

Primus HSM - The Hardware Security Module

Securing SwissPKI™ using Securosys Clouds HSM or on-premise Primus HSM

SwissPKI™

SwissPKI™ from libC Technologies is a feature-rich fully **integrated Public Key Infrastructure**, which helps to expand your enterprise security from large scale deployments to embedded HSM solutions. The solution provides **all necessary out-of-the box components** to increase your digital security in a safe, simple and quick way, to protect your business processes.

The solution addresses large scale cryptographic key management life-cycle, online hardware-to-hardware key distribution, **tamper proof audit** as well as usage logs for compliance with standards and covers the complete certificate and key management life-cycle.

SwissPKI™ integrates with the Securosys Clouds HSM Service or on-premises Primus HSMs, taking full advantage of the built-in backup and replication mechanisms. Advanced Primus HSM features include securing all keys including **PKI meta data objects** directly in hardware **on the HSM**.

SwissPKI™ reduces your operational overhead, reduces costs and increases security: no more licensing, maintenance and support of dedicated systems such as database servers, application and archive servers, monitoring and controls systems.

SwissPKI™ Features

- Multitenant, Communities containing multiple Root CA, Sub CA and Cross Signing
- Certificate and CRL/ARL publisher to multiple destinations
- Certificate Policy Editor, predefined PKI policies
- Time Stamp Authority (TSA)
- Online Certificate Status Protocol (OCSP)
- External Public Trusted Certification Authorities
- Document Signer Service (DSS)
- Protect traffic to internal web-sites with SSL/TLS
- Microsoft Certificate Enrollment
- Certificate Management Life-Cycle Workflow
- Apache SSL certificate provisioning
- External Public Trusted Certification Authorities

SwissPKI™ helps you keep your certificates up-to-date and maintain complete visibility over them across issuing authorities. You can assign roles such as registration officer, authorizer or auditor to trusted persons who can manage issuance, renewal or recovery to streamline your organization's work flows to control each certificate management phase. In addition to the certificate policy management available out-of-the-box, you can provide your own micro-services on a policy basis to control misconfiguration, missing fields and/or use internal trusted data sources to validate certificate content.

The Securosys Clouds HSM service (HSM as a Service) facilitates a fast and smooth implementation, with georedundancy and highest availability.

Benefits

Reduce Operational Cost

- Complete Integration in one system, all PKI components out-of-the-box
- Easy, compliant operation
- PKI meta data on the HSM
- Full license, maintenance and supportAs a service (or on-premise)

Increased Security

- Highest availability
- Tamper proof audit
- Compliance with standards
- Keys are never exposed outside of the HSMs
- High entropy hardware true random number generators
- Designed, developed and manufactured in Switzerland
- Hosted in Switzerland and certified to the standards ISO 9001, 14001, 20000, 27001, 27018

PKI Communities

Demo IT SA

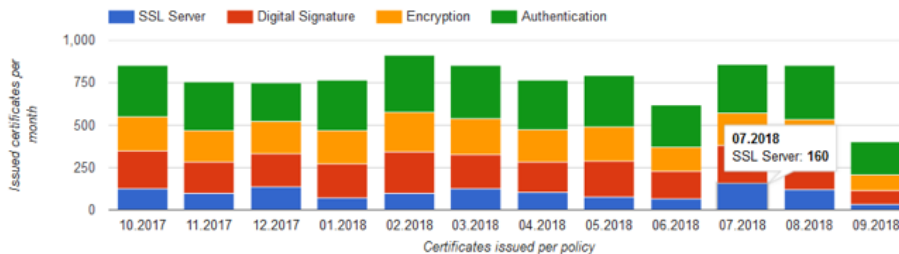
Action



Number of certificates expiring in 30 days

Number of certificates expiring in 60 days

Certificates issued per month and policy



SwissPKI™ Packaging



Cloud PKI Service

Full featured Swiss Managed Public Key Infrastructure as a Service, secured by Securosys Clouds HSM. Ready to use and managed by libC Technologies experts.



aws marketplace

AWS Marketplace

Full featured Public Key Infrastructure, secured by Securosys Clouds HSMs for AWS cloud computing customers. Ready to use. Available in Q4 2018.

Synology

Synology

Public Key Infrastructure for Synology including predefined, ready to use certificate policy templates. Available in Q1 2019.



On Premises

Full featured Public Key Infrastructure on premises secured by Securosys Clouds HSM or dedicated Securosys Primus HSMs. Container ready.

HEADQUARTERS
Securosys SA
Förrlibuckstrasse 70
8005 Zürich
Schweiz
+41 44 552 31 00
info@securosys.ch
www.securosys.ch

Service and Maintenance

By choosing the SwissPKI™ solution, you choose peace and security. LibC Technologies guarantees the availability of their IT engineers and the quality of the platform hosting. Thanks to hosting in a dedicated, experienced data center based in Zurich, Switzerland, your data is secure and confidential.

GERMANY & EU
Securosys
Deutschland GmbH
Darrestrasse 9
87600 Kaufbeuren
Deutschland
+49 8341 438620
info@securosys.de
www.securosys.de

Securosys Clouds HSM - Boosting SwissPKI™ Security

The Swiss Hardware Security Module as a Service. The Clouds HSM service is located and operated in Switzerland. It was built by the experts who designed and manufacture the HSM for the Swiss Interbank Clearing system.

When taking security seriously and complying to regulation standards - such as GDPR - digital keys need to be generated and safeguarded on an HSM. With Clouds HSM, these requirements are fulfilled without time-consuming implementations and operations. Your HSM partition is protected like a bank deposit safe and redundantly secured by five devices: two HSM are based in two geographically separated data centers in Switzerland, backups are held in HSMs in a former bunker of the Swiss Air Force in the Swiss Alps. Every location features double internet access.

Benefits

- HSM as a service, ready to use
- Simple, flexible and scalable
- Highest availability
- Best price-performance ratio
- Simple integration with a wide range of applications
- Fully compliant to security standards
- Secure legal environment
- Easy migration to on-premise