Encryption Consulting and Entrust deliver secure and flexible code signing solution
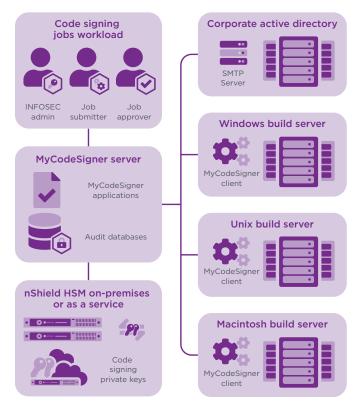
Integrated solution signs code, executables, and scripts with a hardware security module (HSM) root of trust

HIGHLIGHTS

- Validate code author and prevent possible alteration and corruption

- Establish policies and workflows to secure and streamline the process of job submissions and approvals

- Support virus and malware scans and extend to unique code formats

- Include built-in support for signing Windows, Linux, Macintosh, Docker images and Android/IOS applications

- Protect code signing keys with FIPS validated Entrust nShield® HSMs

The problem: private keys used for code signing can be vulnerable to attacks

Where you store the private keys used to sign your code is critically important. Keys stored in software can be vulnerable to attacks that can compromise your entire code signing process, your business' reputation, and the security of customers using your code. The authenticity and integrity of code you

produce depends on the signing certificate. A comprehensive log of all code signing activity is therefore necessary for security audit and compliance.

MyCodeSigner integrates with nShield HSMs, on-premises or as a service, to protect underpinning private keys used to sign code.

Encryption Consulting and Entrust deliver secure and flexible code signing solution

The challenge: verifying that the right code is signed by the right keys, while validating the signing process

Carefully managing your private signing keys to ensure they are never compromised is vital in order to prevent unauthorized code versions from reaching customers. Compromised signing keys can be used to sign code that would otherwise appear to be authentic and coming from its rightful author. As the volume of code you produce increases, verifying that your code is signed by the right keys can be challenging, especially when you need to also maintain audit logs of all signing activity.

The solution: encryption consulting MyCodeSigner and Entrust nShield HSMs

MyCodeSigner is a secure and flexible code signing solution that verifies that codes and scripts are signed by the correct certificates, and validates when the signature process occurs for precise auditing purposes. As code signing plays an increasingly important role in today's software development environments, enabling identification of legitimate software and distinguishing it from malware or rogue code is imperative. Using an open REST API, MyCodeSigner adapts to customized operational requirements and supports virus and malware scans. With built-in support for signing Windows, Linux, Macintosh, Docker and Android/iOS apps, the framework is extendable to include other unique code/document formats.

Integrating with nShield HSMs, MyCodeSigner stores private code signing keys in a tamper-resistant, FIPS 140-2 Level 3 and Common Criteria EAL4+ validated environment. The combined solution delivers the strongest security for critical keys and cryptographic processing, while recording all administrative activities in an audit log, including signing of code and associated approvals.

Why MyCodeSigner with nShield HSMs?

Private signing keys underpin the security of enterprise code signing processes. Keys handled outside the protected boundary of a certified HSM are significantly more vulnerable to attack, which can lead to compromises. HSMs are the only proven and auditable way to secure valuable cryptographic material. nShield Connect on-premises HSMs, and nShield as a Service, secure the generation and storage of the private keys used by MyCodeSigner. nShield HSMs enforce key use policies, separating security functions from administrative tasks. Doing so provides the highest level of security and assurance against key compromise and theft, while delivering scalability, flexibility, and efficiency. Together, MyCodeSigner and nShield HSMs:

- Provide secure authorship
- Ensure publication date
- Maintain software integrity
- Build trust between users

Encryption Consulting and Entrust deliver secure and flexible code signing solution

nShield HSMs enables MyCodeSigner customers to:

- Secure keys within a carefully designed cryptographic boundary using robust access control mechanisms

- Ensure keys are only used for authorized purposes

- Guarantee keys are always available using proven key management, storage, and redundancy features

- Deliver superior performance to support sensitive signing applications

Entrust HSMs

Entrust nShield HSMs are among the highest-performing, most secure and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial and government organizations.

Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

Encryption Consulting

Encryption Consulting is a dedicated consulting firm focused on providing comprehensive encryption services. Areas of expertise include public key infrastructure (PKI), HSMs, code signing, enterprise key management, transparent data encryption, element level format preserving encryption, and tokenization. For more information visit **www.encryptionconsulting.com**

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**

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