



## Enhance the Security of Certification Authority with Securosys Primus HSM

### 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.

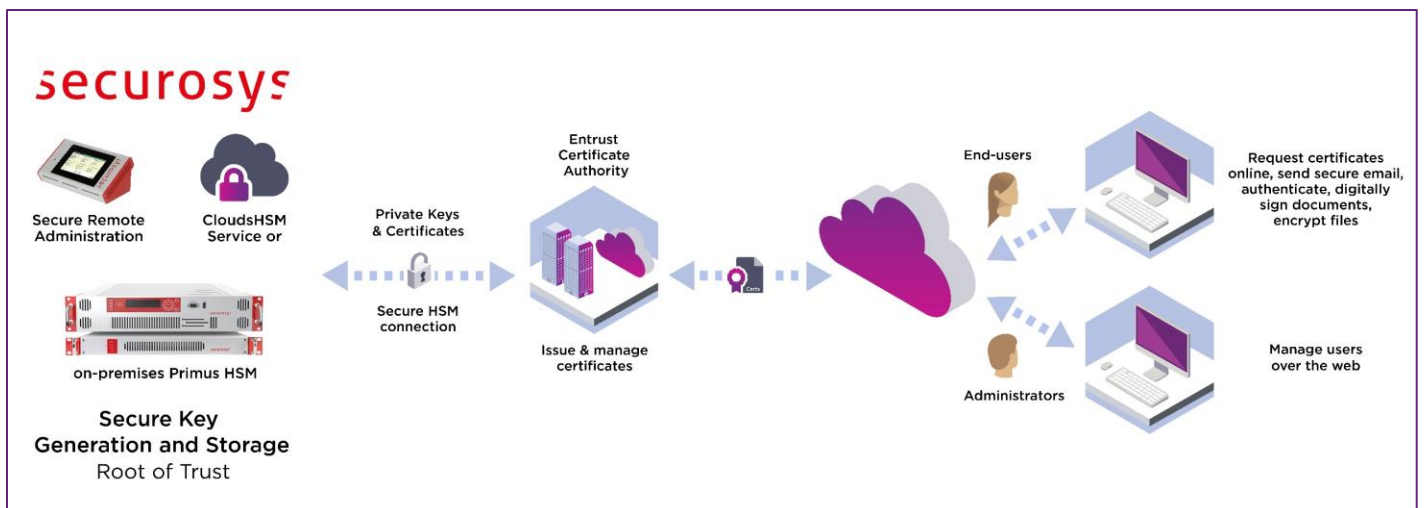
### THE SOLUTION:

An integrated solution with a strong root of trust.

Entrust and Securosys 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 private 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 business needs with regulatory constraints, high-availability PKI, while maintaining best-in-class PKI policies and practices
- Simplify and automate PKI key ceremony and audits based on key attestation
- CloudsHSM or on-premises



## HOW IT WORKS

Entrust's PKI solutions 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.

Securosys Primus HSMs or CloudsHSM integrate fully 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 on-premises Securosys Primus HSMs, or the ready-to-go CloudsHSM service. Securosys HSMs securely generate, store and manage CA private keys, ensure that critical keys are never exposed to unauthorized entities, and are required in case of strong compliance regulations.

## WHY USE Securosys HSM

### Solution value statement

Securosys provides affordable network Hardware Security Modules, up to highest requirements in performance, availability and safety. Start your integration today using the CloudsHSM service, not having to care about setup or operation, and the possibility of later migration to on-site infrastructure. Benefit from fast regional access, load-balancing, and automatic redundancy failover, thanks to built-in large geo-redundant HA cluster mechanisms. Multi-tenancy and large built-in storage allow separation of different instances, and usage for future applications. Minimize risk of exposure and operational failures by taking Root CA partitions off-line, and additional Security Officer intervention for key deletion.

Ease CA key ceremonies and automate audit procedures using Securosys Key Attestation and Audit features, proofing all keys and relevant parameters with a chain of trust originating from our Securosys root certificate.

All HSMs are developed and manufactured in Switzerland using a trusted supply chain and are certified according to FIPS140-2 level 3 and CC EAL4+ (EN419221-5) to fulfill strongest compliance regulations.

Decanus allows for easy and cost-efficient remote management of HSM clusters and CloudsHSM partitions (2-of-n, 2FA) without compromising security (configuration, backup procedures, audit data, offline partition, etc.).

### About Securosys

Securosys SA, based in Zurich, Switzerland, is a market leader in cyber security, encryption, and in securing digital identities. Founded in 2014, Securosys secures the Swiss financial markets on behalf of the Swiss National Bank and supplies more than half of the Tier 1 banks worldwide with hardware security modules developed and built in Switzerland. Securosys offers a wide range of security network appliances focused on commercial applications and operates CloudsHSM (HSMaaS) internationally. All products are developed and manufactured in Switzerland, free from contaminating influences.

[www.securosys.com](http://www.securosys.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](http://entrust.com)

# securosys



Learn more at  
[entrust.com](http://entrust.com)

