THALES

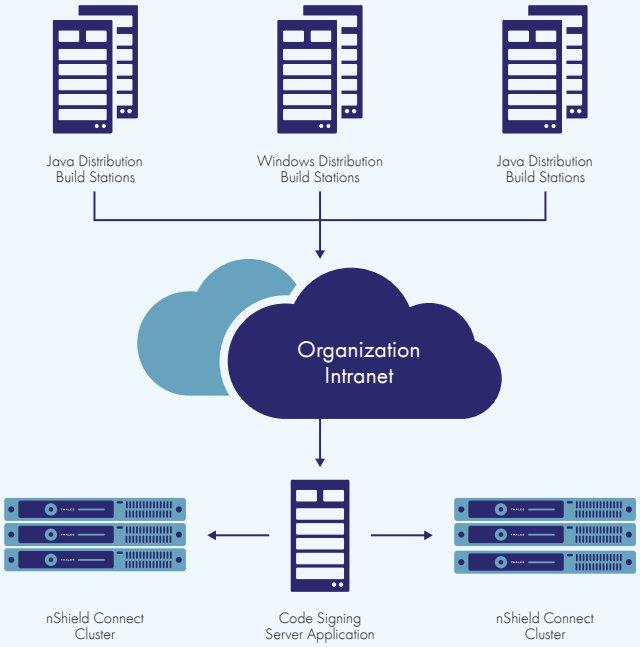
www.thalesesecurity.com

PROTECT AGAINST ADVANCED PERSISTENT THREATS WITH HIGH ASSURANCE CODE SIGNING

- Tamper-resistant security for code signing private keys protects intellectual property and brand equity
- Standard signing tools such as Sign Tool and Jarsigner simplify integration
- Security and key management best practices-based policies and procedures help minimize risk of outsider or insider threats

‹Thales eSecurity›

SECURING CODE SIGNING



Shared code signing HSMs supporting multiple software build stations.

CHALLENGES OF PROTECTING SOFTWARE

Summary

The continuing danger posed by advanced persistent threats (APTs) such as Duqu 2.0 and other sophisticated malware has reinforced the growing requirement for strong mechanisms that assure software integrity and authenticity. Digital signatures provide a proven cryptographic process for software publishers and in-house development teams to protect their systems and end users from these threats.

No matter where their end users reside, the use of digital signatures enables end users to verify publisher identities while simultaneously validating that the installation package has not been changed since it was signed. All modern operating systems look for and validate digital signatures during installation. Scary warnings about unsigned code can cause end users to abandon installation. Code signing has the attention of the developer community worldwide.

SECURING CODE SIGNING WITH THALES

IMPLEMENTING STRONG CODE SIGNING PROCESSES

Given the ongoing evolution of threats like Duqu, many software publishers face requirements to increase the security assurance level of their code signing processes as well as expand the scope of software being signed to include scripts, plug-ins, libraries and other tools. These requirements can be driven by multiple factors, but all tie back to one simple fact: if a threat actor gains control over your code signing private key your identity can be hijacked to cover the propagation of its malware.

A critical and fundamental element of increased assurance levels is strong protection of private signing keys. Just as with any PKI-based technology, if the private key falls out of the control of its owner, it can be used to create digital signatures that will be seen as "valid" and will appear to come from the organization identified in the associated digital certificate. Code signing private key compromise is one of the cornerstones of the well-known Stuxnet attack and its step-son, the Duqu 2.0 APT.

Thales can help you implement strong code signing by not only providing a high assurance method to protect private code signing keys in certified, special purpose cryptographic hardware, but also by implementing a flexible range of capabilities to simplify and automate the code signing process for organizations with more complex environments. This advanced functionality also provides configurable levels of security to implement a customer's desired assurance level around code signing operations. Thales can enable a code signing solution tailored to your specific requirements as well as extensive expertise that includes implementation of industry best practices for lifecycle management of critical code signing private keys and operational signing processes.

HIGH-ASSURANCE HARDWARE-BASED KEY PROTECTION

Today's major operating systems all present dialogs to users during the software installation process that identify the publisher of the software (using information from the code signing certificate), or highlight the lack of information about the publisher if the software is unsigned. Over time, the awareness of users of the risks of installing software from unknown or untrusted publishers has increased significantly. With the arrival of APTs which can utilize stolen private keys to create seemingly valid digital signatures, there is a new wave of awareness of the need to provide stronger protection for code signing private keys, which underpin the trustworthiness of the code signing process.

Generation, use and storage of private signing keys in software leaves those keys significantly more vulnerable to compromise than if they are protected within secure, purpose-built cryptographic hardware security modules (HSMs). Similar to how it is unwise to place keys to homes or cars in common hiding places, software-based keys are easier targets for theft, either from malicious outsiders or from disgruntled insiders. Once a private signing key is compromised, an attacker can create and broadly distribute malware posing as legitimate software using the private key and associated corporate identity.

Strong private key protection provides the secure foundation for the Thales Code Signing solution. Thales offers a wide range of FIPS-certified HSMs to protect code signing keys, from the single workstation, USB-connected nShield Edge up to the high performance, network-attached nShield Connect. And, because any cryptographic security solution requires associated management processes and audit capabilities, the development of environment-specific policies and procedures based on Thales' extensive expertise is also a core component of the Thales Code Signing solution.

Why Hardware-based Key Protection?

- Provides stronger protection than storing keys in software
- Helps prevent advanced persistent threats
- Underpins the trustworthiness of the code signing process

CODE SIGNING OPERATIONS

In addition to enhanced code signing key security, Thales works with customers to address a flexible range of automation requirements for code signing processes as well as for centralized cryptographic key management. These capabilities are particularly applicable for medium to large- sized software-producing organizations where the volume and/or distribution of software build stations warrants shared services and resources. Although there will always be configuration and customization to fit customer environments and integrate with existing software release management processes, Thales has identified three fundamental deployment scenarios:

- **Developer** – individual developer workstations with low volumes of code signing can be addressed with the nShield Edge USB-attached HSM for secure local private key management. Thales Advanced Solutions Group performs secure installation/configuration and develops basic policies and procedures for HSM and key management.
- **Workgroup** – mid-sized organizations with multiple build stations where a shared signing resource is advantageous require the nShield Connect network-attached HSM for secure code signing. In addition to secure installation/ configuration and policy and procedure development, a web service is developed to centralize and automate key management associated with software signing requests from multiple platforms and build stations for stronger security and process simplification.
- **Enterprise** – larger organizations with requirements for high volume, highly controlled software signing approval process workflows with robust end-to-end audit capabilities require a self-service web portal for signing requests in addition to centralized key management. Workflow automation capabilities simplify and streamline business processes around code signing including accepting requests, notifying approvers, managing approvals and timelines, delivering released/signed code and all associated activity logging.

LEARN MORE

Each variant of these scenarios described above sits on a foundation of one or more high assurance nShield HSMs. Thales can fine tune a tailored solution with a code signing software framework and a number of days of professional services to be determined by each customer and Thales and documented in a statement of work. Thales also offers a separate Time Stamp Server that can provide an additional means to validate precisely when code was signed via an embedded trusted time stamp. Contact a Thales representative for more information.

ABOUT THALES ADVANCED SOLUTIONS GROUP

From data encryption to key management to digital signatures, Thales Advanced Solutions Group (ASG) has deployed global security solutions across a broad variety of industries and technology environments. Thales ASG consultants are experienced in meeting the demands of the most security-conscious customers, including many of the best known names in the high technology field. Thales ASG follows a proven methodology that starts with an understanding of customer needs, and has deployed the secure Code Signing solution in response to multiple customer scenarios requiring strong security, key management and process automation.

Additional information on the Thales Code Signing solution and nShield Hardware Security Modules can be found at **www.thalesesecurity.com**

nShield Connect

nShield Edge

THALES

www.thalesesecurity.com

About Thales eSecurity

Thales eSecurity is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premises, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales eSecurity is part of Thales Group.

Follow us on:

Americas – Thales eSecurity Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 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