ISC's CertAgent and Entrust provide high assurance PKI

High assurance public key infrastructure (PKI)

HIGHLIGHTS

- NIAP evaluated and approved as a CSfC component
- Supported on both Windows and Linux platforms
- Easily deployed and managed
- Fits any size organization, scaling up to millions of certificates
- Uses NIST certified FIPS 140-2 Entrust nShield® HSMs

The problem: CSFC requires FIPS 140-2 level 2 hardware protection of certificate authority private keys

While the NSA's Commercial Solutions for Classified (CSfC) parameters may allow an offline trust anchor without hardware key protection, most deployments require one or more online certificate authorities in order to provide timely certificate status information.

The challenge: finding cost effective, performant, hardware protection of private keys

Many CSfC deployments are limited in scope and finding a hardware device that fits the budget, performance, and security requirements is difficult for even the most seasoned PKI teams. Budget constraints often result in the procurement of devices that are unable to perform the required tasks in a timely fashion and limit the scalability of the solution, resulting in wasted time and money.

Information Security CORPORATION

LEARN MORE AT ENTRUST.COM/HSM

ISC's CertAgent and Entrust provide high assurance PKI

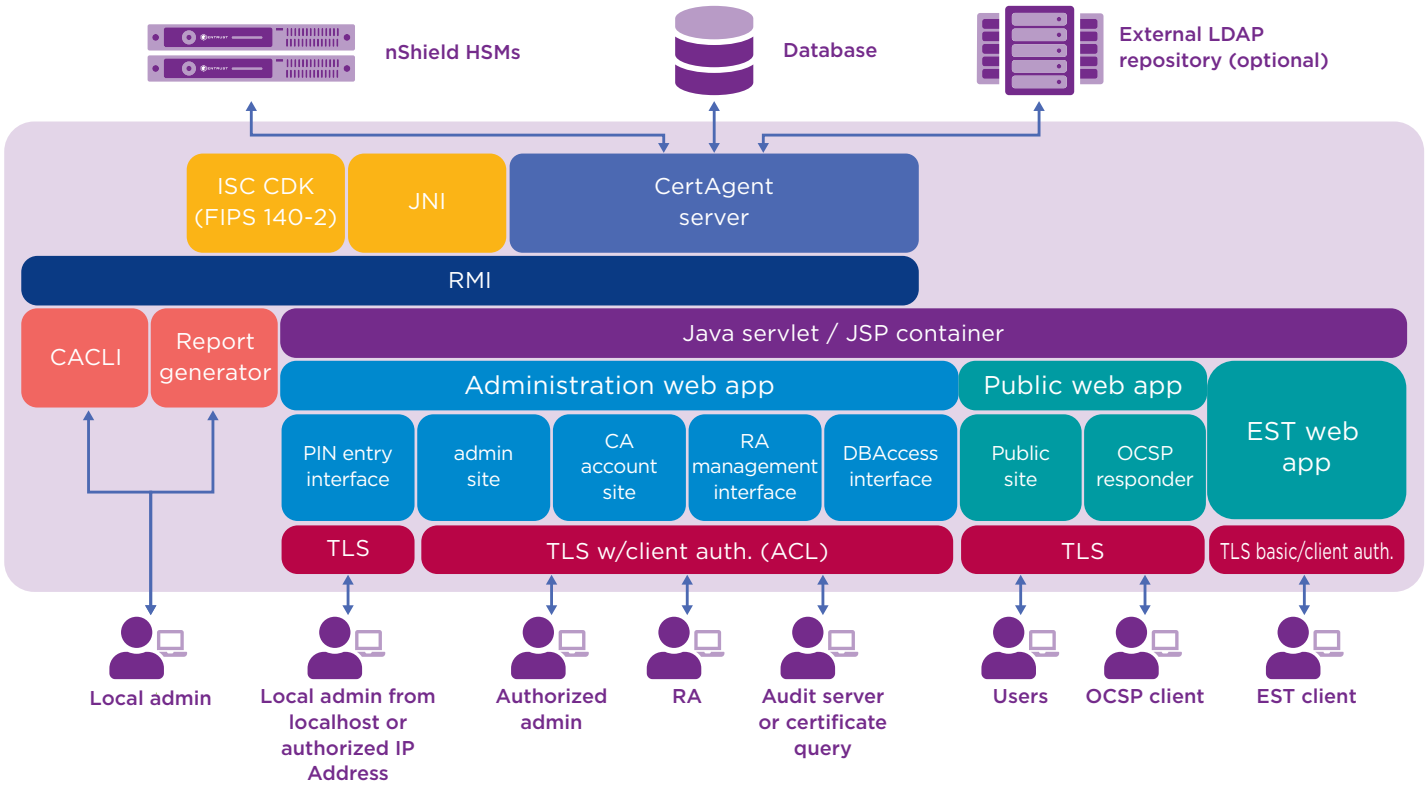
The solution: ISC CertAgent and nShield HSMS

Information Security Corporation's (ISC) CertAgent provides the core features needed to PKI-enable your organization. CertAgent has been evaluated and approved by the National Information Assurance Partnership (NIAP) as a CSfC component.

The nShield family of hardware security modules (HSMs) increases the assurance level of ISC PKI deployments and helps customers meet regulatory requirements and government mandates, including all HSM requirements defined by the CSfC Key Management Capability Package. Entrust and ISC work hand in hand with our customers to ensure that the HSM they choose fits their budget, security, and performance requirements.

Why use nShield HSMs with CertAgent?

Entrust HSMs are a cost effective, highly secure, and performant solution for meeting CSfC requirements. Encryption and authentication keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attack, which can lead to compromise of critical keys. HSMs are the only proven and auditable way to secure valuable cryptographic material. Entrust nShield HSMs integrate with CertAgent to provide comprehensive logical and physical protection of keys. The combination delivers an auditable method for enforcing security policies.



nShield HSMs increases the assurance level of ISC PKI, helping customers meet regulatory requirements

LEARN MORE AT ENTRUST.COM/HSM

ISC's CertAgent and Entrust provide high assurance PKI

nShield Connect HSMs enable ISC's customers to:

- Secure keys within carefully designed cryptographic boundaries that use robust access control mechanisms, so keys are only used for their authorized purpose
- Ensure key availability by using sophisticated management, storage, and redundancy features to guarantee they are always accessible when needed by CertAgent
- Deliver superior performance to support demanding PKI applications

nShield Connect HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. With Entrust HSMs you can:

- Provide a tightly controlled tamper resistant environment for safekeeping and managing encryption keys
- Enforce key use policies, separating security functions from administrative tasks
- Interface with applications using industry-standard APIs (PKCS#11, OpenSSL, JCE, CAPI, and CNG)

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.

Information Security Corporation

Founded in 1989, ISC specializes in the design and development of cybersecurity solutions for government and military applications. With a special focus on high assurance deployments, the company's expertise include:

- PKI credential management
- Automated provisioning of relying applications
- Post-quantum PKI
- Encryption
- Authentication

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** For more information visit **www.infoseccorp.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

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223