cpl.thalesgroup.com

THALES
Building a future we can all trust

Code Signing

Code signing

Code signing employs PKI technologies such as keys, certificates, and digital signatures to ensure the identity and integrity of software. Technology companies share and distribute code through networks with inconsistent and varying security policies, potentially exposing the code to manipulation, corruption or theft.

Many software providers are now making their product available over the internet. As such, it is imperative that code published on the internet be seen as trustworthy by the user who downloads it. While many browsers provide a notice to verify the code's authenticity, no browser can determine that the code has not been tampered with prior to delivery. Therefore, a more active approach must be taken to make the Internet a reliable medium for software distribution.

Digital signatures help maintain the electronic integrity and authenticity of code by associating it with a software vendor's unique signature. In this way, distributing software on the Internet is no longer an anonymous activity as digital certificates ensure accountability, just as a manufacturer's brand name does on packaged software.

Digital certificates

A certificate is a set of data that completely identifies an entity, and is issued by a certification authority (CA). The data set includes the entity's public cryptographic key. When the sender of a message signs the message with its private key, the recipient of the message can use the sender's public key (retrieved from the certificate either sent with the message or possibly available elsewhere in the directory service) to verify the sender's identity.

Thales value

- Validated security with FIPS 140-2 Level 3 and Common Criteria certification
- Only HSM to provide true hardware key generation and storage features for disaster recovery
- Multifactor authentication for administration and management
- Superior performance: A single Thales Luna HSM is capable of up to 20,000 ECC and 10,000 RSA operations per second
- Separation of duties with multi-level access control for all access control keys
- Flexible Deployment Options: Luna HSMs can be deployed either in the cloud, on-premises, hybrid or multi-cloud environments

Customer problem

Preventing software counterfeiting has always been a challenge for publishers. Over time, security measures such as tamper-proof packaging and unique licensing keys were developed to minimize bootlegs and unauthorized copies of software distributed on disks. The Internet lacks the subtle security provided by packaging, shelf space, shrink wrap, and the like. Without an assurance of the software's integrity, and without knowing who published the software, it's difficult for end users to know how much to trust software. In addition, Windows, Java, and Apple require code to be compliant with their digital signing requirements. When code is not correlated to a known publisher a security warning message indicating "Unknown Publisher" is issued requiring the user must authorize the program to run on their machine. For this reason software publishers are facing increased pressure to sign code.

Security threat

- Loss of trust in brand
- Often disguised as legitimate software, malicious malware can be easily distributed to infect unsuspecting desktops with viruses or to install applications to facilitate fraud
- Code needs protection from viruses to provide confidence of authenticity

Hardware Security Module's role

To obtain a certificate from a CA, a software publisher must meet the criteria for commercial publishing certificate. It is recommended that applicants generate and store their private key using a dedicated hardware solution, which can be an HSM.

Thales Luna HSMs store the signing material in a hardware device, thus ensuring authenticity and integrity of a code file.

Luna HSMs

Secure sensitive data and critical applications by storing, protecting and managing cryptographic keys in Luna Network HSMs - high-assurance, tamper-resistant, FIPS 140-2 Level 3 certified network-attached appliances offering market-leading performance.

Luna Cloud HSM

Luna Cloud HSM, available from the Thales Data Protection on Demand (DPoD) Cloud HSM service, offers an as a service billing model without hardware to deploy and maintain.

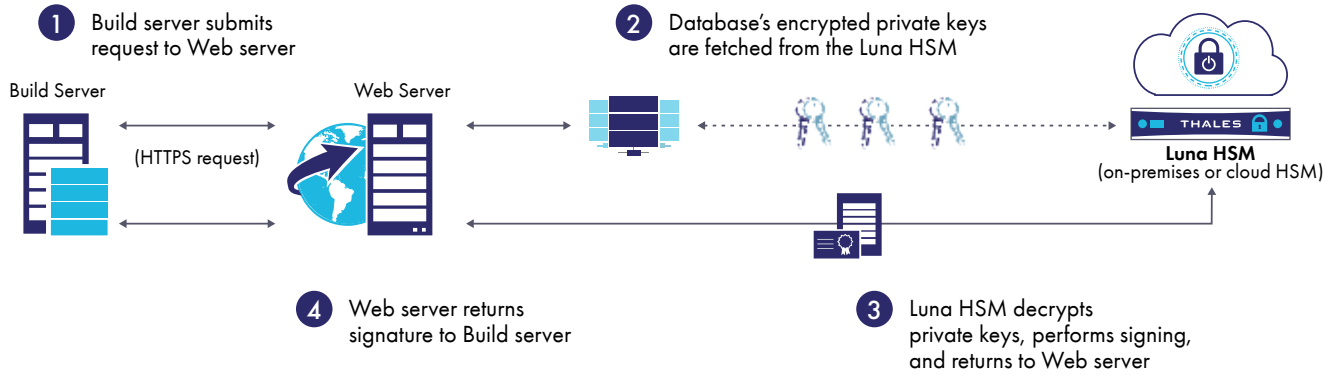
Use case

A software vendor built their business on providing affordable and user friendly software over the internet. They had a requirement that downloaded code be signed prior to running. If the code was not signed, a warning message would be issued when prospects attempted to install the vendor's software. These messages explained that the download lacked digital code signing certificates to authenticate the source of the software. As result, many prospects did not trust the authenticity of the downloaded software and sales over the internet began to slip.

In order to reassure customers that they provide trusted content, the software vendor looked for a solution to sign their code using private and public key systems. The solution was to implement an enterprise Public Key Infrastructure (PKI) featuring VeriSign as the Certificate Authority and a Luna HSM for cryptographic key storage. The Luna HSM was the right choice because it offered FIPS 140-2 Level 3 and Common Criteria certification in a tamper-proof hardware device.

With the PKI in place, prospects and customers gained the confidence that the content they were downloading was authentic and could be trusted. The software vendor was able to instill user confidence in their brand, eliminate security alerts, and increase internet sales of their software.

Code Signing



Benefits gained

Increased Revenue Protection

- Reduced risk of internal/external compromise preserves brand reputation and eliminates cost to repair infected machines of users
- Ensures signer authenticity, data integrity and non repudiation of documents/code

Increased Control and Ease of Software Management

- Simplified key management used to control distribution of the software on the Internet
- Users are able to sign only if they are part of the system which can be administered remotely
- Can be accessed from multiple build systems

Increased Security

- Separate data from keys
- Private keys and other necessary signature credentials stored in hardened appliance

Reduced Cost and Improved Compliance Auditability

- Simplified compliance – all actions auditable
- Can be used for enterprise-wide encryption – consolidate and simplify encryption across the enterprise

Extensive Partner Ecosystem

- Thales has partnered with many code signing vendors including American Megatrends Inc., Adobe, Device Authority, Keyfactor, Microsoft and Venafi, providing certificate and key lifecycle services both on-premises and in the cloud.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.