THALES

Thales e-Security CodeSafe®

Developer Toolkit for nShield

KEY BENEFITS

- Overcomes security vulnerabilities of host-side applications by executing them inside a trusted environment
- Safeguards critical applications from manipulation, malware and Trojans
- Enables HSM cryptographic services to be available to support a wide variety of connecting devices – from mainframes to handhelds
- Delivers certified protection with FIPS 140-2 Level 3 approved tamper-resistant hardware

Business applications running on host servers are increasingly vulnerable to a variety of attacks and advanced persistent threats (APTs) that can compromise critical operations and lead to massive costs and disruption of services. While sensitive applications often employ cryptographic mechanisms to protect sensitive data, these applications can still be the target of attack by APTs and vulnerable to manipulation unless protected within a hardened environment. The Thales CodeSafe developer toolkit provides the unique capability to move sensitive applications within the protected perimeter of a FIPS 140-2 Level 3 certified nShield hardware security module (HSM).

Software risks

Software-only systems are vulnerable to a multitude of internal and external threats and therefore are very challenging to protect. For applications that employ cryptography, increased protection is particularly important to reduce the risk of theft of private encryption or signature keys that can render the cryptography essentially useless. CodeSafe enables strong protection for applications, data and cryptographic keys.

>> CodeSafe

A trustworthy environment

CodeSafe allows sensitive applications to run within a secure environment where they are protected from a variety of attacks. CodeSafe enables developers to write applications that are securely loaded and executed on FIPS 140-2 Level 3 HSMs. Protected from manipulation, applications can decrypt, process, and encrypt data inside the secure environment. As a result, applications and data are afforded significantly increased protection.

Features

- **CodeSafe Direct** – Provides a direct TCP/IP connection, irrespective of native operating system, to an nShield HSM running secure execution code
- **Remote CodeSafe Deployment** – Enables an HSM administrator to individually upgrade and dispatch secure execution code to HSMs from a central location
- **CodeSafe SSL** – Enables sensitive data contained in secure socket layer (SSL) streams, such as PINs, personal account numbers and passwords, to be processed inside the secure boundary of a CodeSafe SSL application running in an HSM

Protect applications

A company's intellectual property may include parts of its applications—for example, the algorithm used to detect fraudulent financial transactions or the production logic in a manufacturing plant. Thales CodeSafe protects not only the data but also the application itself from theft, even in uncontrolled environments utilizing outsourcing and contracting.

Thales CodeSafe also protects sensitive applications from manipulation by hackers or rogue administrators by providing the ability to digitally sign trusted applications so that their integrity is verified prior to launch.

Prevent intellectual property theft

Delivers remote control of sensitive applications no matter the environment

- **Clientless approach** – Enables cryptographic services to be offered regardless of the operating system or configuration used by the customer, whether server or mainframe
- **Remote application updates** – Allows application or handheld owners to maintain up-to-date application execution environment without physical presence

Never expose sensitive SSL data

Most SSL connections are decrypted inside the web server, opening a security gap. Thales CodeSafe safeguards sensitive data by providing true end-to-end SSL encryption.

- **True end-to-end encryption** – Terminate SSL inside a Thales HSM, keeping data safe from attacks by hackers or rogue administrators
- **Secure SSL data processing** – Sensitive data, such as PINs and passwords, is securely processed inside the HSM

Technical Specifications

Development environment:

- GNU C Compiler
- Portable Operating System Interface (POSIX) API

What's needed to get started:

- Thales FIPS 140-2 Level 3 nShield HSM
- CodeSafe Activation
- Thales CodeSafe Developer Toolkit (developers only)
- CodeSafe SSL Activation (optional)

Thales CodeSafe supports Windows, Solaris, Linux, AIX, and HP-UX. For more information please see www.thales-esecurity.com or scan the quick response (QR) code on a smart phone.

Americas: 2200 North Commerce Parkway, Suite 200, Weston, Florida 33326 • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific: Unit 4101, 41/F, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa: Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com