Entrust CodeSafe®

Enabling application code to run within the protected confines of a tamper-resistant Entrust nShield® hardware security module (HSM)

ENTRUST

SECURING A WORLD IN MOTION

Are you:

- Seeking to overcome data security concerns to exploit cloud and internet channels?
- Worried over insider attacks and malware impacting your security-sensitive applications?
- Interested in executing these applications inside a protected environment to achieve a higher assurance system?

Learn how to:

- Deploy a security architecture that protects you from threats directed at servers where security sensitive cryptographic applications typically reside
- Employ code signing techniques to eliminate the risk of unauthorized application changes or malware infection
- Use Entrust's unique CodeSafe technology to run these applications within a FIPS 140-2 Level 3 certified environment and strengthen your data security posture

Contents

Introduction

Why are security-sensitive applications vulnerable?

Business applications running on host servers are perennially vulnerable to advanced persistent threats (APTs) introduced through malware as well as insider attacks and hacking. Attacks can compromise and disrupt critical government and enterprise operations and lead to massive costs and interruption of services. While many applications today employ built-in cryptography to safeguard the confidentiality and integrity of the sensitive data they process, it is still possible to manipulate these applications within the host server environment.

How can hardware security modules (HSMs) help?

Industry best practices prescribe the use of HSMs to store and manage sensitive keys used by the cryptography employed by security-sensitive applications. Traditionally, HSMs provide a protected environment for cryptographic processing and a trusted mechanism to enforce established security policies on key use.

How can you further protect security-sensitive applications?

While the use of HSMs enhances the security of applications running cryptographic processes by safekeeping and managing the keys used for encryption and digital signatures, safe key storage and management alone cannot guarantee the trustworthiness of security-sensitive applications. In today's threatened environment, applications that initiate cryptographic processes can be manipulated by insider attacks, malware, and Trojans that can exist within the enterprise application layer. For this reason, applications that request cryptographic processes of security-sensitive applications should also be executed within a protected environment.

In order to ensure robust protection of security-sensitive applications, validation of application integrity, tamper-resistant execution, and a strong binding between the application and the cryptographic processes supported is necessary. It is this need that Entrust CodeSafe is designed to address.

The problem

Security mechanisms associated with host servers can be defeated by insiders and/or network attacks that can find conduits for malware to be introduced into the host system. Moving the security-sensitive cryptographic processes of these applications within an HSM makes them inaccessible to these attacks. CodeSafe ensures the integrity of security-sensitive applications by:

- Isolating them from attacks that can directly or indirectly manipulate, disrupt, or deny operations
- Signing and authenticating security-sensitive applications when they are loaded into the HSM

CodeSafe enables customers to strengthen their security posture beyond the level already afforded by the HSM – including safeguarding sensitive key material, facilitating its lifecycle management, and providing a trusted mechanism that:

- Renders any unauthorized software changes impossible
- Prevents data from being copied to disks or external repositories
- Protects against super users who might read memory space at will

CodeSafe enables customers to strengthen their security posture beyond the level already afforded by the HSM.

What is CodeSafe

Entrust CodeSafe is a powerful capability that enables application code to run within the protected confines of a tamper-resistant nShield HSM. CodeSafe prevents potential rogue commands from being executed by protecting the software that initiates cryptographic processes. Supported on all FIPS 140-2 Level 3 versions of the nShield HSM family (except nShield Edge), CodeSafe enables customers to develop application code to run inside the HSM. This capability protects security-sensitive cryptographic processes from the otherwise threatened application server environment and creates a trusted space within the nShield HSM alongside associated key material.

CodeSafe encompasses two components: a developer toolkit to compile applications and prepare them to be imported into the HSMs, and a run time environment that protects the application when in use. CodeSafe not only carves out a segregated and protected space for security-sensitive applications to be executed, but it also creates a strong binding between the cryptographic processes and the keys they use (see Figure 1). This important binding establishes the policy that ensures that keys and data can only be used by authorized and immutable applications. CodeSafe enables users to securely deploy functions utilizing cryptography

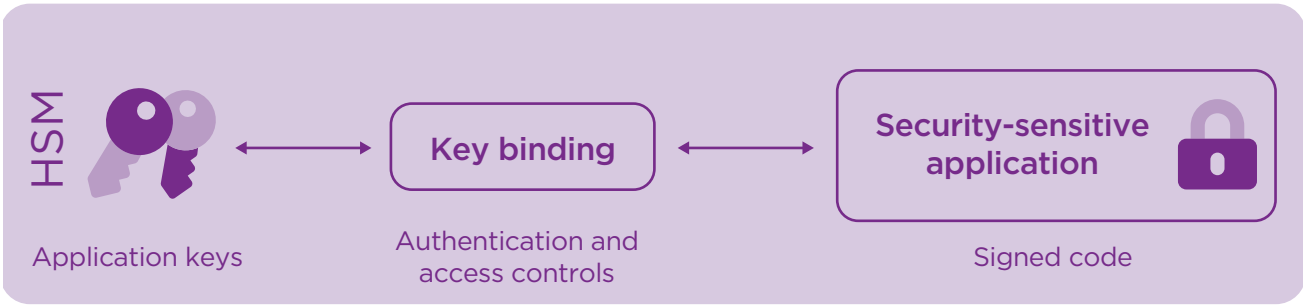

Figure 1: Schematic representation of CodeSafe working process.

alongside unattended servers or within unprotected environments where the operation of the system is outside direct supervision by controlling access to the use of private keys, non-volatile user memory, and hardware-secured time.

A typical corporate data processing environment with and without the capability offered by CodeSafe is illustrated in Figure 2. In the illustration, the Application Layer is representative of the general IT setting comprising enterprise business applications, data management functions, and backup systems. This environment is complemented with an HSM Layer shown at the bottom where specialized security functions such as cryptographic key storage and management, dual controls, and auditing are maintained. With CodeSafe, shown on the right side of the figure, the security-sensitive application is fully contained within the defined security perimeter so that a full range of services can run securely.

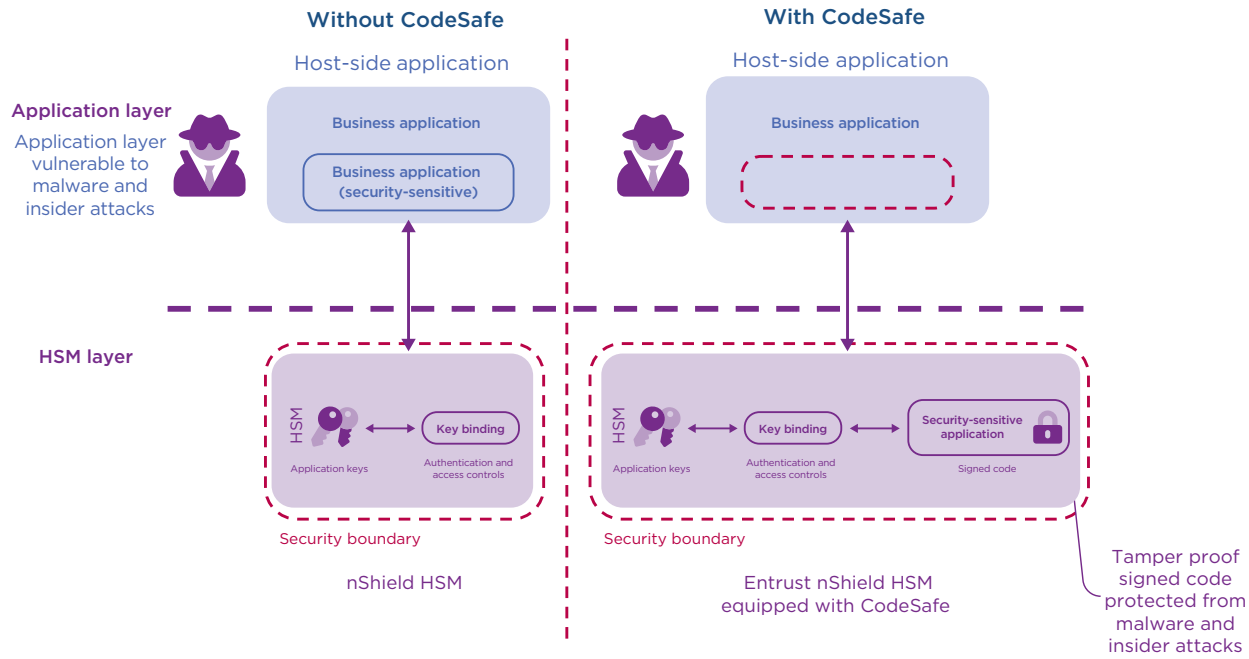

Figure 2: CodeSafe protects security-sensitive applications within Entrust nShield HSMs.

How to use CodeSafe

CodeSafe can be used to solve complex business problems where custom functionality, industry rules, or algorithms must be implemented with a high degree of trustworthiness. The product's capabilities, management options, and deployment choices are described in further detail in the following paragraphs.

CodeSafe environment and developer toolkit

CodeSafe establishes a secure environment or sandbox that application developers can use to engineer custom applications. The CodeSafe developer toolkit, activated through a license, enables this secure environment to be established.

Applications developed within this environment can then run inside the HSM. Since developing and testing software for critical enterprise processes can be a complex undertaking, the CodeSafe developer toolkit also allows testing and debugging of programs outside the HSM while developing a mechanism that binds the code to the trusted HSM's resources. As shown in Figure 3, the application development process involves an iterative test cycle requiring proper code signing and authentication for secure execution.

The CodeSafe developer toolkit allows testing and debugging of programs outside the HSM while developing a mechanism that binds the code to the trusted HSM's resources.

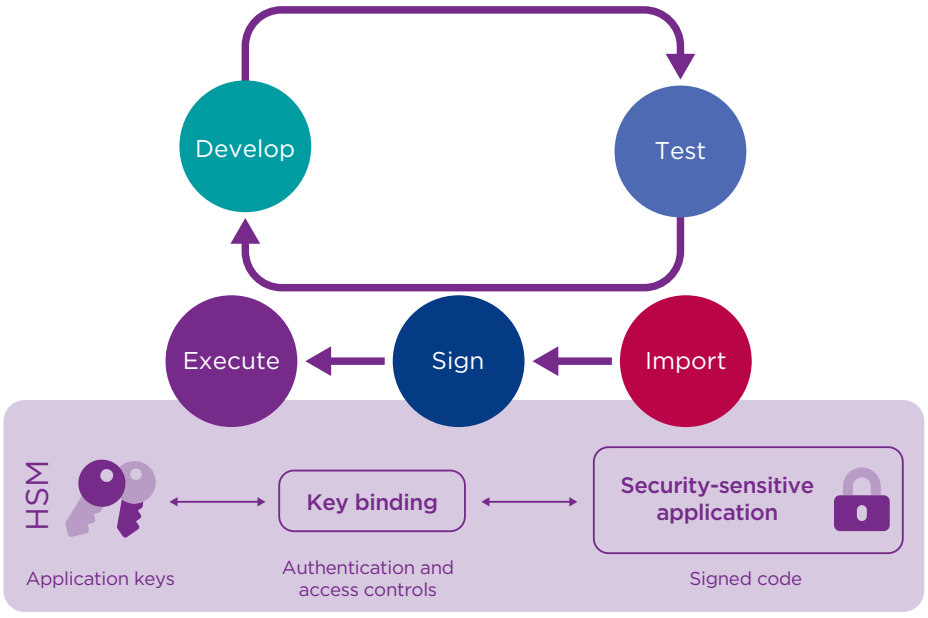

Figure 3: Application development process using CodeSafe.

Management and deployment choices

Lifecycle management of security-sensitve applications is an important consideration. CodeSafe applications can be designed to either accept commands from applications on client hosts, or to attach to a network listener or I/O descriptor on their client host. Digital signatures over the application code itself and the application instance's deployment configuration allow for secure updates to code or data, with separation of controls between developers and those tasked with deploying the built applications. The digital signature on the deployment configuration allows the application to identify itself as it is running on the HSM, and to access keys designated as restricted to instances of that application only.

Systems administrators and DevOps engineers have great flexibility in deploying CodeSafe applications; any CodeSafe application can either be instantiated dynamically by its client software, loaded onto the HSM and started at system boot time, or, through the CodeSafe direct feature, it can be deployed directly onto an Entrust nShield Connect HSM and attached to a network listener on the appliance platform. This direct connection also eliminates the need for a client machine, reducing cost and simplifying architecture.

CodeSafe enables customers to securely update and publish their own customized applications and secure execution code.

Examples of CodeSafe in action

Representative deployment scenarios where CodeSafe is used include secure content distribution, protected authentication, secure clock, and trusted counter. The following brief case studies describe these scenarios in more detail and provide a system-level view of how CodeSafe helps enhance their security.

Secure content distribution

Data exchanged over online transactions requires encryption to ensure confidentiality and integrity. While encryption is afforded through the TLS protocol, the gap mentioned earlier often leaves sensitive data in the clear in vulnerable places. To extend the protection afforded to TLS sessions, CodeSafe is used to ensure end-to-end encryption of sensitive data. CodeSafe enables re-encryption of the TLS data before it leaves the HSM and is passed to the business applications or storage servers in the IT environment.

With increasing use of web-based applications, distributing access credentials quickly and securely to authorized account holders has become a challenging process since TLS alone cannot guarantee secure content delivery to end users. CodeSafe enables sensitive data such as PINs and passwords contained in the TLS stream to be terminated and re-encrypted or tokenized

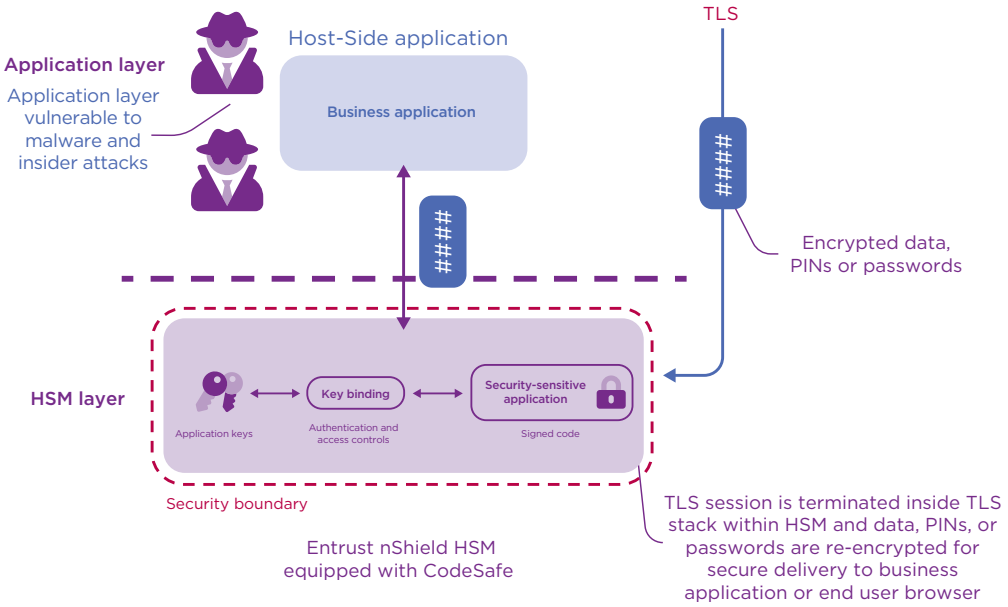

Figure 5: TLS termination and data re-encryption provides end-to-end security

all within the security boundary of the Entrust nShield HSM, before being passed to the user's browser. Enforcing strong access controls and use policies, the HSM ensures secure content distribution to the end user. A schematic representation of these scenarios is shown in Figure 5.

Protected authentication

Online banking transactions are often targets for fraudulent activity. To reduce fraud, a mechanism that safeguards the authentication process itself, beyond the host where it is often executed, provides a much higher level of assurance when validating user identities. CodeSafe protects the authentication process using the TLS termination capability and an authentication algorithm resident in the HSM. Running the authentication process from the secure confines of the HSM removes potential vulnerabilities and facilitates auditing. As shown in Figure 6, CodeSafe terminates the user's TLS session inside the HSM and uses the protected authentication algorithm within the device to validate passwords and to sign associated pass/fail responses.

> CodeSafe protects the authentication process using the TLS termination capability and an authentication algorithm resident in the HSM.

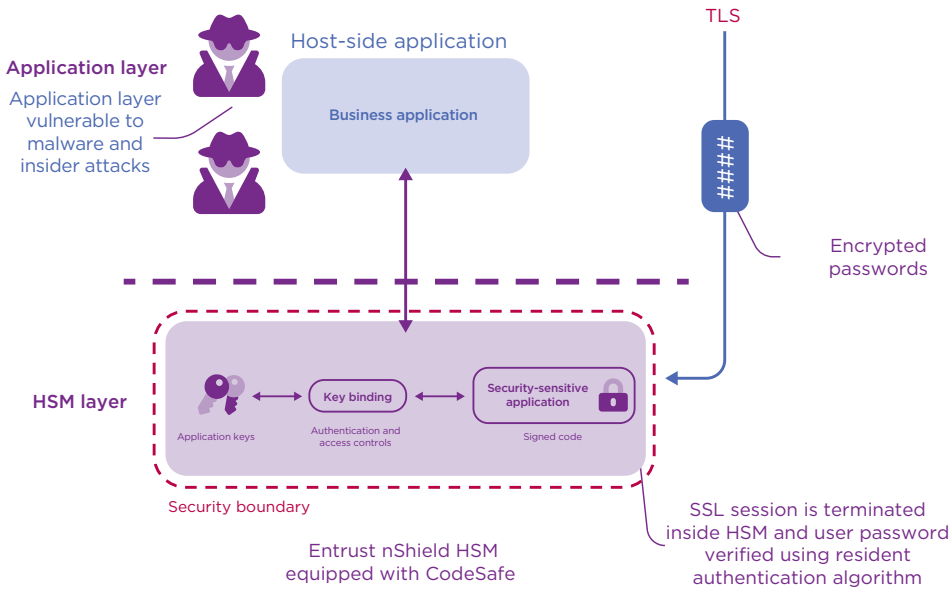

Figure 6: Entrust nShield HSM used to protect the authentication process

Secure clock

Cryptographic mechanisms such as digital signatures and hashing algorithms that use certificates issued by a public key infrastructure (PKI) depend on a trusted time source to ensure they can guarantee long-term validation of data authenticity and integrity. CodeSafe provides the capability to enable an Entrust nShield HSM to offer a trusted clock calibrated to coordinated universal time (UTC) for issuance of time stamps used to establish the state of data at a particular moment for high assurance long-term data integrity validation. An illustration of how an Entrust nShield HSM is used to provide a secure time stamping capability using the trusted clock is shown in figure 7.

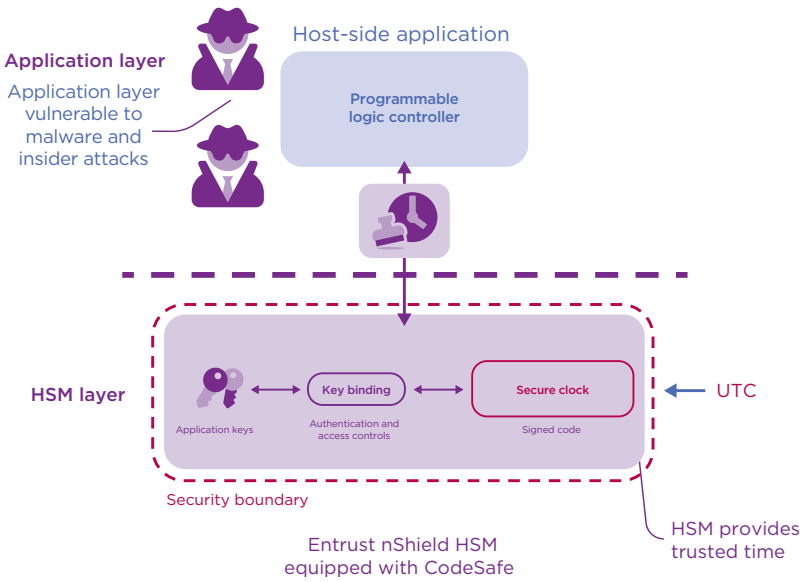

Figure 7: Entrust nShield HSM used for a secure time stamping application

Trusted counter

Business applications depend on trusted irreversible mechanisms to account for time and resources. These trusted mechanisms, or monotonic counters, are often used by product companies to control volume contract manufacturing operations with confidence. Companies running batch processes in their manufacturing facilities generate key pairs and certificates to create unique product identifiers corresponding to every unit to be produced. With the proliferation of off-shore contract manufacturing and fragmented supply chains, product companies use trusted counters together with digital identifiers and signatures in their "manufacturer's self-defense kits" against product piracy.

Protecting against piracy and counterfeiting of high-value electronic equipment requires advanced technologies. As shown in Figure 8, by placing an Entrust nShield HSM within the contract manufacturer's facility, the owner of the process is able to create a trusted business logic or counter that controls the issuance of the product identifiers for the manufacturing process, helping to ensure that only the authorized number of products is produced. Once the count of new product credentials reaches the authorized production run, the HSM stops issuing credentials and provides an alert to shut down the production process, preventing overruns that could feed the gray market and protecting owner's intellectual property.

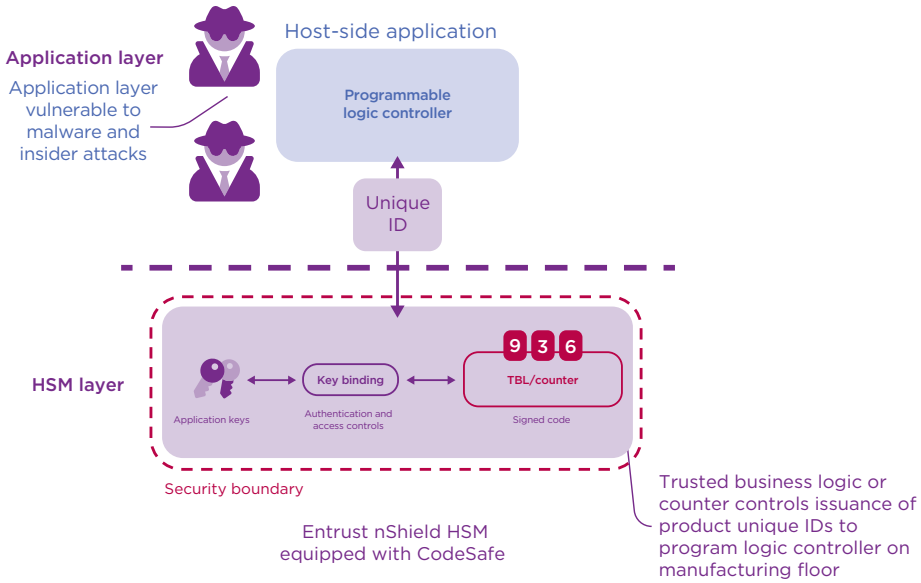

Figure 8: Trusted business logic enforces strict controls in manufacturing

Summary

The proliferation of distributed systems, outsourcing and cloud computing is making security-sensitive applications running on host servers more vulnerable and challenging to protect. CodeSafe protects applications deployed in HSMs by signing and authenticating them as they are loaded and by providing a strong binding between the cryptographic processes and the keys they use. By moving security-sensitive applications away from threatened servers in the organization's IT environment and safeguarding them within a dedicated HSM, CodeSafe prevents potential rogue commands from being executed by protecting the software within FIPS 140-2 certified hardware.

CodeSafe enables the enterprise to achieve the highest level of assurance and control over critical applications for a more robust security posture.

CodeSafe protects applications deployed in HSMs by signing and authenticating them as they are loaded and by providing a strong binding between the cryptographic processes and the keys they use.

For more information

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**

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