield HSMs, teams can establish unified policy and operational administration. The architecture significantly reduces the effort associated with manual, direct administration of keys on each HSM. Instead, policies can be established once, and applied consistently across the environment. Through this centralized approach, organizations can more efficiently support not only more HSMs, but more business applications.
- **Increase resilience.** Security World makes it easy to establish seamless and robust load balancing and failover capabilities so teams can optimize performance and ensure there's no single point of failure in their HSM operations. Security teams can efficiently add or replace HSMs in their Security World domain.
- **Flexibility and scalability.** Security World equips teams with the flexibility they need to align their HSM operations with their organization's specific environment, operational approaches, and security needs. Depending on their requirements, security teams can manage key authorization in a manual or fully automated fashion. For example, in transactional environments, operations can be pre-authorized and performed on demand, while highly sensitive tasks can require the manual intervention of multiple administrators. Security World offers rapid scalability, making it easy to add HSMs to an existing group, whether to boost performance, expand load balancing and failover, or increase key processing capacity.

How it works

Security World enables application keys to be managed by multiple HSMs, while ensuring alignment with policies and controls, so the security of keys isn't compromised. Following are the fundamental attributes of the Security World architecture.

nShield Security World: creation and management

A Security World domain is created on an nShield HSM. The HSM generates a master key for the Security World domain and writes a set of smart cards, which are referred to as the Administrator Card Set (ACS). (More information on these card sets is available in the "Authorization Token" section below.)

The primary use of these ACSs is to authorize the programming of the same Security World master key into other nShield HSMs, which makes them part of the same Security World domain. In this way, security teams can add HSMs into the Security World domain, whether they want to add an HSM to expand cryptographic processing capacity, or to replace another HSM. These operations can only be executed by a quorum of security officers equipped with ACSs.

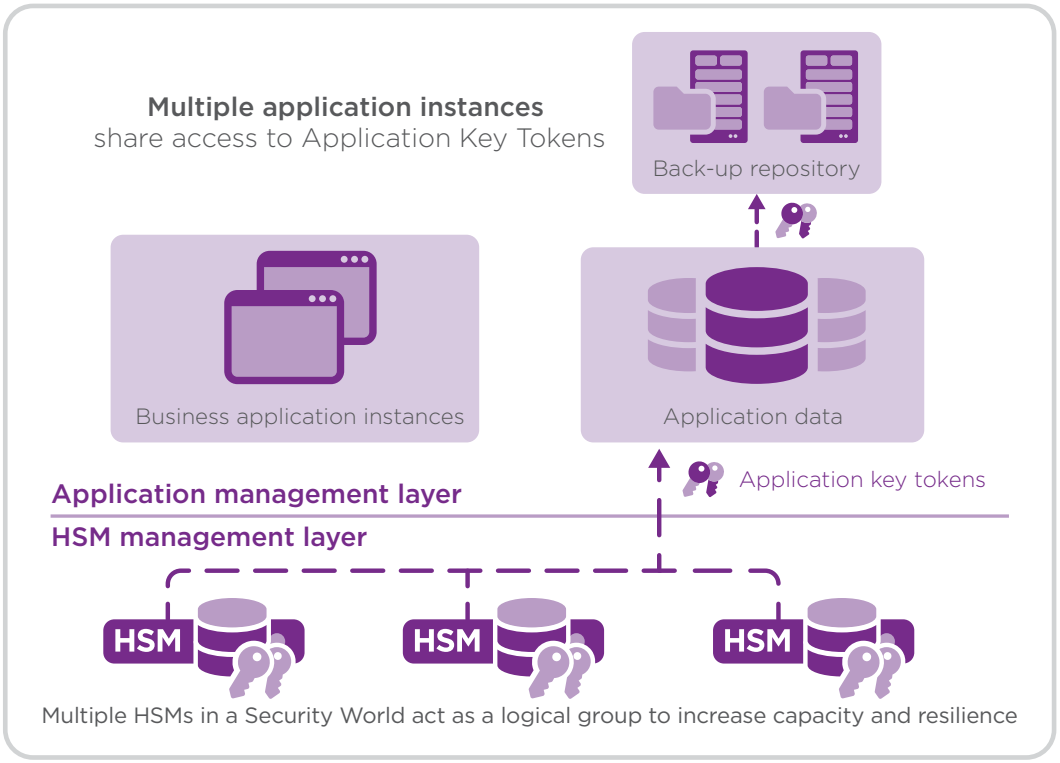


Figure 1. In a Security World deployment, security teams can uniformly manage logical groups of HSMs.

Application key tokens: wrapping of application keys

The Security World architecture is dedicated to the security of sensitive keys, including the keys that are employed within user applications. Application keys can include the following:

- Private signing keys associated with an e-invoicing application
- Private keys used as part of a TLS/SSL handshake process
- Secret symmetric keys used to encrypt credit card numbers
- Root of trust keys used to protect subordinate column-level encryption keys in a database encryption deployment

Process: how application key tokens are created

When application keys are generated in a Security World domain, the nShield HSM encrypts them using the Security World master key and converts them into application key tokens.

Once the application key tokens are created, client applications can load them onto any nShield HSM in the Security World domain. As a result, administrators do not have to access or modify the application key itself to authorize its use by another HSM in the domain.

Since they are stored as regular files on the client host, application key tokens can also be replicated on all authorized HSM clients, and can be backed up onto recovery media. Once an application key token is created, it can only be unwrapped within an nShield HSM belonging to the same Security World domain, and the application key within can only be accessed in accordance with the policies that have been established.

Application key token components

The application key token consists of the following categories of components:

Key material

Key material is composed of the application key, which is encrypted via the AES 256 bit algorithm. Users can choose which encryption key to use, which determines the authorization method for the application key. Following are two options available:

- First, the key can be encrypted using the Security World master key, which means any client application can load and use the resulting application key token, without further authorization, on any nShield HSM that is part of the Security World domain. This is referred to as a module protected key.
- Second, the user can employ an authorization token. When this approach is used, an authorization requirement must be met every time a client application loads a key onto an nShield HSM in Security World. (More information is available in the "Authorization Token" section below.)

Certificates and records of state

When HSMs produce a key, a key generation certificate is created, which is also included in the application key token. The public key that was used to sign the key generation certificate is also included.

At the moment the HSM generates the key, the HSM's state is recorded, offering a granular record of control and ownership. The state information provides a complete picture of the HSM that generated the key, including its identity and provenance.

Each nShield HSM has a long-term fixed key that is generated when the HSM is manufactured, and never changes throughout the life of the HSM. This key signs the state message, and includes a certificate or "warrant" signed by Entrust. The key that signs the warrant is always under the exclusive control of Entrust, proving that the HSM that generated the key is a genuine nShield HSM.

Access control lists (ACLs)

ACLs are a significant part of the metadata included in the application key token. Within Security World, there are a number of mechanisms used to ensure the security of ACLs. The ACL is wrapped along with the key when the key is generated; ultimately the ACL is kept as secure as the key itself, and stays with the key throughout its lifecycle. When keys are generated, the application gives the ACL one-time usage. The ability to generate an encrypted copy of a key for inclusion in the key token can only be done once, during the session in which the key is generated.

The ACL determines the capabilities of the key, including whether it can decrypt or encrypt, whether it can be wrapped by other keys or be used to wrap other keys, and more. ACLs can specify what authorizations are required for a specific operation to be performed. ACLs can be used to establish a very simple scenario, enabling a key to encrypt data, for example, or they can define complex hierarchies of keys that must be loaded, using respective tokens, before selected operations can be executed. In addition, ACLs can establish limitations on a key, such as time-out intervals or the number of permitted operations.

Authorization tokens

In Security World environments, authorization tokens can be used to approve the loading of specified keys. The authorization token is associated with the application key when the application key is generated. As a result, the application key will then require the authorization token to be presented and validated before the key can be loaded onto an HSM.

Within Security World environments, there are two forms of authorization tokens:

- **Sets of smart cards.** Through smart card sets, security teams can establish quorums, or a minimum number of cards that are required to perform a specific task. For example, in an environment with five administrator smart cards, three cards may be required to authorize the addition of a new HSM into the Security World domain. There are two categories of smart card sets in a Security World domain: an ACS, which is used to authorize administrative tasks and disaster recovery, and one or more Operator Card Sets (OCS), which authorize HSMs to use application keys.
- **Softcards.** Softcards employ a single-factor authorization model, offering a practical alternative in scenarios in which it is impractical to gain physical access to HSM smart card slots.

The key usage authorization method is chosen when the key is generated and stored in Security World. Administrators can implement key usage authorization policies in their organization by selecting the appropriate authorization method for each application key. Users can choose module protection (see above), an OCS or softcard.

When OCSs are selected, administrators can choose from a number of options. They can define how many cards are in a set and how many cards are required to conduct an operation. They can also define the passphrase for each card and whether to have a passphrase at all. Finally, they can specify whether cards remain in the nShield HSMs' readers or are removed after use. These capabilities offer an extremely versatile and powerful way to implement policies.

Capabilities for policy enforcement

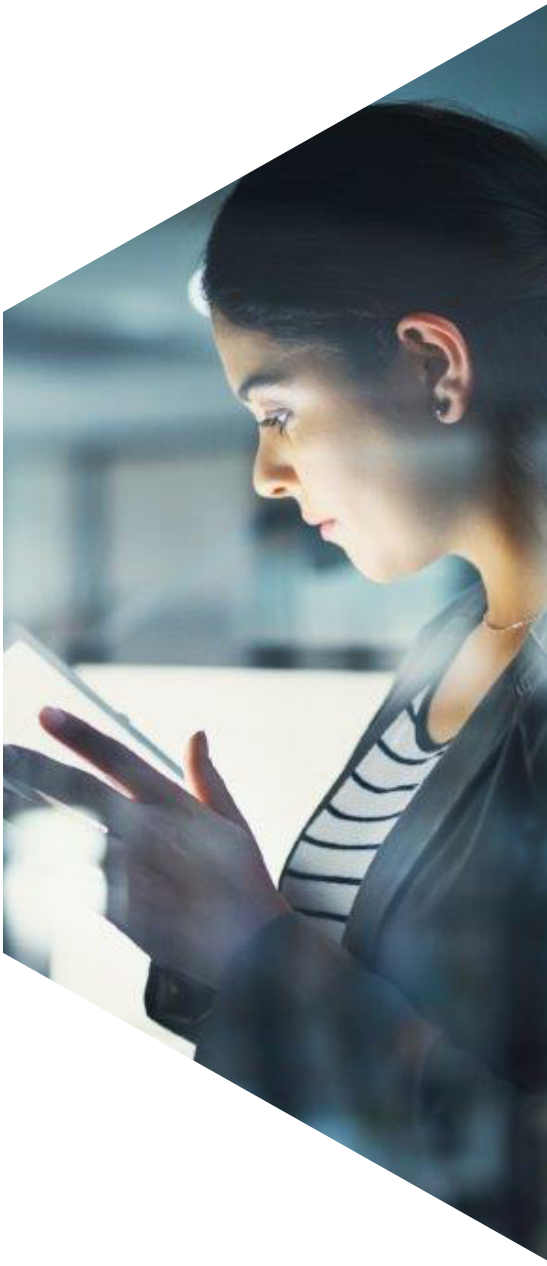
Through the capabilities outlined above, application keys can be encrypted and safely distributed and stored outside of the HSM, and across multiple HSMs, without in any way degrading the security of the keys. By leveraging the controls afforded through smart cards, HSM policies, ACLs and more, security teams can implement uniform policies across their environment, while having the ability to apply controls to specific HSMs, technology environments, user groups and so on.

In Security World environments, raw key material is always protected by certified nShield HSMs. Once saved to storage outside of the HSM, application key tokens can be backed up and restored using normal backup procedures. Client applications designed to perform authorized cryptographic operations can load application key tokens back onto any HSM in the Security World domain. There are three ways to enforce key loading and usage policies:

- **Access to application key token.** If the application key token doesn't exist on an application server, that server simply cannot load that key onto a target HSM. This policy is enforced outside the HSM, through synchronization of specific application key tokens across the application server estate.
- **Token authorization.** If a key is protected by an authorization token, such as a softcard or a smart card set, users must present that token before they are permitted to load the key into the HSM. This policy is enforced inside the HSM.
- **ACLs.** Once an application key token is loaded and unwrapped on an HSM, the application key can only be used for specific purposes and under specific conditions, as described in the ACL that is bundled in the application key token. This policy is enforced inside the HSM.

CONCLUSION

As organizations continue to contend with escalating threats and increasing security and compliance demands, the need for cryptography and HSMs will only continue to grow. With nShield HSMs and Security World, organizations can address their expanding HSM requirements – while maximizing operational and cost efficiency and security. By leveraging these offerings, organizations can more effectively adapt to their evolving technological environments, security imperatives, and business objectives.



For more information

Visit us at **entrust.com/HSM** to learn how we can protect your business critical information and applications, on your own premises, in the cloud and in virtual environments.

To find out more about Entrust nShield HSMs

HSMinfo@entrust.com
entrust.com/HSM

ABOUT ENTRUST CORPORATION

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