



securosys

Secure Enterprise-Grade Key Management

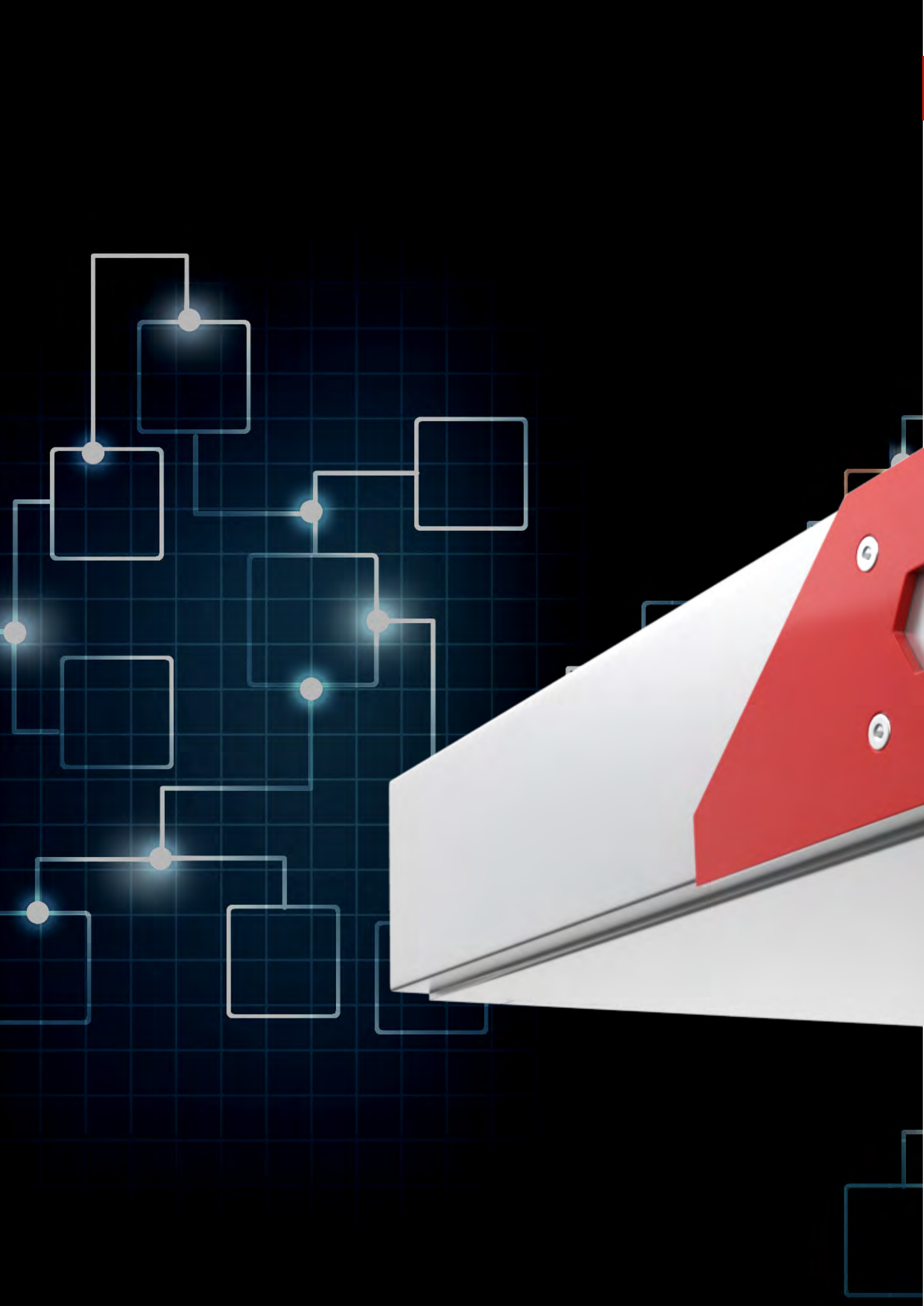
for Crypto Assets and
Blockchain Systems

**/ BLOCKCHAIN AND
CRYPTO-ASSETS HSM**




Securosys SA
Förllibuckstrasse 70
8005 Zurich, Switzerland

Email info@securosys.ch
Phone +41 (0)44 552 31 00
www.securosys.com



SECURING BLOCKCHAIN AND CRYPTO ASSETS



Crypto currencies are currently experiencing a boom. Thanks to the blockchain technology used, they offer the advantage that transactions can be viewed by anyone who belongs to the corresponding distributed system. At the same time, however, transaction partners remain anonymous. Moreover, the blockchain cannot be manipulated unnoticed due to its inherent structure. Unfortunately, news often report that crypto assets worth millions of dollars have been lost or stolen. However, this is not because of the blockchain itself, and it is avoidable: First, providers of crypto trading platforms must offer secure storage of crypto keys, and second, crypto merchants should ensure to select only such secured platforms for their transactions with crypto currencies. Securosys offers a solution at hand and furthermore is in the process of developing additional functionality according to market requirements.

AN UNSAFE LINK IN CRYPTO ASSETS: THE WALLET

The most insecure link in the digital-currency system is the wallet, which is located on the application level. A crypto-currency owner uses this application to manage his crypto assets. It contains the private key corresponding to the special crypto object. For the wallet to be secure, the keys must be stored in a secure location.



Cold Storage

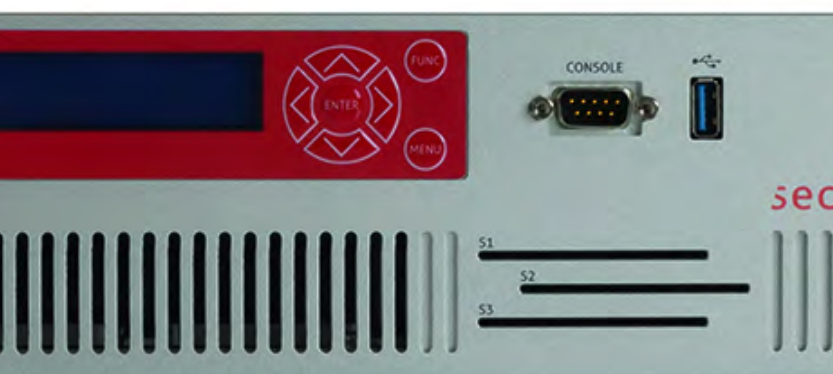
Storing the private key on a PC is completely unsafe, as there are already countless methods for infiltrating PCs. Many crypto-asset owners therefore prefer "cold storage": a storage method in which the carrier of the crypto key is not directly connected to the Internet. A piece of paper or a USB stick are the two most common forms of cold storage. It is obvious that these methods are unsafe and do not scale well: Paper and USB sticks can easily be lost or stolen. Moreover, when printing on paper, the printer also keeps a copy of the document in its memory; another location that can be hacked.

The solution is that the wallet provider maintains a dedicated crypto keystore based on a **Hardware Security Module (HSM)** for his customers. Large crypto investors should either possess their own HSM crypto key storage or use an **HSM service** to secure their crypto assets.



Multi-signature

At Securosys, we focus on securing crypto assets and developing new solutions to meet market needs. For this purpose, we closely work together with trustworthy and innovative partners. One of our functional extensions solves the problems concerning digital signatures: It can be ensured that not just a single authorized person alone is going to use the private key relating to a crypto-asset. This is made possible by a special procedure requiring for each action at least two concurrent authorizations out of a whole group, which is called multi-signature, or "multisig" for short. Additional functions for crypto assets, crypto currencies and blockchain are in development.



SECUROSYS

BLOCKCHAIN HSM




















Protecting the Key is Critical

As with any crypto-based infrastructure, protecting keys is paramount to ensuring a blockchain system's security. A successful Blockchain system needs highly reliable methods of interfacing with the strong key protection practices afforded by HSMs, and these HSMs must deliver the scaling and flexibility a decentralized blockchain model needs.

The Most Important Key Features At a Glance

- ▶ Key / Seed Generation
 - The HSM has a dual True Random Generator TRNG entropy source, and NIST SP800-90 compliant RNG.
 - Key derivation on asymmetric keys including built-in [BIP 32](#)
 - Direct secure address generation (hash of the public key), which delivers extra PQC protection in the HSM
- ▶ Side-channel protection
 - Prevents extraction of keys without compromising the storage
- ▶ HW-based tamper response
 - Cannot be compromised by software bugs
- ▶ Segregated functions in hardware and hardware "firewalls"
 - Prevents attack by silicon vendor
 - Mitigates risk from compromised software interacting with business logic
 - Process segregation that reduces risks associated with the communication stack being compromised
- ▶ Cryptographic functions in hardware
 - Side channel protection
 - Protection from Spectre / Meltdown kind of attacks
 - Field upgradable FPGA implementation
- ▶ Role model with multi factor authentication
 - Segregation of duties avoids risks with single admin having all information
 - Mitigates risks associated with hacked admin accounts
- ▶ Integrated key access control
- ▶ Device clustering for HA redundancy and performance scalability with integrated secure backup feature
- ▶ Smart Key Attributes (fine-granular access to individual keys)
 - Integrated multi-signature authentication scheme.
- ▶ Support for various crypto currencies
 - ETH, BTC based, Ripple, IOTA and many more

SUPPORTED CRYPTO CURRENCIES

 Bitcoin	 Cardano	 Tezos
 XRP	 Binance Coin	 VeChain
 Ethereum	 Monero	 Zcash
 EOS	 IOTA	
 Tether	 Dash	
 Litecoin	 NEO	
 TRON	 Ethereum Classic	
 Stellar	 NEM	

... and many more, including derivatives of top crypto currencies



Interested in what crypto security standards are applied in today's crypto exchanges? Or want to know more about integrated key access control?

Contact us at info@securosys.ch

securosys

Securosys SA is a market leader in cyber security and encryption based in Zurich, Switzerland. Founded in 2014, Securosys secures the Swiss financial markets on behalf of the Swiss National Bank and protects transactions worth over 100 billion Euros every day. The company serves more than half of Tier 1 banks worldwide with hardware security modules developed and built in Switzerland.



Securosys SA
Förllibuckstrasse 70
8005 Zurich, Switzerland

Email info@securosys.ch
Phone +41 (0)44 552 31 00
www.securosys.com

