securosys

Available globally. Managed in Switzerland.

Securosys CloudHSM: Your Online Key Vault

Securosys CloudHSM is the best solution for you if you need

- maximum security for your data and keys
- HSMs run by experts
- HSM as a service – simple, flexible, scalable, always up to date & ready to use
- devices from a trusted provider
- global & highest availability

The Swiss Hardware Security Module as a Service

The Securosys CloudHSM is operated in Switzerland, Germany, Singapore and the US. It is available with dedicated HSMs or as shared service in multi-tenancy HSMs. CloudHSM was built and is operated by the experts who designed and manufacture the HSM for the Swiss Interbank Clearing system.

Compliant Application

When taking security seriously and complying with regulatory standards, digital keys need to be generated and safeguarded in an HSM. With CloudHSM, these requirements are fulfilled without time-consuming implementations and operations by just using the service via standard APIs.

HSM Availability according to Swiss Banking Standards

Your HSM partition is protected like a bank deposit safe and redundantly secured by two HSMs that are based in geographically separated data centers in Switzerland. Additionally, the data is synchronized to an HSM in a former bunker in the Swiss Alps for business continuity purposes. Every location features redundant internet access. For pre-production and test environments we provide a Sandbox service with double redundancy.

Service Packages

	Multi-tenancy HSM Subscription			Dedicated HSM Subscription[1]	
	ECO (Economy SME)	ECO CC (CC certified, ZertES, eIDAS)	SBX (Sandbox for Pre-production & Testing)	Platinum (Basic)	PLATINUM (Enterprise)
Platform[2]	2x1 +1 3 HSMs in 3 data centers	2x1 +1 3 HSMs in 3 data centers	2x1 2 HSMs in 2 data centers (in debug mode)	Dedicated HSMs hosted in data centers	Dedicated HSMs hosted in data centers
Administration	Operated and managed by Securosys specialists (ISO 27001 compliant)				
Performance[3]	Up to **600** Sig./Min	Up to **600** Sig./Min	Not guaranteed	up to **1`200** Sig./Min	Up to **12`000** Sig./Min
Capacity	**10 MB**[5]	**10 MB**[5]	**10 MB**[5]	**120 MB**[1]	**240 MB**[1]
Support[4] Availability Response time critcal/major/minor	24 x 7 x 365 2/8/24h	24 x 7 x 365 2/8/24h	24 x 7 x 365 8/12/24h	24 x 7 x 365 1/4/8h	24 x 7 x 365 1/4/8h

[1] More options available: additional partitions, performance, customer owned HSM operation
[2] Synchronized Partitions in Active Datacenters + Backup Datacenter

[3] Performance measured in #RSA4096/ECC512 signatures per minute
[4] Security Officer intervention available during Securosys office hours CET 09:00 – 17:00
[5] Additional storage can be bought at 100MB increments

Benefits & Features

- *Ready to use:* No hardware evaluation or setup required. Operational within hours.
- *No time and effort:* Our experts maintain the devices and keep the system and security up to date. Your employees are not in need of any additional training sessions, nor do they have to install or maintain anything. Thus, there is more time left for your core business.
- *Complete data isolation:* Your data is kept in a Primus Hardware Security Module. Access by other CloudHSM users is impossible. Using Partition Administration on Decanus- Securosys Remote Control Terminal you can even lock out the HSM operations team from any management tasks on your partition. Privacy and data protection are always guaranteed.
- *Global availability & business continuity:* The HSMs are located in four active data centers. Every location features double internet access, thus guaranteeing no downtime. Due to the globally synchronized system, CloudHSM provides the lowest latency acess to private keys from anywhere in the world. Additionally, your data is kept safe from environmental dangers in an EMP/HMP protected bunker (BSI zone 3 / NATO zone 2).
- *Simple integration:* The service fits seamlessly into existing systems.

- *Fully compliant to security standards:* The Primus HSMs are FIPS 140-2 Level 3 certified and Common Criteria certified according to EN 419 221-5 for eIDAS or ZertES applications. Service operation and data centers complying to ISO 27001.
- *Security policy à la carte:* You don't have to craft a security policy from scratch, because the service is set up based on best practices. You may adjust the policy according to your needs.
- *Best price-performance ratio:* With our service, no capital lock-up is required. Operation will fully be outsourced. Total cost of ownership is drastically reduced.
- *Wide range of applications:* CloudHSM supports a variety of cryptographic algorithms including PQC to address the requirments of applications like PKI, SSL, TDE, signing, crypto assets, etc. Secure connection between your application and the CloudHSM is established using standard API provider software (PKCS#11, openSSL, JCE/JCA, MS CNG and RestAPI).
- *Easy withdrawal from the cloud:* In case you decide to leave our service to insource your HSM, you may do so by activating simply your on-premise HSM.

HEADQUARTER
Securosys SA
Max-Högger-Strasse 2
8048 Zürich
SCHWEIZ
+41 44 552 31 00
info@securosys.com
www.securosys.com

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

APAC
Securosys
Hong Kong Ltd.
Unit 704B Sunbeam Centre
27 Shing Yip Street
Kwun Tong
Hong Kong
+852 8193 1646
info-apac@securosys.com
www.securosys.com

USA
Securosys
3957 Royal Troon Hills
El Dorado Hills
California
+1 (279) 321 9421
info@securosys.com
www.securosys.com