THALES

www.thales-esecurity.com

ENTRUST AND THALES SOLUTION ENHANCES SECURITY, DELIVERS HIGH PERFORMANCE AND FACILITATES REGULATORY COMPLIANCE

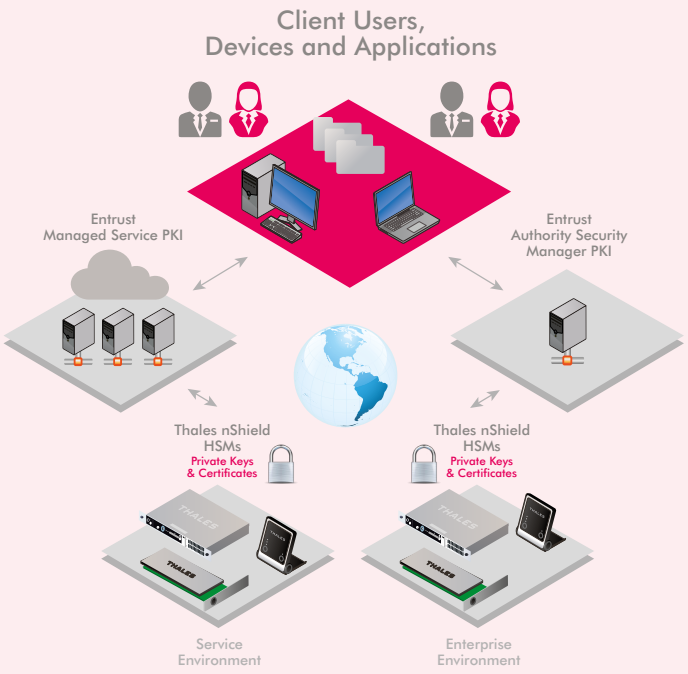
Solution Benefits

- Establish identity-based security across the enterprise, including mobile applications
- Issue PKI certificates to control access to enterprise resources – with on-premise or hosted deployment options
- Manage the lifecycle of certificate-based identities, including backup and recovery
- Provide high assurance security to safeguard sensitive private keys
- Deliver FIPS 140-2 Level 3 and Common Criteria EAL4+ certified tamper resistance

Entrust®
Securing Digital Identities & Information

Thales e-Security

Entrust-Thales Solution for Enhanced Secure Enterprise and Managed Services PKI

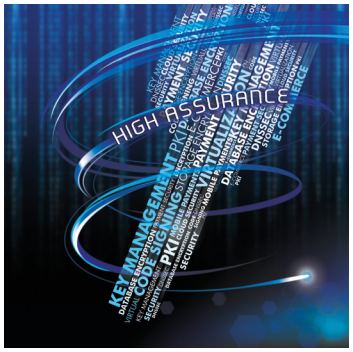


The Problem: Critical Business Applications are Increasingly Dependent on PKI Services

Public key infrastructures (PKIs) establish the identity of users, devices and applications for secure access to critical enterprise systems and resources - delivering essential elements of a secure environment. With increasing dependency on online transactions and authentication methods in today's environment, and the emergence of new requirements for PKIs such as supporting issuance of device certificates for BYOD (Bring Your Own Device) programs, applications rely on PKIs to deliver appropriate levels of assurance. Strong protection for private keys, used by in-house or hosted PKIs, is an essential element of an effective security strategy.

The Challenge: Secure Management of Certification Authority (CA) Keys

The trustworthiness of a PKI depends on the protection afforded to the private keys in the CA hierarchy and associated verification processes. CA keys stored in software are more vulnerable to compromise than those protected in dedicated hardware. High assurance key protection and management solutions enhance security and reduce risk for a trusted business ecosystem.



Entrust-Thales Solution for Enhanced Secure Enterprise and Managed Services PKI

The Solution: Entrust and Thales Deliver Performance and High Assurance

Entrust Authority Security Manager and Entrust Managed Services PKI establish and manage certificate-based security for critical business applications. Entrust Authority Security Manager enables customers to deploy and manage their own digital certificates. The product authenticates users, controls access and secures cryptographic applications. For customers seeking a hands-off approach, Entrust Managed Services PKI delivers a hosted solution.

Thales Entrust Ready nShield™ hardware security modules (HSMs) integrate out-of-the-box for efficient deployment with Entrust PKI offerings. The combined solution protects the confidentiality and integrity of sensitive key material. Organizations looking to extend the security of in-house or hosted PKIs can deploy Entrust solutions with nShield HSMs to achieve high assurance and operational efficiency. nShield HSMs ensure that cryptographic operations occur within a protected environment and critical keys are never exposed to unauthorized entities.

Why Use HSMs for PKI Deployments?

While it is possible to deploy PKIs without HSMs, CA keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attacks which could compromise the PKI's credential issuance and certificate revocation capabilities. HSMs are widely considered to be a best practice for PKI deployments, and are the only proven and auditable way to secure valuable cryptographic material. HSMs enable organizations to:

- **Secure CA keys** within carefully designed cryptographic boundaries that employ robust access control mechanisms with enforced separation of duties to ensure keys are only used by authorized entities
- **Ensure availability** by using sophisticated key management, storage and redundancy features to guarantee keys are always accessible when needed
- **Deliver high performance** to support increasingly demanding transaction rates

nShield HSMs securely generate, store and manage CA private keys. The Entrust Ready certification of nShield HSMs assures interoperability, ease of deployment and enhanced security.

Thales

Thales nShield HSMs are high-performance cryptographic devices designed to generate, safeguard and manage sensitive key material. Certified to stringent security standards, nShield HSMs:

- Store keys in a secure, tamper-resistant environment
- Comply with regulatory requirements for public sector, financial services and enterprises
- Enforce security policies, separating security functions from administrative tasks
- Support high-performance elliptic curve cryptography (ECC)

Thales nShield HSMs are available to match specific performance and budgetary needs:

- **nShield Edge:** Portable USB-attached HSM for low-volume offline root CA configurations
- **nShield Solo:** Embedded PCI or PCIe HSM for SSL web servers and security appliances
- **nShield Connect:** High-performance, network-attached HSM for high availability environments

Entrust

Entrust Authority Security Manager and Entrust Managed Services PKI issue and manage digital identities. Entrust solutions:

- Store and manage private keys securely in dual-rooted CAs
- Manage PKI certificate lifecycle automatically across enterprise
- Publish certificate revocation lists (CRLs) for certificate validation
- Maintain auditable database of private key histories

Whether using the in-house PKI or the managed service, Entrust solutions allow organizations to establish and maintain a trustworthy environment by providing certificates that secure off-the-shelf applications using encryption, digital signatures and strong certificate authentication.

For more detailed technical specifications, please visit www.thales-esecurity.com or www.entrust.com

Entrust® Ready

Follow us on:

Americas – Thales e-Security 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 – Unit 4101 41/F 248, Queen's Road East, Wanchai, Hong Kong, PRC • 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