ENTRUST TECHNOLOGY ALLIANCE PROGRAM

THALES

An Integrated Solution to Enhance the Security of Your U.S. Federal Government Security Infrastructure

THE CHALLENGE:

Security and Management of Certification Authority (CA) Keys

The new age of connectivity drives powerful growth opportunities in the modern enterprise, but it also requires you to change the way you protect information, networks and devices. Public key infrastructure (PKI) solutions establish trusted identities for users, devices, applications and services, as well as ensure secure access to critical enterprise systems and resources, delivering critical elements of a secure environment.

Strong protection for the private keys used by on-premises or hosted PKIs is essential to an effective security strategy. The level of trust in a PKI deployment depends on the level of protection provided to the private keys at the core of this trust infrastructure. CA keys stored and managed in software can be at risk of compromise via advanced threats, impacting the trustworthiness of the environment. The challenge is how to reduce this risk.

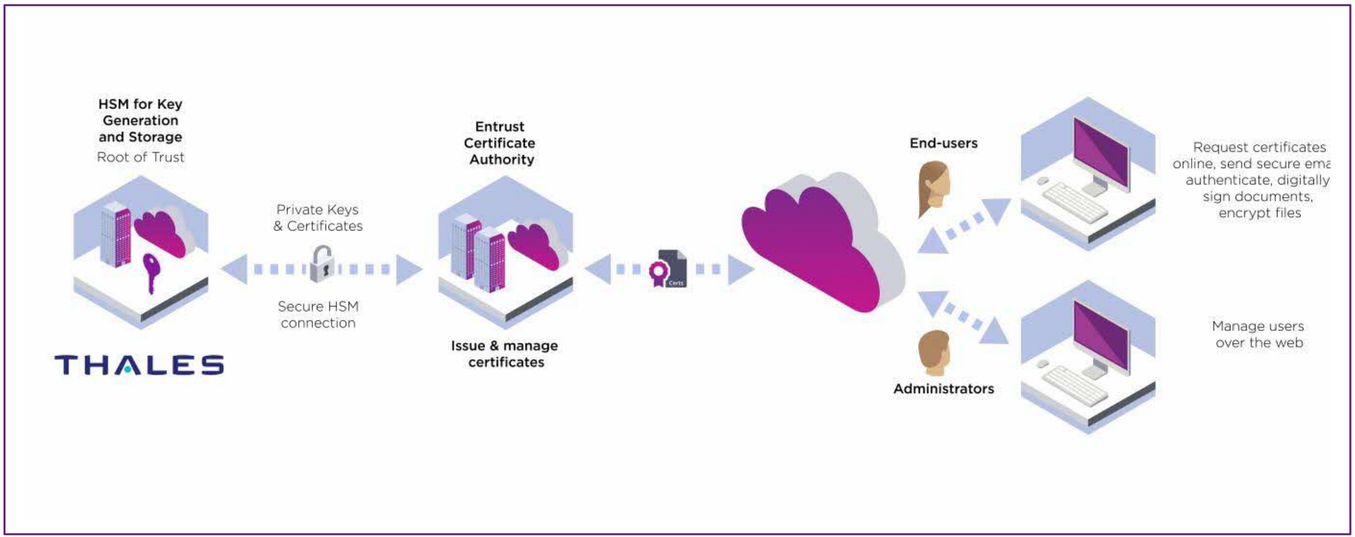
THE SOLUTION:

An integrated solution with a strong root of trust

Entrust and Thales Trusted Cyber Technologies (Thales TCT) have teamed up to offer a high performing solution for the U.S. Federal Government that integrates the best of both companies' security technologies to ensure trusted identity, signing and encryption, while knowing your privates keys are safe and secure.

Key Benefits

- Provide trusted identities for people, systems, and things
- Provide root of trust to safeguard sensitive private keys
- Balance your usability needs with regulatory constraints, all while maintaining best-in-class PKI policies and practices
- Maintain operational continuity with high-availability PKI
- Satifsfy modern use case demands with horizontal scaling


HSM for Key Generation and Storage
Root of Trust
THALES
Private Keys & Certificates
Secure HSM connection
Entrust Certificate Authority
Issue & manage certificates
Certs
End-users
Administrators
Request certificates online, send secure ema authenticate, digitally sign documents, encrypt files
Manage users over the web

HOW IT WORKS

Entrust's PKI portfolio of solutions can provide a complete trust environment to accommodate and scale to any business needs. As companies increase their digital sophistication and expand their use cases, they rely on certificates to establish a higher level of trust, and secure people, systems, and devices. Entrust Certificate Authority allows organizations to easily manage the digital keys and certificates that secure these identities. For customers seeking a hands-off approach, Entrust Managed PKI (mPKI) delivers a hosted solution.

Thales TCT's T-Series HSMs integrate with Entrust PKI to protect the confidentiality and integrity of sensitive keys. Organizations of the U.S. Federal Government looking to extend the security of on-premises or hosted PKIs can deploy Entrust solutions in conjunction with Thales TCT T-Series HSMs to ensure that critical keys are never exposed to unauthorized entities. Thales TCT HSMs securely generate, store and manage CA private keys within the confines of a FIPS 140-2 Level 3 hardware device, designed specificially for the government.

WHY USE THALES TCT LUNA NETWORK HSM

Luna T-Series HSMs are the choice for government agencies when storing, protecting and managing cryptographic keys used to secure sensitive data and critical applications. Meeting government mandates for U.S. Supply Chain, the high-assurance, tamper-resistant Luna T-Series HSMs are designed, developed, manufactured, sold, and supported in the United States.

Luna T-Series HSMs offer industry-leading cryptographic performance and security optimized for government mandated algorithms and key lengths. Thales TCT's keys-in-hardware approach protects the entire life-cycle of keys within the FIPS 140-2 Level 3 validated confines of the HSM. In addition, the T-Series Luna HSM is approved by CNSS for use in National Security Systems PKI.

With the addition of an embedded quantum random number generator (QRNG) chip in the Luna T7 Crypto Module, Thales TCT is offering the industry's first FIPS 140-2 compliant HSM capable of generating quantum enhanced keys. Using principles of quantum physics, the QRNG chip produces high quality entropy which is the basis for all random numbers and cryptographic keys generated by the HSM. Customers can dynamically change between classical key generation and quantum enhanced keys as threats emerge over time

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. For more information, visit www.thalestct.com

thalestct.com

THALES

About Entrust

Consumers, citizens, and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services, or logging onto corporate networks. Entrust offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports, and ID cards to the digital realm of authentication, certificates, and secure communications. With more than 2,500 Entrust colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

entrust.com

Learn more at
entrust.com

ENTRUST
TECHNOLOGY ALLIANCE
PROGRAM

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com entrust.com/contact