Entrust code signing solutions

High assurance security for code signing

HIGHLIGHTS

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

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

Entrust 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:

- Reduces the risk of key theft, corporate impostering, and malicious software alteration
- Enables end users to verify the source and integrity of software and detect alteration or insertion of malicious code
- Helps prevent users from abandoning installation due to operating systems' strong warning dialogs for unsigned software
- Provides access control, approval workflow, automation and auditing capabilities for code signing operations

To deliver these capabilities, Entrust offers two code signing solutions which are based on 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.

LEARN MORE AT ENTRUST.COM/HSM

Entrust code signing solutions

Code signing with Entrust 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.

Code signing solutions use the software originator's public/private key pair and a digital certificate, which includes the software originator's public key and is signed by a suitable CA, to enable the end user to verify the code. The process starts when the software originator hashes the code to be distributed, and uses their private key to sign/encrypt the hash. They then distribute the encrypted hash and the original code, along with the digital certificate, in a package to the end user. As the final step, the end user uses the software originator's public key to decrypt the encrypted, hashed code and compares the resulting hash with a regenerated hash of the received code. If the hashes are identical, the code is verified.

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

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 Entrust 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.

nShield general purpose 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; also available as-a-service nShield HSMs are available in three form factors:

- nShield Connect, an appliance serving multiple applications across a network; also available as-a-service
- 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

Entrust code signing solutions

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 Defender for checking files for viruses before signing.

The Entrust Code Signing Gateway is customized solution for each customer's unique environment by the Entrust Professional Services team.

Code signing with direct HSM integration

Direct integration with a 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 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**

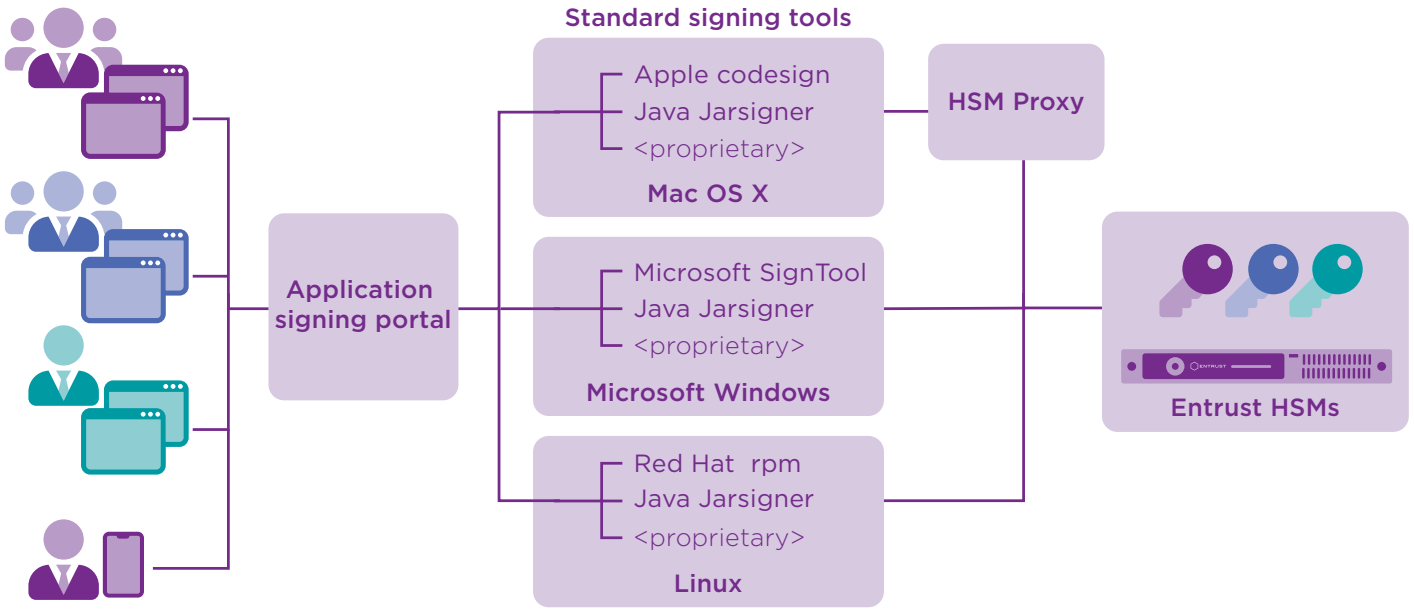

Figure 1: Code Signing Gateway schematic

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