An Integrated Solution to Enhance the Security of Your 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.

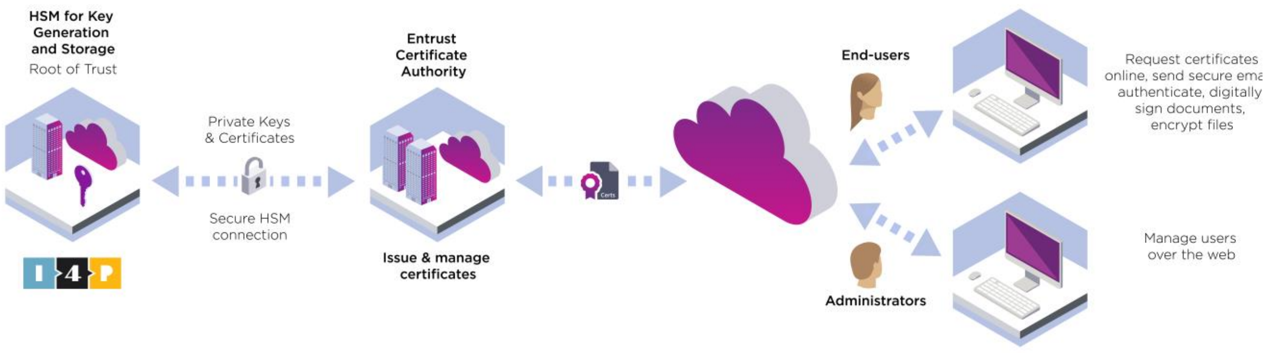
THE SOLUTION:

An integrated and highly secure solution with a strong root of trust

Entrust and i4p have teamed up to offer a high performing solution 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 business continuity with high-availability PKI
- Satifsfy modern use case demands with horizontal scaling


HSM for Key Generation and Storage
Root of Trust
I4P
Private Keys & Certificates
Secure HSM connection
Entrust Certificate Authority
Issue & manage certificates
Certs
End-users
Request certificates online, send secure ema authenticate, digitally sign documents, encrypt files
Administrators
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.

i4p's Trident HSM integrates with Entrust PKI to protect the confidentiality and integrity of sensitive keys. Organizations looking to extend the security of on-premises or hosted PKIs can deploy Entrust solutions in conjunction with i4p's Trident HSM to ensure that critical keys are never exposed to unauthorized entities. i4p HSMs securely generate, store and manage CA private.

i4p's revolutionary products offer exceptional services and a high level of protection. The company provides ideal and flexible solutions for data protection challenges in several industries including banking and financial services, government and manufacturing as well as data safe-keepers.

WHY USE TRIDENT HSMs

Trident HSM has successfully attained Common Criteria EAL4+ certification level under the Protection Profile for Cryptographic Module for Trust Services (EN 419221-5) with strict conformance.

Every Trident HSM comes equipped with an integrated Tamper Detection Module (TDM) with multiple sensors that constantly monitor the environment even when the device is not powered. Also, the Trident HSM allows for unlimited local client applications (LCAs) to be installed into its protected environment.

Trident is the first hardware security module that can combine a high level of hardware security with the benefits of secure multi-party cryptography (SMPC) to meet the highest level of data protection requirements in the business world.

In SMPC mode it can generate, sign and encrypt RSA key pairs in a revolutionary distributed manner. When configured in this mode, the secret key will never exist as a whole, on any device, neither at the moment of generation, storage or computing. The key material cannot be identified independently on any of the devices, so even if one or even two of them is compromised in any way, the information obtained is worthless to the attacker.

About i4p

i4p is a Hungarian company that develops highly secure hardware and software solutions, as well as related services capable of disrupting the IT security market. i4p informatics was founded by the former owners of a Hungarian QTSP. After a successful exit, the decision was made to utilize their expertise and to found I4p, in order to create the best, most secure, and user-friendly cryptographic solutions. The result is the family of Trident products: HSM, RSS, TSS and SFS. The company's mission is to provide a technological background to the ever-changing regulations on data security and data protection and to develop and launch distributed cryptographic processes and distributed platforms based on them.

i4p.com

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