nCIPHER

www.ncipher.com

High assurance security for code signing

- Secures authorship, publication date and content
- Establishes software integrity
- Protects valuable code signing keys

nCipher code signing solutions

CODE DISTRIBUTION CHALLENGES

Business IT is complex and uses software from a wide variety of sources in order to run an organization. Companies who develop software, whether for internal use or to sell to their customers, need to create or support mechanisms that prove the authenticity of their software. Ensuring this security requires the following:

- Validating the signing process, so only the right code is signed by the right keys
- Managing private signing keys so that they will not be stolen, allowing unauthorized versions to reach their customers
- Providing an audit trail of all signing activity

nCipher code signing solutions

nCipher has significant expertise in developing and implementing secure code signing solutions that solve the process, integrity, authorization and private key protection challenges by providing the following capabilities:

- Code signing using nCipher nShield® hardware security modules the risk of key theft, corporate impostering, and malicious software alteration
- Enabling end users to verify the source and integrity of software and detect alteration or insertion of malicious code
- Help prevent users from abandoning installation due to operating systems' strong warning dialogs for unsigned software
- Providing access control, approval workflow, automation and auditing capabilities for code signing operations

To deliver these capabilities, nCipher offers two code signing solutions which are based on nCipher nShield hardware security modules (HSMs) as the root of trust. These solutions are:

- Code Signing Gateway
- Code Signing with Direct HSM Integration

WHAT IS CODE

Code can be viewed as a binary package of information that is consumed or executed by target platforms. Examples of code include executable packages, installer packages, firmware packages and embedded environments.

CODE SIGNING WITH NCIPHER HSMS AS ROOT OF TRUST

Code signing is the application of digital signatures to software publishing. Code signing enables end users to verify the source and integrity of software by authenticating the publisher's identity; it also helps prevent users from abandoning software installations as operating systems present strong warning dialogs for unsigned software.

The private key is critical to the security of the code signing system and must never be revealed or shared. If the private key is compromised, the trust system fails. The private signing key security underpins the code signing process.

For sensitive applications such as code signing protecting the private key both when in use and not in use is critical to creating a secure solution. HSMs provide a certified tamper resistant environment for securing keys throughout their lifecycle.

NSHIELD GENERAL PURPOSE HARDWARE SECURITY MODULES (HSMS)

nShield HSMs are certified, hardened, tamper-resistant devices that provide a secure environment for generating and protecting keys used by for a variety of applications. nShield HSMs are available in three form factors: nShield Connect, an appliance serving multiple applications across a network

- nShield Solo, a PCIe card serving applications on a single server
- nShield Edge, a USB-attached desktop device for lower volume transactions
- nShield HSMs are certified to FIPS 140-2 Level 2 and Level 3

nCipher code signing solutions

CODE SIGNING GATEWAY

For larger organizations that need a highly controlled software signing approval process, the Code Signing Gateway provides a range of flexible and centralized workflow automation functions that help software development organizations meet strong security requirements. The Code Signing Gateway is a centralized, customer-hosted server that runs nCipher code signing workflow applications.

The Code Signing Gateway manages workflow, accepts requests, notifies approvers via email, manages time-outs, acknowledges approvals, logs activity, and delivers signed code to the staging area. Multiple user roles can be supported, including, for example: Code Signing Gateway administrators, enterprise, desktop, IoT or mobile application developers, management team and the code signing approvers. Active Directory integration is used for work group authorization and authentication of users.

nCipher nShield HSMs are used to protect the private key used to sign code. The signing keys reside in the HSMs and are mapped to multiple signing profiles that can be created in the Code Signing Gateway.

The Code Signing Gateway integrates with standard signing tools such as, Oracle Jarsigner, Microsoft SignTool, the Apple code sign tool, and Android's code signing utility. The process schematic is illustrated in Figure 1.

Additional functionality includes multiple signing profiles that can be defined to utilize a number of digital certificates that support multiple signing profiles, centralized logging, file archiving, integration with a time stamp service as well as integration with Microsoft Windows Defender for checking files for viruses before signing.

The nCipher Codes Signing Gateway is customized solution for each customer's unique environment by the nCipher Advanced Solutions Group (ASG).

CODE SIGNING WITH DIRECT HSM INTEGRATION

Direct integration with a nCipher nShield HSM provides a solution for a small number of developers with simple separation of duties. It is typically used for individual developer workstations or dedicated code signing servers. The private key used for code signing is generated and protected by the nShield HSM.

Code signing integrates with the HSM using standard APIs, for example Java Cryptography Extension (JCE) and Microsoft CAPI and CNG and uses third-party tools such as Jarsigner, SignTool and Open SSL to create signing requests for execution by the HSM.

LEARN MORE

To find out more how nCipher Security can deliver trust, integrity and control to your business critical information and applications, visit ncipher.com

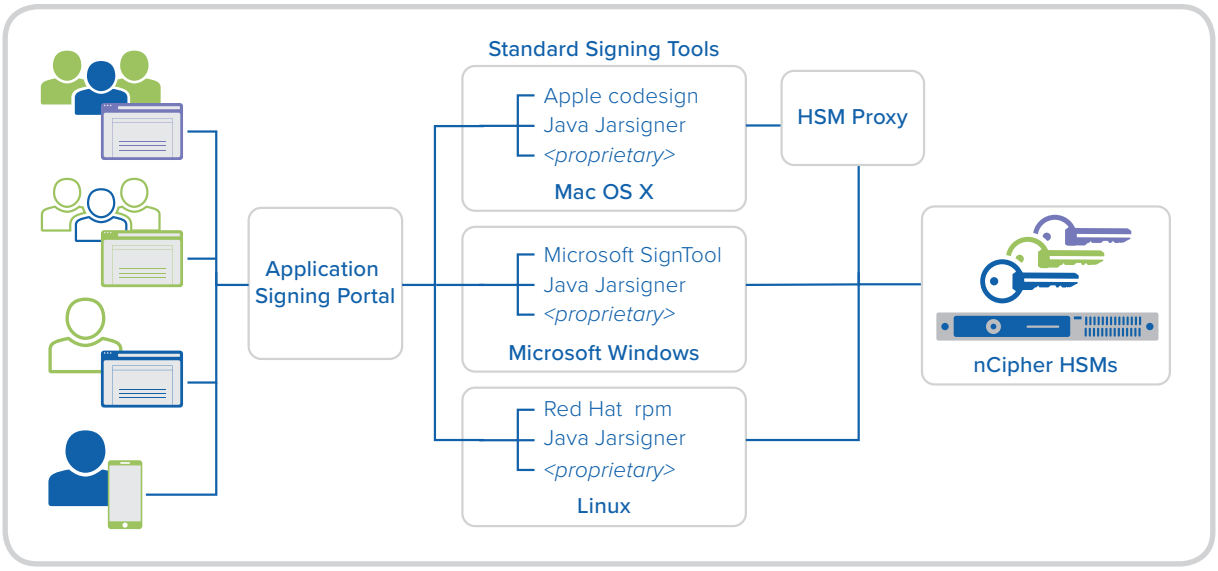

Figure 1: Code Signing Gateway Schematic