securosys

Secure Enterprise-Grade Key Management

for Crypto Assets and Blockchain Systems

Whitepaper for Securosys SA (**"Securosys"**)
Initial Token Offering

Secure management and storage of private keys for crypto assets and blockchain systems is paramount. Existing solutions like printouts or offline storage on USB sticks are neither secure nor reliable, nor do they scale for institutional applications. **Securosys** is extending the functionality of its hardware security modules (HSM) for secure storage, access and use of blockchain and crypto assets keys.

Also, **Securosys** will develop secure computing platforms and key management systems, which are currently lacking in blockchain systems. To support and serve customers on-site all over the world, Securosys is going to expand its international presence.

Securosys has decided to conduct an Initial Token Offering (ITO) to finance the development of the mentioned new platforms and the scaling of its existing operational business. These tokens can be converted into **Securosys** company shares. They entitle to the same amount of dividends as the corresponding company shares. **Securosys** has reserved 25% of its shares for this ITO.

The following whitepaper details the value proposition of our business, the products we deliver and the token sale including the token mechanics.

Securosys is a proven company, with a proven team, and proven products. Securosys HSMs protect the Swiss financial infrastructure operated by SIX Group AG on behalf of the Swiss National Bank, securing financial transactions of more than CHF 100 Billion every day. In 2017 Securosys had revenues of CHF 4.7M and an EBITDA of CHF 1.1M, and thus achieved the second year of profitability.

CONTENTS

01

/ Blockchain and Crypto Assets Secured by Yesterday's Systems

Synopsis

The rise of Bitcoin and other crypto assets has provided a disruptive change to the Internet. A network of information now has become a network of value, too. In every aspect of life we are concerned with storing our values in a safe way, but in the crypto sphere, this is not an easy task yet. Switzerland based **Securosys** identified a large need for security in handling crypto assets, private keys, and a safe execution of blockchain protocols. That is why we are expanding our existing product line of high security hardware to the blockchain and crypto sphere.

Securosys is an expert in high-security technology. Our products are proven in traditional financial exchange markets and will now be applied to new markets. We believe that an Initial Token Offering is the most suitable way to finance this endeavor. By raising money within the community affected and targeted by our products, we want to achieve a widespread adaptation of the Token. To make it attractive and to stand out of the mass of tokens sold at this time, we will entitle SET Token holders[1] to an equivalent of 25% of all future dividends and potential exit gains generated by **Securosys**. The token also carries the option of converting it to shares of **Securosys** in case this is wished. We are Switzerland based, fully compliant with Swiss regulations, and certified by multiple quality control providers.

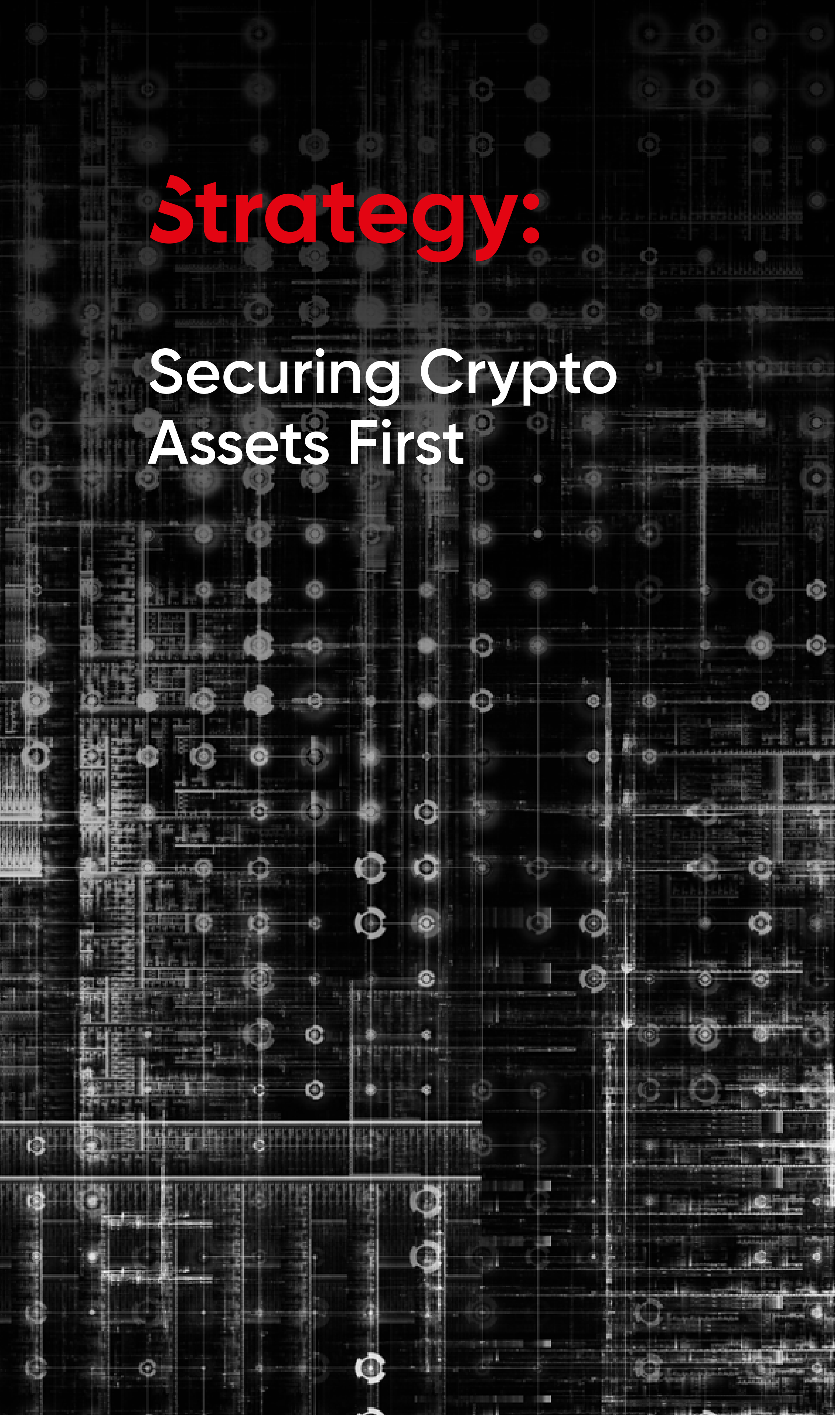
Today's systems are neither secure nor reliable for holding crypto assets. Trading in crypto currencies is conducted with minimal security and safety. The private keys, which represent entitlement to actual funds and identities, are not properly stored. Today's systems just leave them on computers and desktops, open to anybody who has access or can penetrate the system. So-called cold storage systems try to take these private keys offline. This is done by printing them on paper or storing them on a USB key. Neither of these solutions satisfies the requirements of secure enterprise-grade systems, nor do they scale for institutional applications. In addition, such solutions do not allow for multiple and quick accesses as they are needed in professional applications. They also cannot guarantee long-term (multi-year) availability.

[1] The token holder is deemed as the person that is entitled to certain tokens.

Markets in Desperate Need for Secure Solutions

Holding crypto assets, the private keys, on paper or on a USB key, might be an acceptable solution for small, private investors. However, they do not meet security requirements for institutional investors. These storage methods do not meet their need for operational efficiency, speed and volume of transactions and ability to comply with regulations. The approach of storing keys on off-the-shelf servers solves the scalability problem, but leaves a huge gap in security, as these machines are not designed to handle high-level security data.

Rules, regulations, as well as audit requirements on financial systems require safeguarding private keys securely in Hardware Security Modules (“HSMs”). This, for example, is the case in the Swiss SIC system and the SWIFT international payment network. To reach the same level of trust and reliability in blockchain and crypto assets systems, it is a must to adapt these systems to offer an equivalent level of protection.



Strategy:

Securing Crypto Assets First

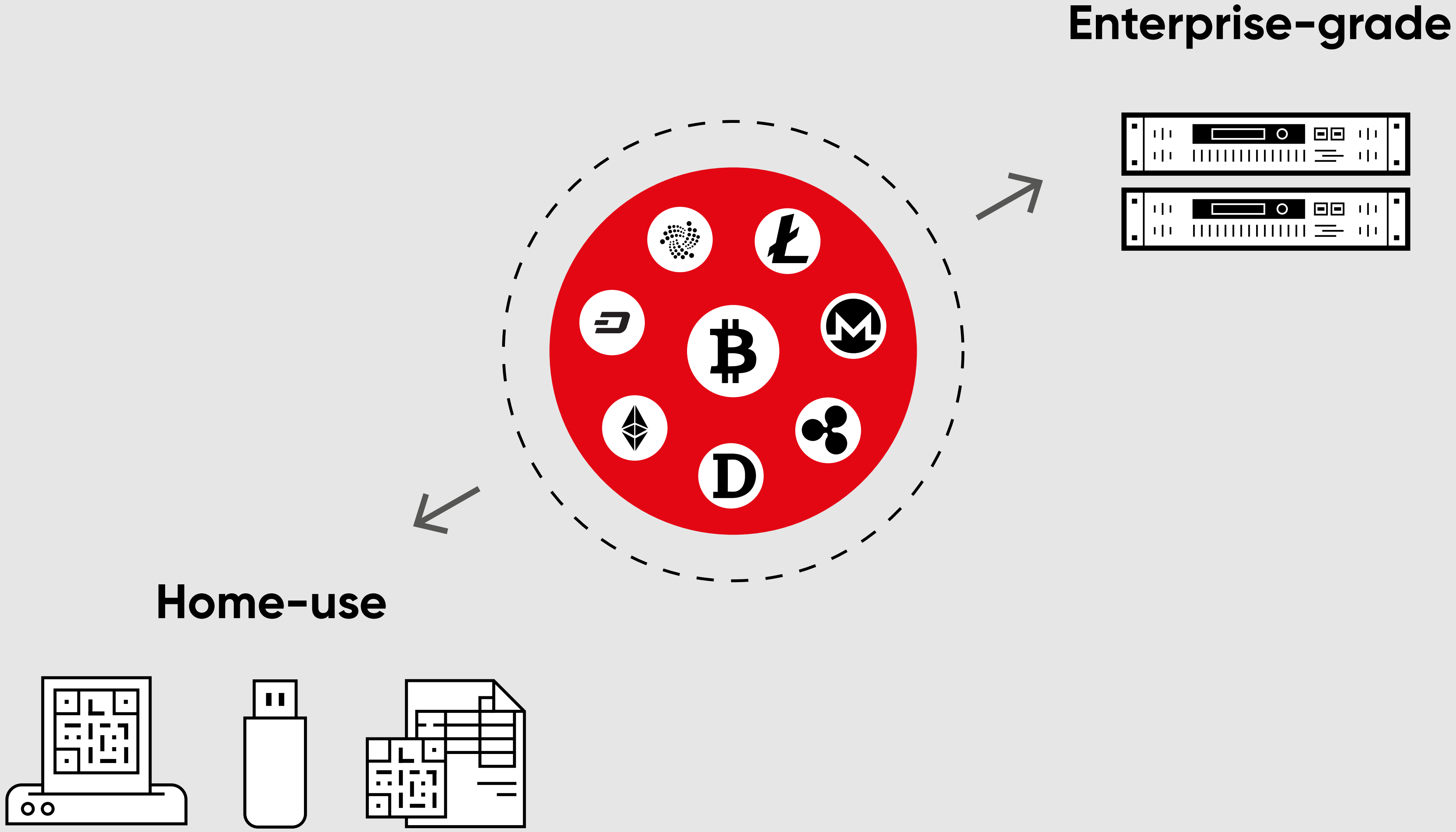
In order to protect private keys properly, they need to be stored in tamper-proof, reliable systems protected against unauthorized access. These systems have to be capable of performing all operations required for trading and storage without delay. The keys must be stored in future-proof digital vaults that stay operational for decades. The proven solutions are purpose-built hardware security modules (HSM) that are operated in redundant configuration.

Securosys already offers a range purpose-built HSMs that are used to protect financial transaction systems. These include the SIX Swiss Stock Exchange and the Swiss Interbank Clearing System (SIC). In the latter, Securosys HSMs are used in the settlement of transactions amounting over 100 Billion USD daily[2].

These network security appliances – HSMs – are the most secure way to protect private keys. By expanding the line of Securosys HSMs with specialized functionality, they will meet the very demanding requirements of crypto assets and crypto currencies. Also, they are going to provide secure storage, scalability, and operational ease for secure enterprise-grade applications. The resulting Blockchain HSM (called BC-CA HSM) will provide native support for crypto assets, tokens, and currencies like Bitcoin, Ether, Ripple, Iota, and their derivatives. They will also support operational processes like multi-signature (“multisig”) approval to use the private keys and allow for a secure and easy integration. It is the perfect platform for institutions and organisations like banks, funds, and custodians to securely manage private keys of crypto assets.

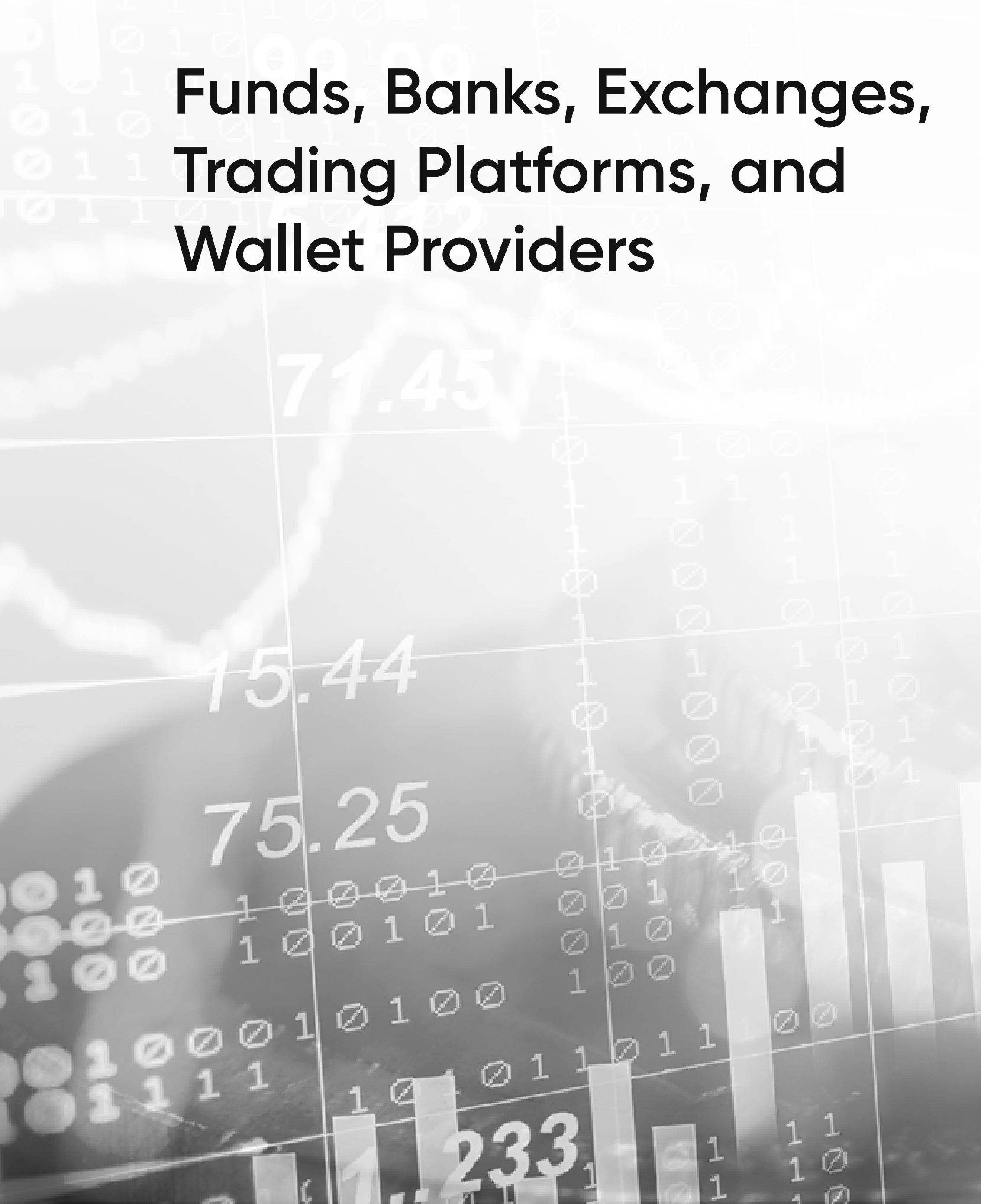
[2] SIC is a traditional financial system, therefore, it does not operate every day of the year but only from Monday to Friday, excluding Swiss holidays.

So far, crypto assets like Bitcoin, Litecoin, Ethereum, etc. are used by early adopters – individuals who manage crypto currencies on their home systems. With institutional investors moving into the space, these home-grown solutions do not scale to the enterprise level. For secure, reliable, and manageable operations HSM, hardware security modules, are needed.



Use Case & Market:

Funds, Banks, Exchanges, Trading Platforms, and Wallet Providers



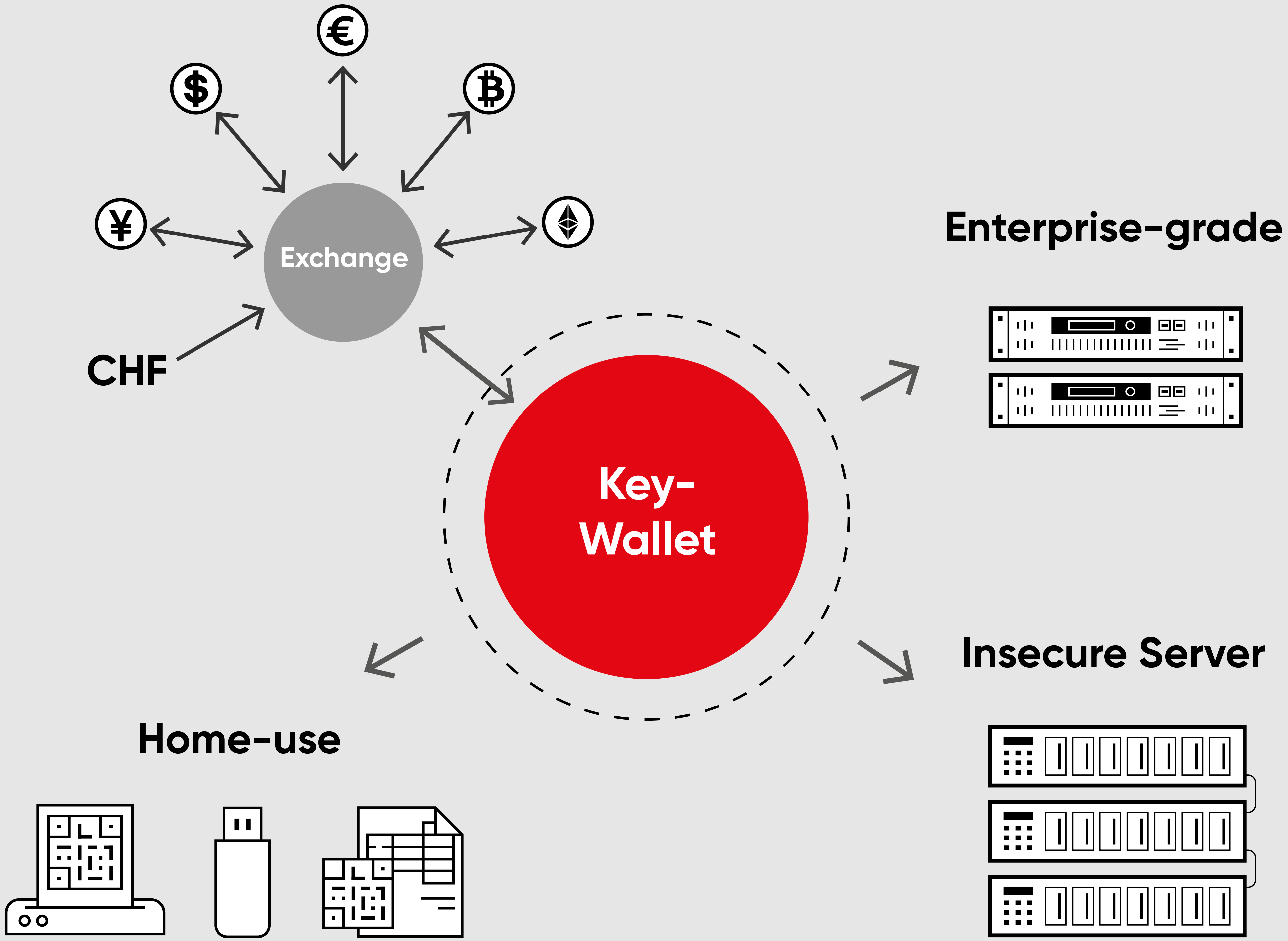
While banks that are moving into the crypto assets space understand the need to protect private keys, first movers are often overwhelmed by the complexity and thereby are at high risk of losing assets. In this group of pioneer adopters almost anybody knows someone who has lost private keys or wallets (software constructs that hold private keys) at least once. Crypto wallets, which are not properly secured, are exposed to very high risks. They can be drained by means of identity theft and unauthorized use of the private keys. Once a wallet or private key is lost, it is gone for good. It is cryptographically nearly impossible to find it again. Numerous real world examples already exist and a few of them have incurred huge losses[3].

The hack of Mt. Gox [6] was the first and probably the most prominent incident. Hackers looted about 740,000 Bitcoins after having copied Mt. Gox's private keys from a "wallet.dat" file not appropriately protected. Only recently, an USD 500M incident was reported on the digital currency XEM [7]. Unfortunately, this is not a phenomenon that is going to go away soon. The first of eleven predictions by The Element Group sees the hacking of a major coin exchange in 2018 "… due to lax operational standards and risk management infrastructure" (see [8]).

The institutional first movers, which are taking crypto assets management and trading to the institutional level, have realized the need for secure enterprise-grade solutions. **Securosys** is already working with industry-leading FinTech companies to provide hardware solutions for securing crypto assets.

[3] Beside Mt Gox, new examples are the theft of NEM tokens valued $500M from Coincheck in 2018, the $187M Nano tokens stolen from BitGrail, and the manipulation of wallets at Binance.

Exchanges for crypto currencies are at the forefront of handling crypto assets for their customers. Wallets holding customers' keys need to be secured properly. Thefts of crypto exchanges, ranging in the billions, could have been avoided if hardware security modules had secured the wallets. Instead, assets were left unprotected on servers on-site and in the cloud.



Use Case & Market:

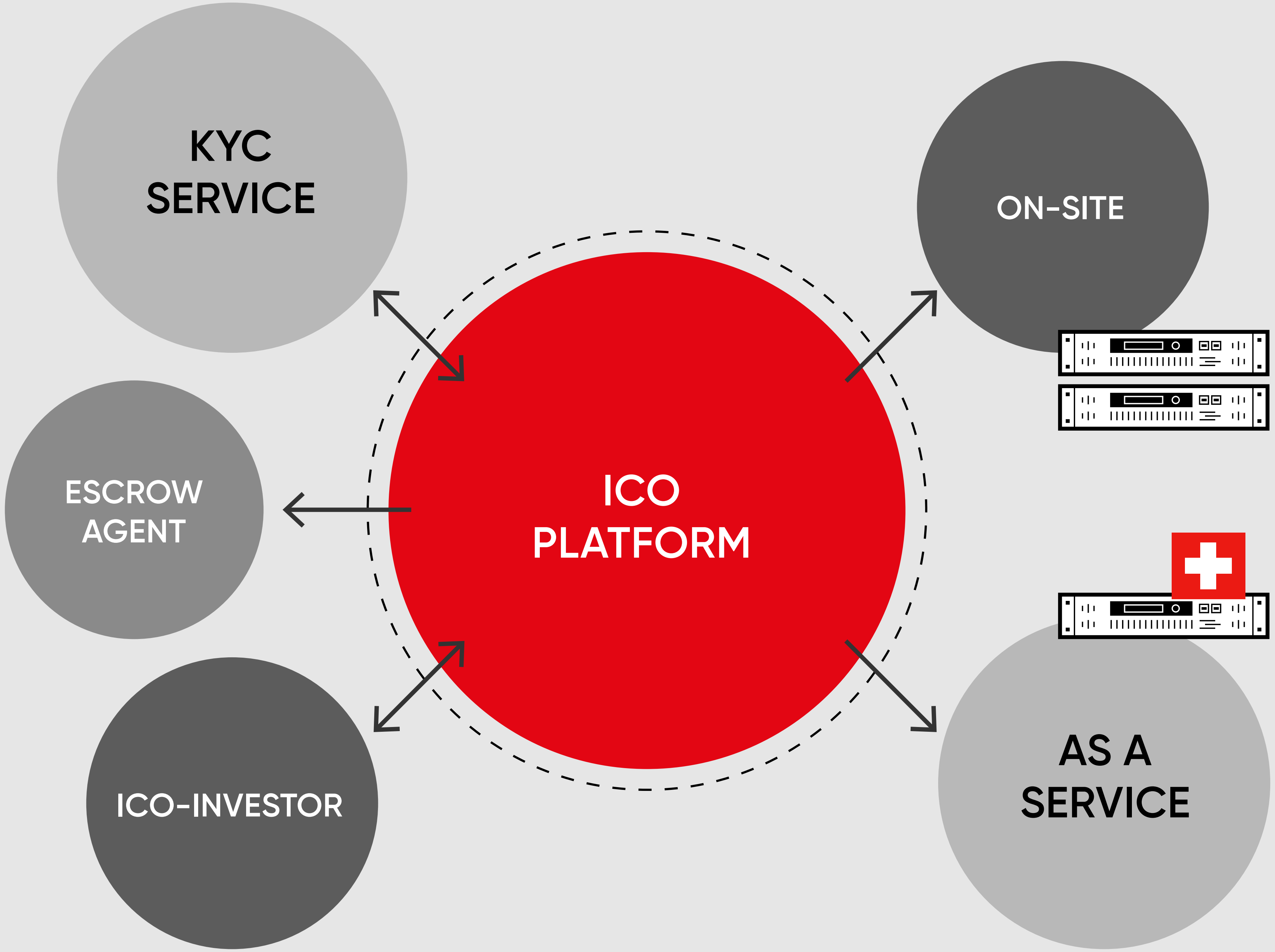
ICO Platforms

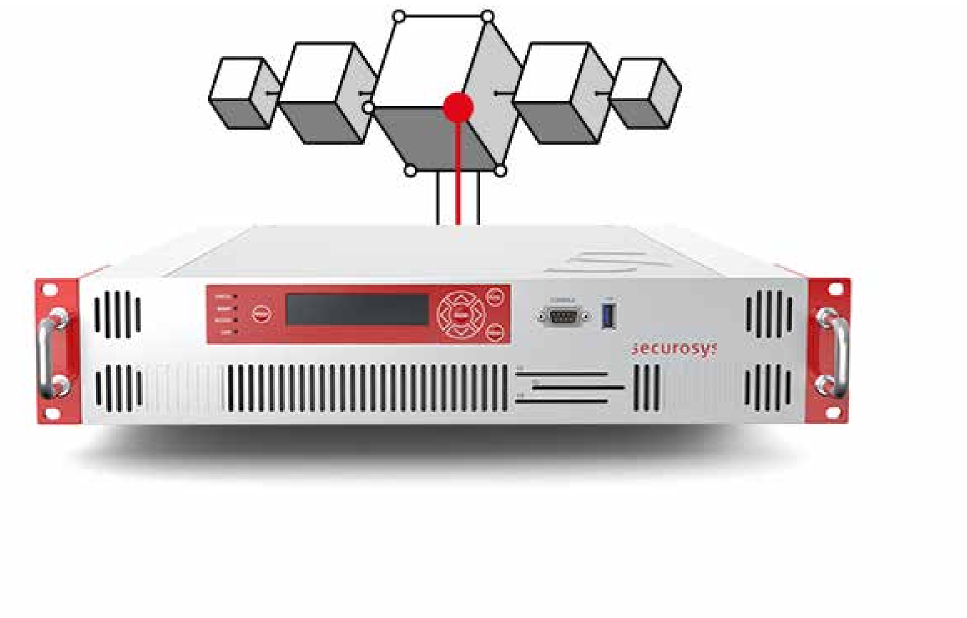
Initial coin and token offerings (ICOs/ITOs), like the SET ITO proposed in this whitepaper, are an efficient funding alternative at any stage of a company. They can complement or replace venture capital-based funding and initial public offerings (IPO). They allow a larger audience to take part in the early financing stages. So far, only private investment companies, i.e. venture capital companies, were able to participate in most of these investment opportunities. Also, ICOs might move IPOs to a new stage, the IPO 2.0, through tokenization of shares and securities. This new IPO 2.0 market will require offering platforms that are stable, reliable, efficient, and secure. It is the digitalization of the process that allows for a greater automation and thus the possibility to handle a larger audience. Moreover, capital markets are desperately looking for tools to conduct ICOs in a secure and compliant way.

However, currently existing (legacy) systems often lack the efficiency needed to handle massive amounts of small-scale investors. Transactions from thousands of participants have to be processed manually, which is not only costly but is also lacking security.

To increase trust and security and simultaneously provide scalability, an enterprise-grade platform has to be developed using blockchain-ready HSMs. It is evident, given the advantages of the process, that many long established players like the big consulting and accounting firms will move into the ICO space and play a dominant role. **Securosys** started working with an early mover to build a secure ICO platform that takes full advantage of **Securosys** technologies. In particular, the increased scalability of an automated solution with secure enterprise-grade key management is going to be superior to existing ICO platform systems.

ICO Platforms have to provide and work with many services. This includes KYC/AML (know your customer/anti-money laundering) regulations and escrow agents. A key function is also to provide the first wallets for the ICO/ITO investors. The only secure, scalable and reliable way is with HSMs, either by operating physical boxes or as a cloud service.





Product:

Blockchain and Crypto-Assets HSM (BC-CA HSM)

Several companies offer HSMs for typical public-key infrastructure (PKI) systems. Yet, they do not provide a viable solution for blockchain and crypto-assets systems. Critical blockchain-specific operations must be executed within the HSM using private keys that cannot leave the protected environment of a HSM.

Securosys will add the following functionalities to its HSMs that can be accessed from applications running outside of the protected HSM environment:

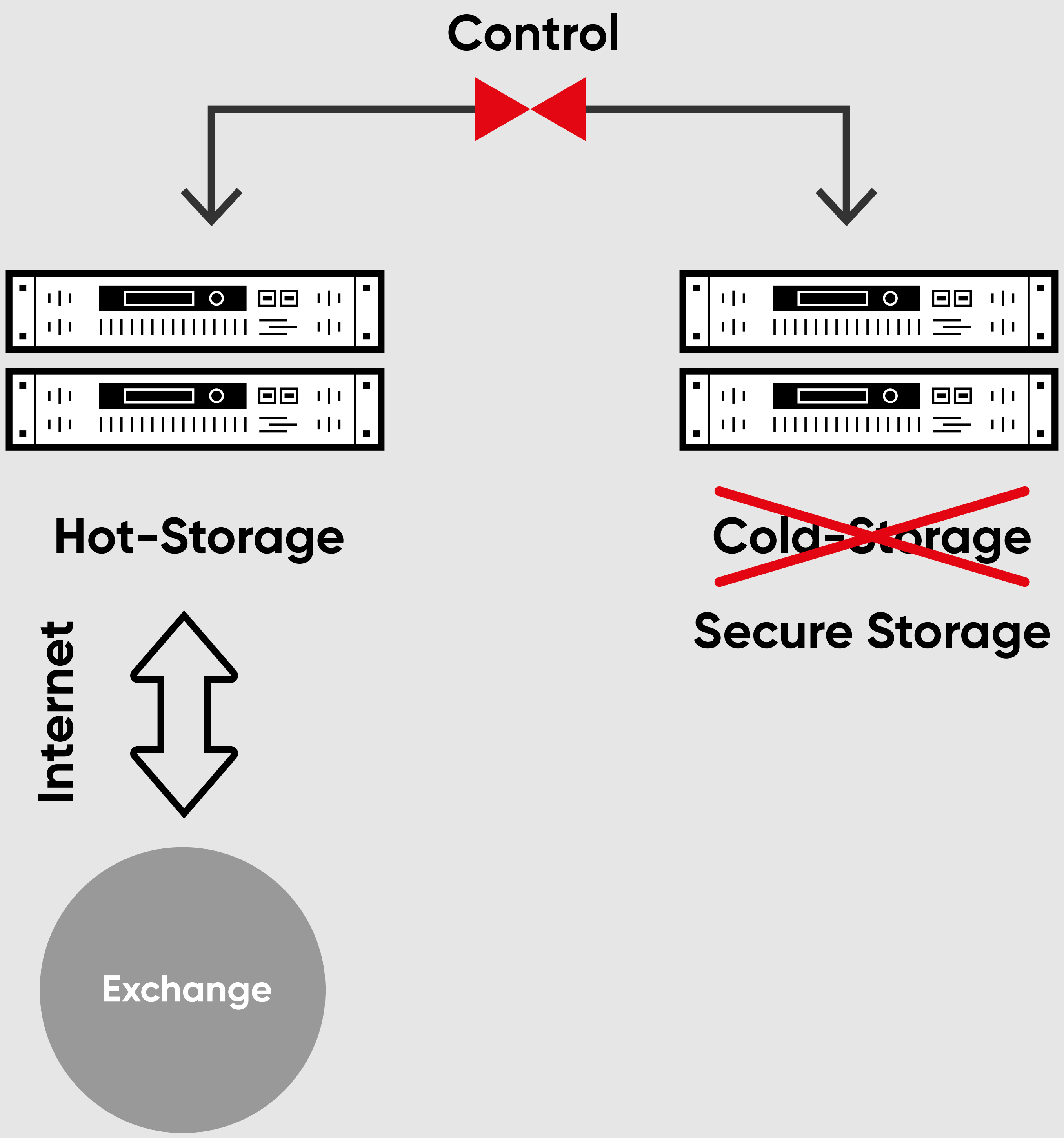
- Native support of algorithms and mechanisms used by different crypto currencies[4];
- Enhanced access control to ensure that assets based on private keys are not distributed erroneously, lost, or stolen;
- Multi-signature authorization capabilities;
- Efficient and secure methods for online (hot) and offline (cold) storage;
- Efficient and secure methods to transfer assets between hot and cold storage.

Securosys is in the process of adding these functionalities in its existing line of products for present-day customers. Since crypto finance is still in its infancy, this will be an ongoing effort.

[4] For example, the algorithm ECDSA with the secp256k1 curve that is used in Bitcoin and Ethereum.

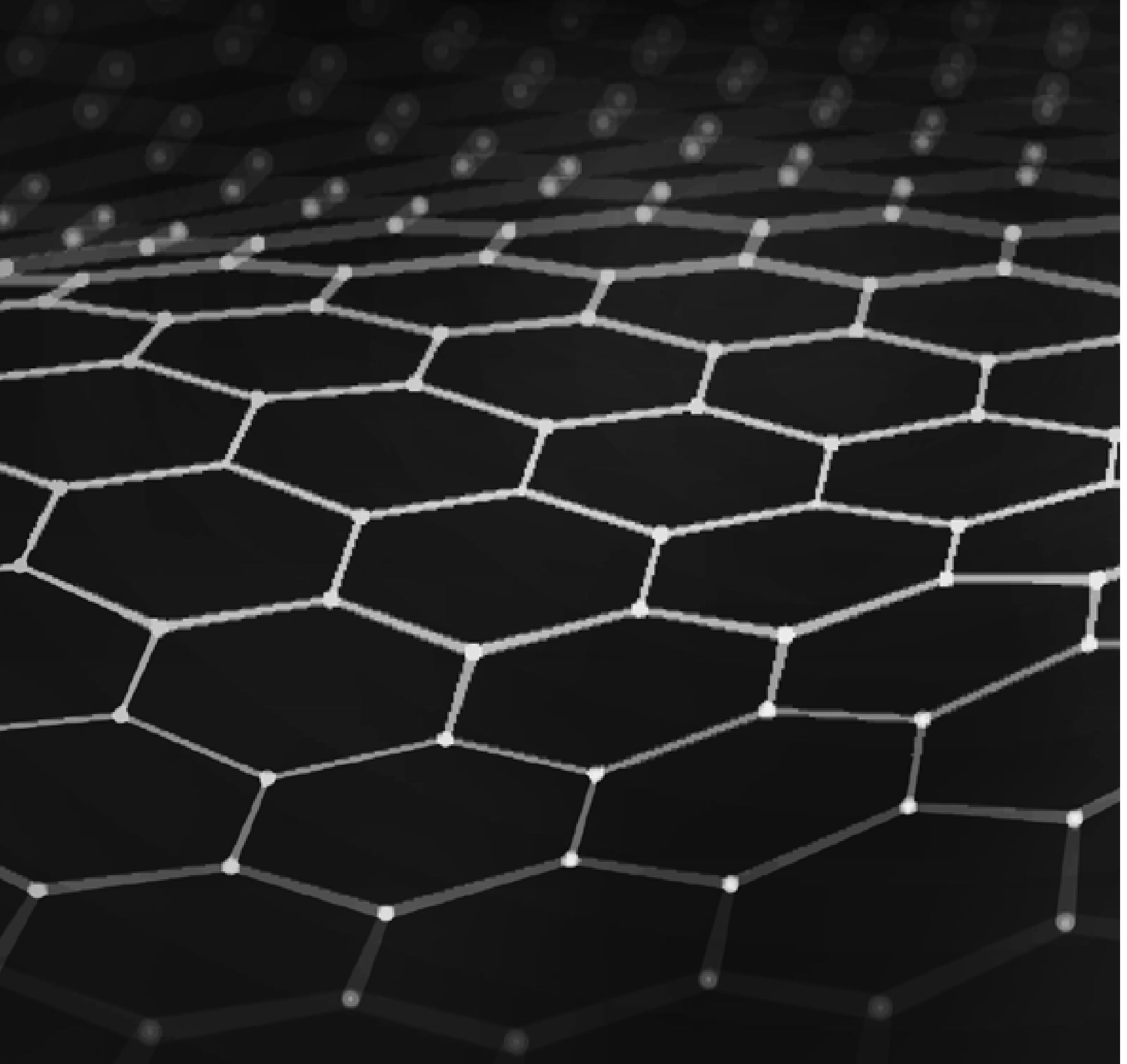
Cold storage used to be the way for the crypto community to keep assets secure. Nonetheless, paper or USB keys are neither reliable nor safe, nor do they guarantee long-term availability. Crypto assets should be accessible immediately, similar to funds in a savings account. With Securosys' HSM clusters, crypto assets can be securely moved between hot and secure storage as demonstrated by the systems of our solution partner Crypto Storage AG.

The BC-CA HSM is the perfect platform for banks, funds, custodians, and any other institutions which want to offer secure storage of crypto assets to their customers. Moreover, it serves a critical need of crypto exchanges and ICO platforms for the secure generation, management, access, and use of private keys.



Strategy:

Expand Hardware Security for Blockchain Systems



Currently, blockchain systems are operated on standard shared computer platforms, on-site, in the cloud, or on virtualized systems. As the recent vulnerabilities of Spectre and Meltdown [1] have shown, these platforms are not secure as long as unknown programs can be executed on the same hardware. This is typically the case in virtual machine (VM) systems. In particular, anybody running a full blockchain node or a block verification platform like a lightweight node, is exposed. The pitfalls may lurk in unexpected places like the code of a smart contract. The solution is a trusted execution platform, where only known programs and processes are running without any chance of unintended interaction. This goes beyond the simple software protections of VMs. It needs to be controlled taking the hardware into account. Such a trusted execution platform is going to fit subscribers' needs of public and private blockchains.

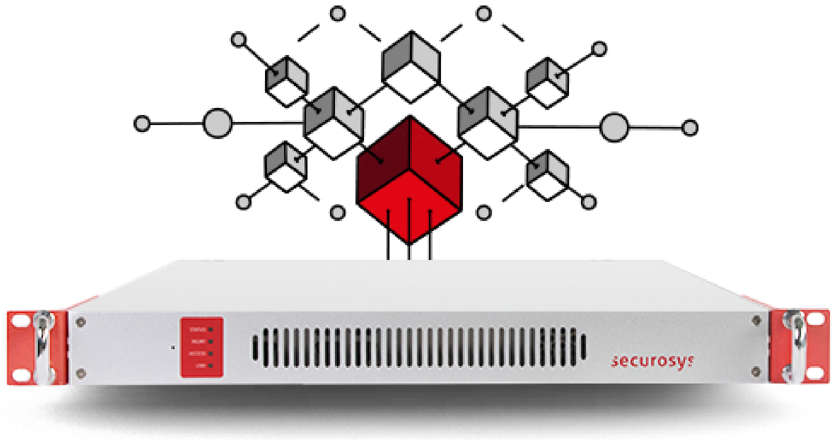
Recent developments in blockchain functions require an even higher protection. Platforms running Proof-of-Stake (PoS), lite nodes, or lightning nodes in the Bitcoin environment must not only provide tamper-proof functionality, they also have to keep the assets associated with them secured. This is a task that a trusted execution platform, developed by **Securosys** with a HSM (called "TEP HSM"), can provide. The TEP HSM can be used for many applications including financial services, FinTech, IoT, energy services, insurances, etc.

Use Case & Market:

Any Blockchain System

While the focus is currently on crypto-currency systems, more and more blockchain systems will evolve for many different markets and applications. These include public and private blockchains as well as permissioned ledgers where the ledgers are shared among invited participants. Such systems will include stock exchanges and commodity trading platforms that will take advantage of blockchain technology. In addition to efficiency gains, this technology facilitates compliance with regulatory requirements.

Currently, many existing crypto-currency blockchain systems are being expanded. Improvements include off-network systems to speed up transactions or to reduce transactions costs like the lightning network for Bitcoin. In addition, some crypto finance systems are modified to reduce the power consumption of mining operators – for example by implementing PoS instead of Proof of Work (PoW). In most cases lightning and PoS assets must be held on the node, thus requiring a secured execution platform like the Trusted Execution Platform HSM.



Product:

Trusted Execution Platform HSM (TEP HSM)

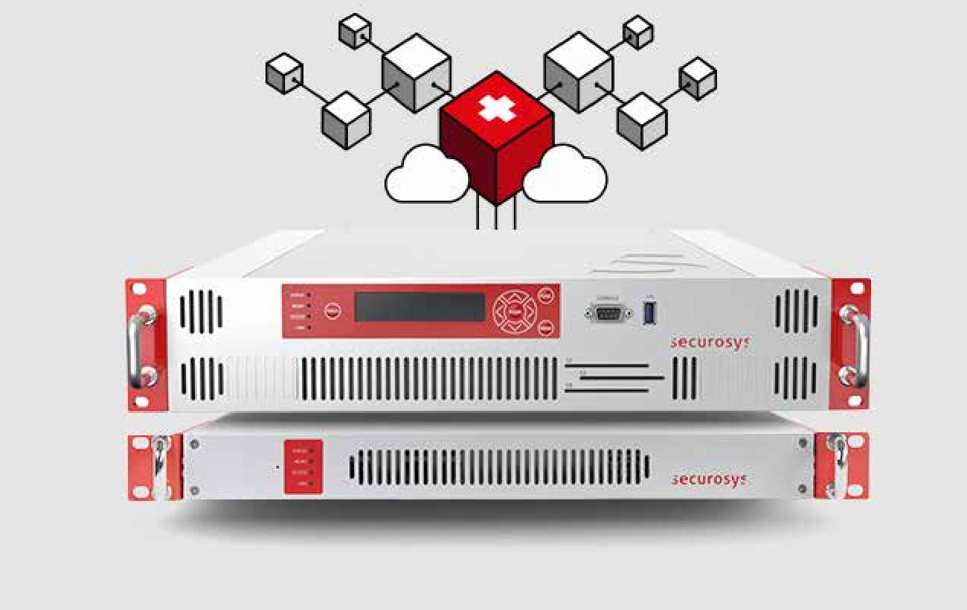
While the BC-CA HSM is targeted at specific usages with no option to run any applications, the Trusted Execution Platform HSM (TEP HSM) is a more open system. **Securosys** and its partners will include different applications in the TEP HSM that are needed for new functions in blockchain and crypto assets systems. These applications are going to be executed on the TEP HSM itself.

These applications include
(more will be added over time):

- Lightweight blockchain nodes to validate transactions and proper execution of smart contracts
- Transparent management of crypto assets including threats and alerts
- Secure lightning node (Caspar, Raiden, etc.) to execute off-blockchain transactions while properly protecting assets
- Proof of Stake (PoS) blockchain nodes to replace energy consuming mining while properly protecting assets, i.e. the stake
- Management of key wallets
- Crypto currency exchange
- Client management GUI
- Hosted services management tools

The advantage of the TEP HSM is that any application software is run in a shielded process on the system preventing any unwanted, uncontrolled interactions between the HSM and the TEP. Different than on a VM, where any random application can be executed only selected processes that are specifically compiled for the TEP HSM, can run on it. This prevents vulnerabilities like Spectre and Meltdown or any future issue of becoming a problem.

While it is technically feasible to add TEP HSM functionality to existing Securosys HSMs, this can only serve as an intermediate step to proof functionality. A more optimized next-generation TEP HSM platform will deliver an order of magnitude better performance, management efficiency, and improved application security.



Product:

BC-CA HSM and TEP HSM

ALSO AVAILABLE AS A SERVICE

Customers will have a choice to acquire the BC-CA HSM and TEP HSM devices from **Securosys** and operate them themselves. As an alternative to on-premise installation, the Securosys Clouds HSM Service will be expanded to offer the functionality as a hosted service.

Strategy:

International Distribution and Support

Even though **Securosys** already provides HSMs as a service (Securosys Clouds HSM) and is going to add the new products BC-CA and TEP HSM to it, customers are going to want to operate these systems under their own (physical) control and jurisdiction. International distribution and support is therefore required to serve customers worldwide.

Securosys will invest to expand its international reach by establishing local subsidiaries in key markets. Working with regional integrators and system providers to offer solutions matching different geographic needs. After further expansion within the EU, the establishment of local providers in APAC, Middle East, and Americas will follow.

02

/ Purpose of the ITO

Synopsis

Securosys wants to broaden its product portfolio for blockchain and crypto assets applications. In addition, **Securosys** plans to expand its marketing, sales reach, and growth globally. The following details the planned steps.

New Product Offerings

Primarily, new and evolving markets in the blockchain and crypto-finance environment will be addressed. The particular security requirements of these markets ask for adaptation of Securosys' product offerings, i.e. extended functionality of the HSM products (BC-CA HSM) as well as new platforms to serve specific needs (TEP HSM).

Extend International Reach, Distribution, and Support

To support FinTech and crypto asset-handling customers worldwide, **Securosys** is going to expand its marketing activities and sales channels into additional geographical areas. Improved international presence and logistics benefit both the existing international customer base and accelerate the growth of a new group of customers in the blockchain and crypto assets world.

Adding local subsidiaries will allow **Securosys** to interact with and manage its partners, resellers, integrators, and customers quicker and more efficiently. Deliveries can be managed from local inventory and repairs can be handled without the need of sending equipment or people around the world. Local support staff can provide assistance and serve customers immediately using their own language.

Expected Impact

These innovative products will allow **Securosys** to act as a first mover for the provision of secure and trusted infrastructure in the rapidly evolving global markets around crypto currencies, digital assets, blockchain, and autonomous systems. The real innovation introduced with crypto currencies is going to be the blockchain technology, which is bound to stay. It will change the way in which all kinds of organizational entities (e.g. government agencies, enterprises or automated systems) interact. To be widely adopted, however, blockchain technologies, public and private, require a secure and trusted infrastructure that **Securosys** is going to provide.

Securosys products and services will be the backbone of the infrastructure in the blockchain and crypto finance world. Customers and partners can leverage this to securely provide their own services and applications based on them.

Due to the expanded distribution channels, the existing and the new product portfolio will reach more customers. With the help of regional support centers, customers and partners get local support and quicker access to experts. This will enable **Securosys** to become an internationally recognized brand in the field of blockchain and cyber security.

The combination of new products with improved distribution will enable **Securosys** to grab a large share of the new blockchain and crypto assets market. As a result, it will allow the company to grow its revenues and profits substantially.

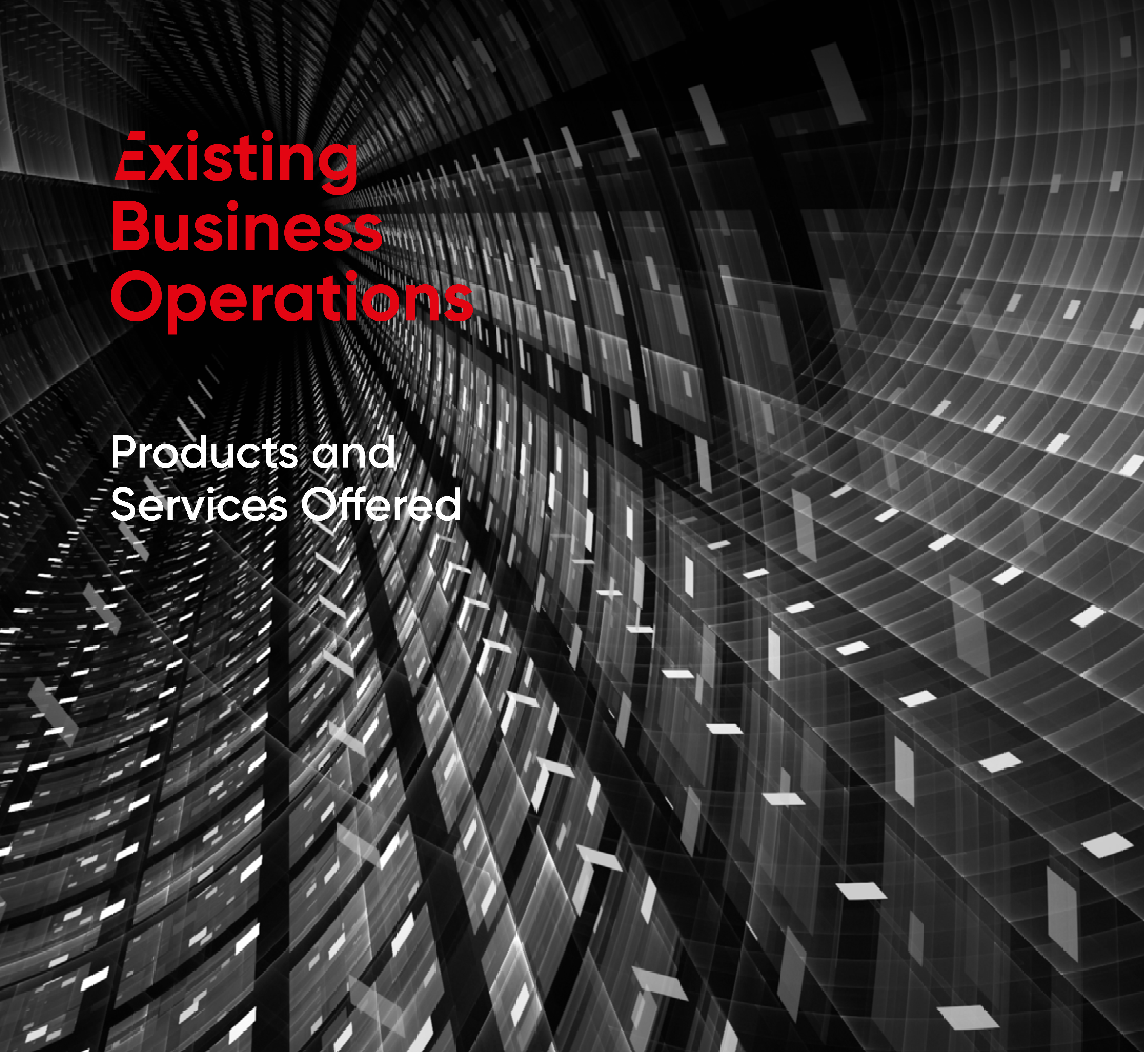
03 / Business Description

Business Model – Revenue Streams

- **Securosys** security network appliances – e.g. HSMs – are bought and operated by the customer. They are provided with an annual maintenance and support contract.
- Alternatively, these appliances can be rented, while the customer still operates them, maintenance and support is included.
- Licenses for TEP HSMs and the applications running on them.
- Many customers are used to cloud services and do not want to operate the equipment by themselves; they will rely on Securosys Clouds HSM services.
- Blockchain and Crypto Assets extensions will be sold as separate software licenses that only run on Securosys HSMs.

Sales Channels

Sale and distribution can either be fulfilled directly by **Securosys** or through our worldwide partner network that we already started to establish and will expanded with the proceeds of this ITO. Besides the established resellers and integrators of HSMs, we will strive to work with leaders in FinTech, banking, MedTech, financial consulting, energy, supply chain, and insurances that implement blockchain technologies.



Existing Business Operations

Products and Services Offered

Securosys offers a wide range of security network appliances and related services focused on encryption key management and encrypted communications.

Hardware Security Modules (HSM)

A Hardware Security Module is paramount to generate and store passwords, certificates, and encryption keys. Instead of having this critical information just stored in a file on a network server, it is securely locked away in a HSM. Therefore even if the network is breached and files are accessed, the most critical information, i.e. passwords, certificates and encryption keys, remain protected.

In blockchain and crypto finance systems in particular, the protection of private keys is paramount as it corresponds to the actual assets. If that private key is lost the asset is gone forever. If that private key is stolen, whoever has the key is in total control of the asset (e.g. he can sell it).

Securosys currently offers three different families of HSMs:

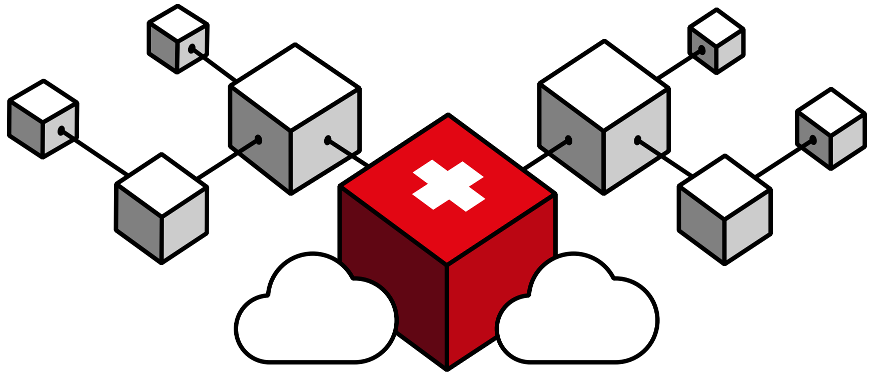
- Primus HSM S500
- Primus HSM X-Series X200, X400, X700, X1000
- Primus HSM E-Series E20, E60, and E150

The **Primus S500** is exclusively used in the Swiss Interbank Clearing System operated by SIX-SIC under the supervision of the Swiss National Bank (SNB). The **Primus X-Series** and **E-Series HSM** are generally available and can be used without any restrictions. When combined with the **Decanus** remote access device, visits to the datacenter can be avoided as most operations can be performed remotely without compromising security.

Decanus remote access terminal for HSM management

Primus HSM X-Series X200, X400, X700, X1000

Primus HSM E-Series E20, E60, and E150



HSM as a Service: Securosys Clouds HSM

The Securosys Clouds HSM offers data security at minimal effort and cost for the user. It is a HSM offered and used as a service. Running a HSM cluster professionally requires a wide range of expertise and resources, often lacking in IT teams. This service will suit organizations that handle sensitive customer data and consider owning, operating, and maintaining a HSM as too burdensome or not a part of their key capabilities.

Packages include:

- Clouds HSM ES (enterprise standard)
- Clouds HSM ECO (SME economy)
- Clouds HSM SBX (sandbox)

The HSM as a service is built on top of the Securosys Primus HSM. This very secure and high-performance Clouds HSM is located in and operated from Switzerland. This means the data is subject to Swiss data protection law, which is one of the strictest in the world.

The Clouds HSM service cluster is set up in two geo-redundant and dual-homed Swiss data centers. One is situated in the Zürich area, and the other one in the Swiss Alps in a former bunker of the Swiss Air Force. It is EMP secure underneath 1000m of solid rock, powered by green hydroelectric power.

Network Encryption Appliances

The **Centurion** encryption appliances secure broadband multi-site communications easily and cost-effectively. The built-in support of Ethernet and IP makes the devices ideal for all layer-2 and layer-3 carrier Ethernet, MPLS and IP networks in any configuration. It supports link, point-to-point, point-to-multipoint, or mesh networks. Neither network reconfiguration nor a sacrifice of performance is required. The mature and proven devices handle even the most complex network topologies with ease.

The **Centurion** is based on a platform of a vetted German partner and is enhanced with a **Securosys** true random number generator for key generation. The **Centurion** can perform the key management either itself or the Primus HSM can perform this task for it.

The following devices are available:

- Centurion H-Series H100M, H1G, H10G (100Mbit/s to 10Gbit/s)
- Centurion F-Series F40G, F100G (40Gbit/s to 100Gbit/s)

P&L Statement for 2017

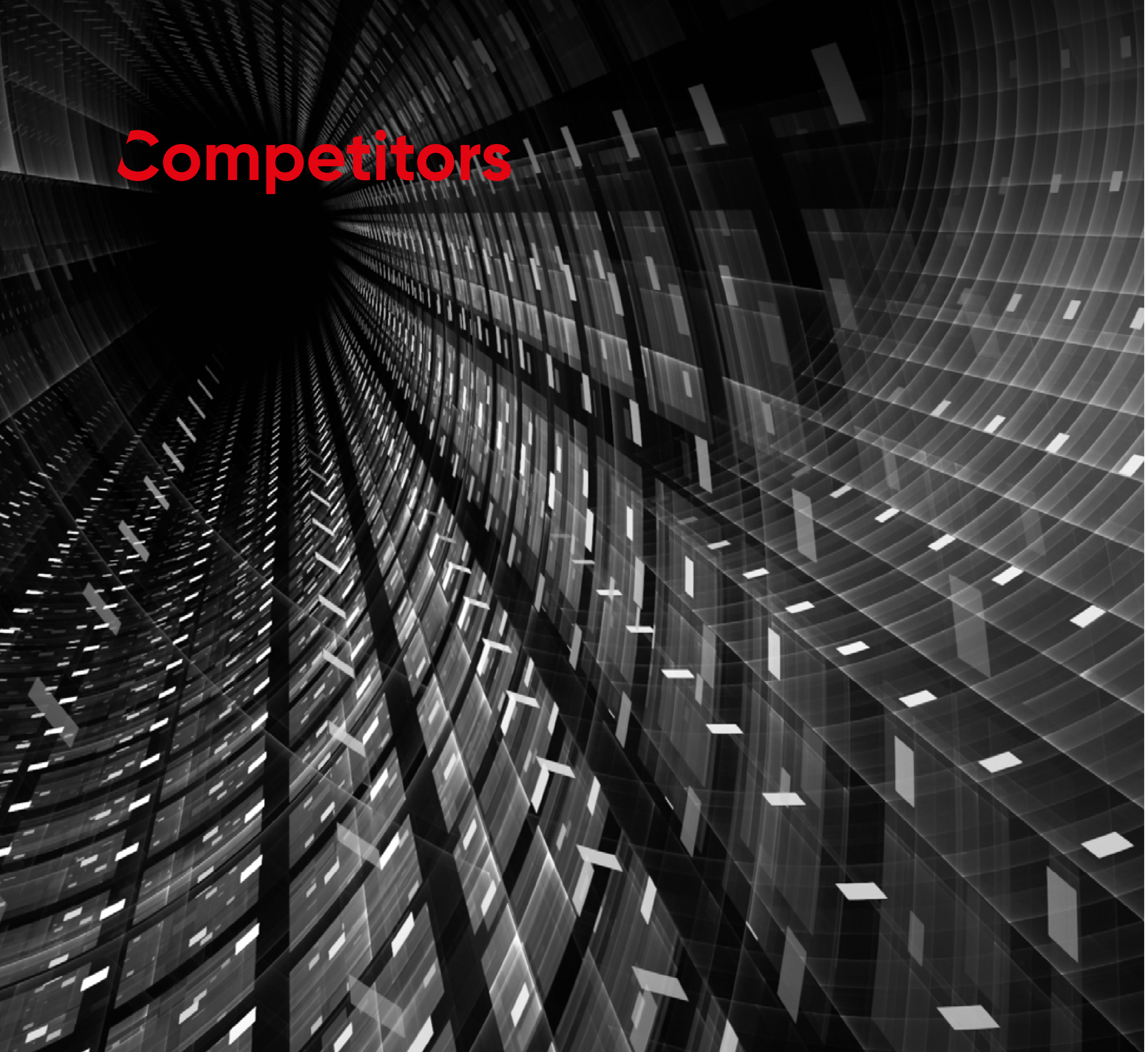
Securosys closed 2017 out with revenues of CHF 4.7M. EBITDA was CHF 1.1M, with a profit after taxes and depreciation of CHF 0.47M, resulting in the second year of profitability for the company.

Revenues	**CHF 4.7M**
EBITDA	**CHF 1.1M**
After Taxes and Depreciation	**CHF 0.47M**

THE SECOND YEAR OF PROFITABILITY FOR THE COMPANY

Market Overview

The crypto asset and blockchain market is still a blue ocean for HSM suppliers. There is not any company yet that has established itself as the leader in this market. **Securosys** will focus on becoming the go-to solution provider. However, in the existing HSM market, several competitors are active. Thales E-Security and Safenet/Gemalto (currently in acquisition by Thales) dominate the field. **Securosys** as a new entrant generated a big splash when it replaced the aging Safenet/Gemalto products by its trusted and more secure Securosys HSM platform in the Swiss Interbank Clearing system.



Competitors

Safenet/Gemalto

Safenet, based in Baltimore, MY, USA, was founded by two former NSA employees. Gemalto, a Belgium company, acquired it in 2013. End of 2017 Safenet/Gemalto signed a deal to be acquired by Thales for USD5.4 Billion. The takeover is yet to be approved by different regulatory bodies. While the deal creates a huge security company, it also opens the field for new and nimbler companies like **Securosys**.

Compared to Safenet/Gemalto, **Securosys** offers a more modern architecture platform with several key features such as synchronization across a cluster that offers better security and higher reliability. Based on customer feedback, Securosys HSMs are easier to integrate and deliver higher performance. Recently Safenet/Gemalto started to be active in the blockchain and crypto assets field.

Thales E-Security

Thales E-Security is part of the French defense conglomerate Thales, that builds cyber security equipment but also tanks, submarines, missiles, landmines, etc.

Thales own HSM platform originates from an earlier acquisition of NCipher out of Cambridge, UK. Due to the ongoing acquisition of Safenet/ Gemalto, it is still undecided whether both platforms will be maintained. This creates uncertainty with customers and in the sales channel.

Thales E-Security has also started to operate in the blockchain field.

Other Vendors

There are several, more locally focused vendors of HSMs. These include Utimaco in Germany, Kryptus in Brazil, and FutureX in the US. While some of them have tried to expand outside their home market, none has achieved a worldwide brand recognition so far.

Cloud HSM Providers

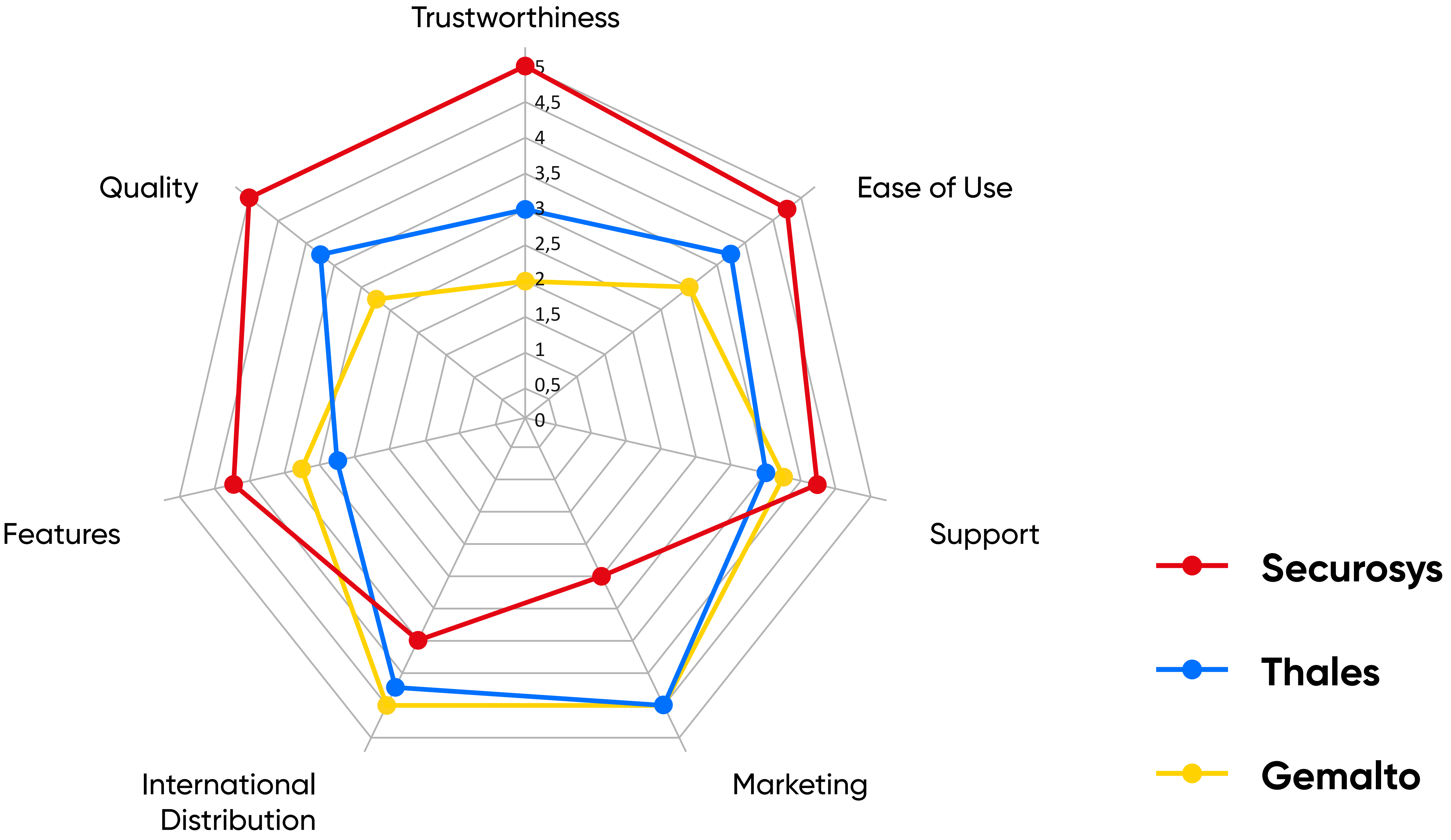
The main HSM as-a-service providers are AWS Cloud HSM and Microsoft Azure Vault.

AWS offers full HSMs for rent (until recently only Safenet/Gemalto HSMs, now also Thales HSMs). Here the customer is responsible for its configuration and operation. The service appears quite expensive in fees. Moreover setup and operation seem complex, requiring a lot of effort by the customer, while restricting usage.

Microsoft Azure Vault operates at the other end of the spectrum charging for single keys and per signature. This is very cost-effective and only becomes expensive when support and SLAs are required. This service uses Thales HSMs.

Several smaller providers are trying to offer HSMs as a service. However, they rely on the HSMs of big vendors like Safenet/Gemalto and Thales.

Comparison



Survey at SUDC2018 on May 23, 2018 in Zurich.

Existing Markets

Besides crypto assets and finance, Securosys HSMs are currently sold into the following markets:

- PKI
- legacy finance systems
- GDPR
- eID
- eIDAS
- digital signatures.

In finance applications, HSMs are used to provide appropriate protection for signing and verifying transactions. HSMs are indispensable parts not only of the Swiss Interbank Clearing system, but also for any payment transaction system.

A Public-Key Infrastructure (PKI) is used to establish a chain of trust so that a user, service, computer, or application can be authenticated, a secure connection established, or the origin of software or documents validated. This is achieved through certificates, which a PKI creates, manages and distributes, but also revokes. A certificate contains the public key and needs to be readily available. Its corresponding private key must be kept safe and secret. The appropriate level of protection can only be achieved by means of a HSM. Usage examples include securing Microsoft Active Directory Certificate Service (AD CS) and Azure Cloud Services.

The EU's General Data Protection Regulation (GDPR) came into effect on May 25th, 2018. It stipulates that personal data relating to EU citizens must be protected. The GDPR also applies to companies operating outside the EU that hold data on EU citizens. Anyone that fails to comply with the provisions on data protection risks a heavy fine. The only technical measure explicitly mentioned in the GDPR for protecting data, is encryption. It is important to note here that encryption itself is not sufficient; the encryption keys themselves must also be protected. Again, encryption keys should be stored on a dedicated device. Securosys HSMs and Clouds HSMs, are ideal for this purpose because they can easily be integrated into any environment.

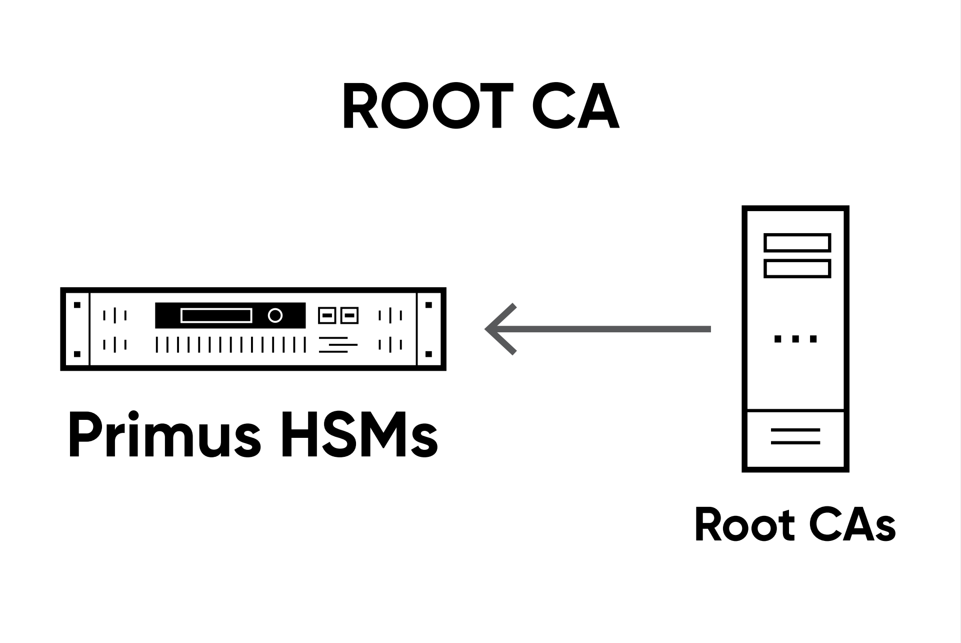
Electronic Identification (eID) solutions are currently widely deployed by governments and organizations, for example to access services provided by government authorities, banks or other companies. Issuers of eID are in need of generating, safeguarding and managing large numbers of private keys, which again need to be adequately protected.

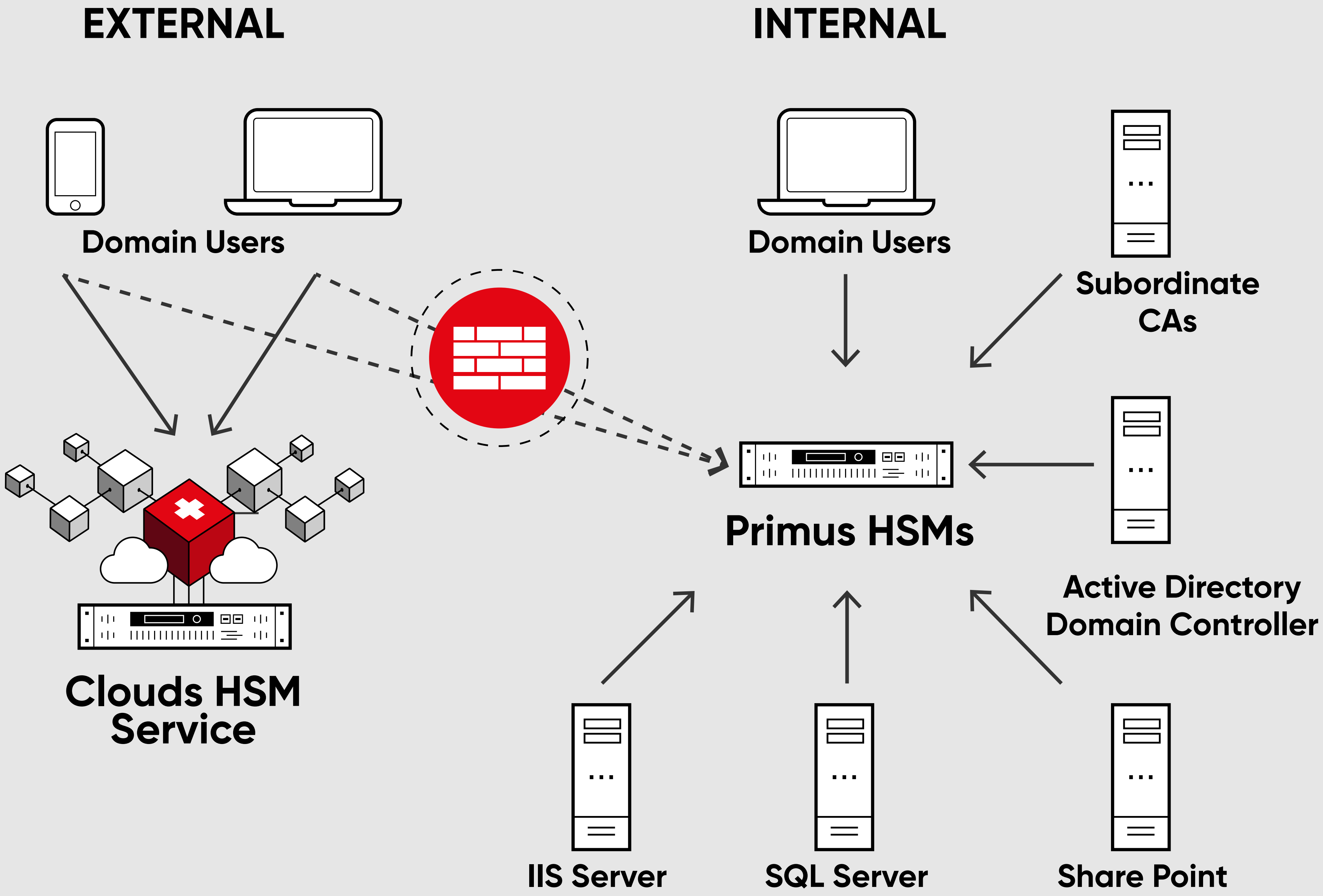
Recent EU regulations on electronic identification, authentication and trust services (eIDAS) for electronic transactions have created standards for qualified digital signatures, electronic seals, timestamps and other proof for authentication. To adhere to these standards, service providers need to protect their cryptographic keys in tamper-resistant devices, like Securosys HSMs.

Simple Integration of Primus HSM in Microsoft Systems

Microsoft

The Primus HSM can easily be integrated in a MS system by installing the Primus CNG Provider. This enables all Windows servers and clients to generate and store their private keys and certificates securely in the HSMs, and perform all related cryptographic functionality, like signing or certificate validation, hardware accelerated on the Primus HSM.





04 / Technology

Synopsis

The whole technology stack and intellectual property of the Securosys HSMs belongs to **Securosys**. This includes the design, hardware, and electronics of the Primus HSM, the software and firmware for bootloader, the different systems, as well as the FPGA[5].

Most of it was developed by **Securosys** itself, a small portion was acquired from vetted suppliers. As with any modern system, **Securosys** is also relying on open source software.

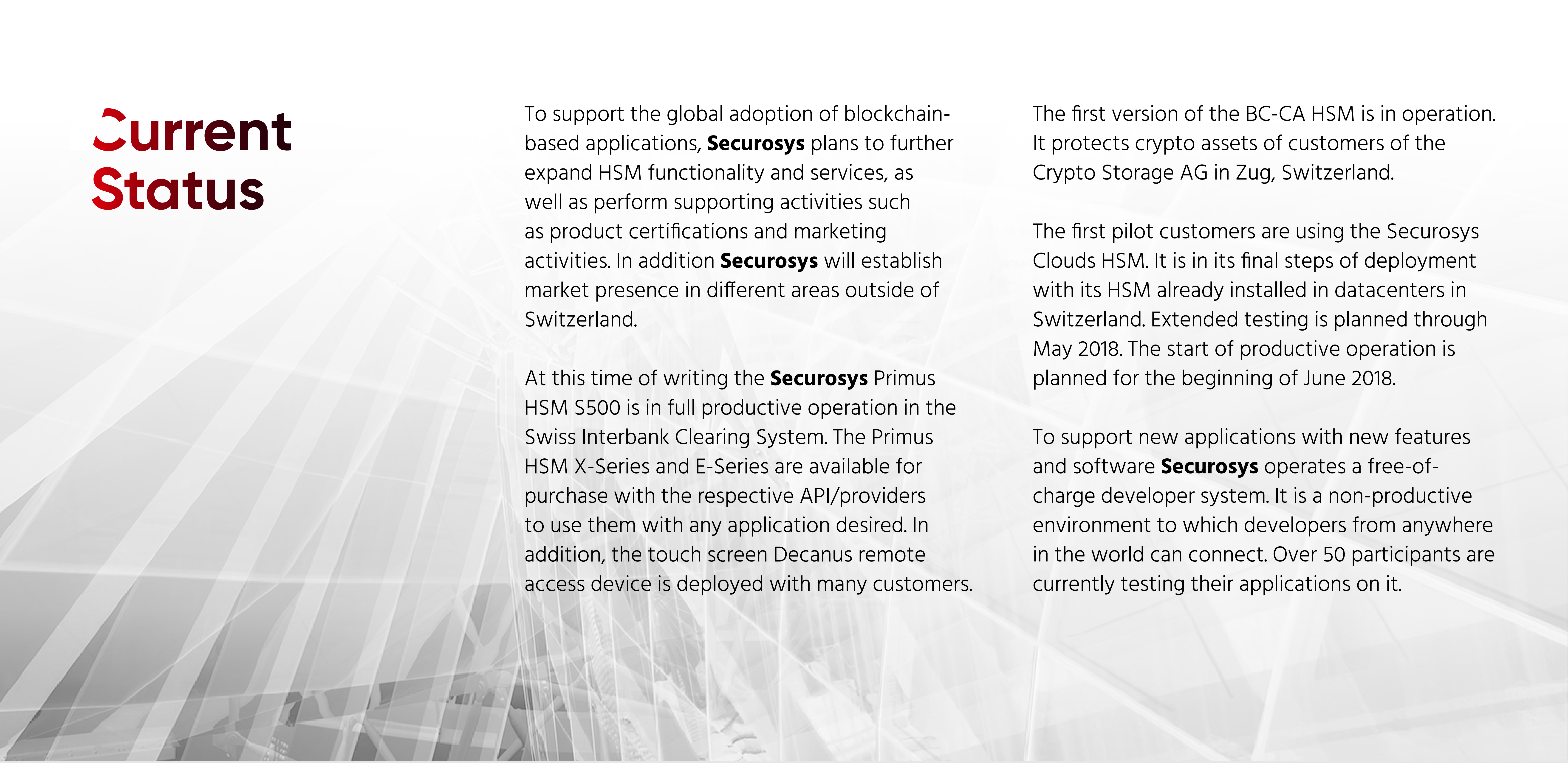
[5] FPGA are field programmable gate arrays. They are used to accelerate functionality that does not perform well on standard computer platforms. Examples are cryptographic algorithms, where a lot of long integer operations (512 bits to 4096 bits and beyond) are used.

Patents and Trademarks

Securosys is filing patents for certain HSM functionalities. Unfortunately, due to the delicate nature and criticality of the process (i.e. to prevent competitors from copying) the details thereof cannot be disclosed at this time.

The name securosys has been registered as trademark in Switzerland, Europe, USA, Australia, Japan, Singapore, and India.

05 / Proposed Roadmap



Current Status

To support the global adoption of blockchain-based applications, **Securosys** plans to further expand HSM functionality and services, as well as perform supporting activities such as product certifications and marketing activities. In addition **Securosys** will establish market presence in different areas outside of Switzerland.

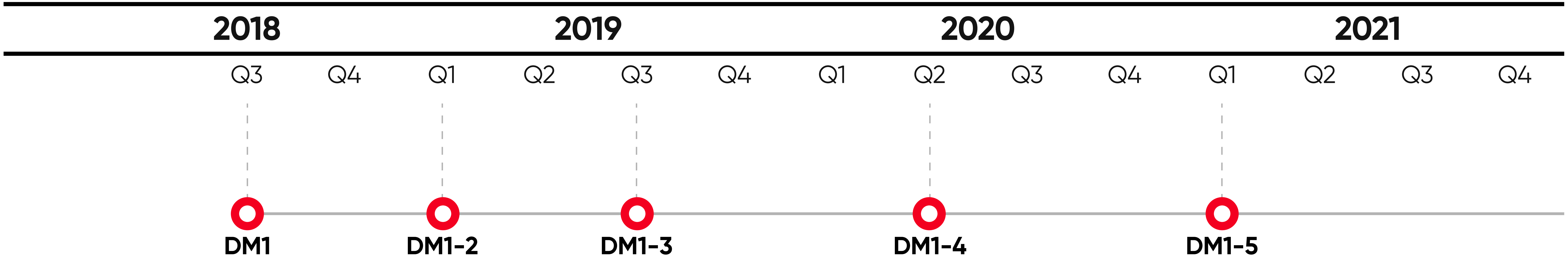
At this time of writing the **Securosys** Primus HSM S500 is in full productive operation in the Swiss Interbank Clearing System. The Primus HSM X-Series and E-Series are available for purchase with the respective API/providers to use them with any application desired. In addition, the touch screen Decanus remote access device is deployed with many customers.

The first version of the BC-CA HSM is in operation. It protects crypto assets of customers of the Crypto Storage AG in Zug, Switzerland.

The first pilot customers are using the Securosys Clouds HSM. It is in its final steps of deployment with its HSM already installed in datacenters in Switzerland. Extended testing is planned through May 2018. The start of productive operation is planned for the beginning of June 2018.

To support new applications with new features and software **Securosys** operates a free-of-charge developer system. It is a non-productive environment to which developers from anywhere in the world can connect. Over 50 participants are currently testing their applications on it.

Product Development: Blockchain HSM



2018 Q3: DM1

2018 Q4

2019 Q1: DM1-2

2019 Q2

2019 Q3: DM1-3

2019 Q4

2020 Q1

2020 Q2: DM1-4

2020 Q3

2020 Q4

2021 Q1: DM1-5

2021 Q2

2021 Q3

2021 Q4

Development Milestones (DM#):

DM1

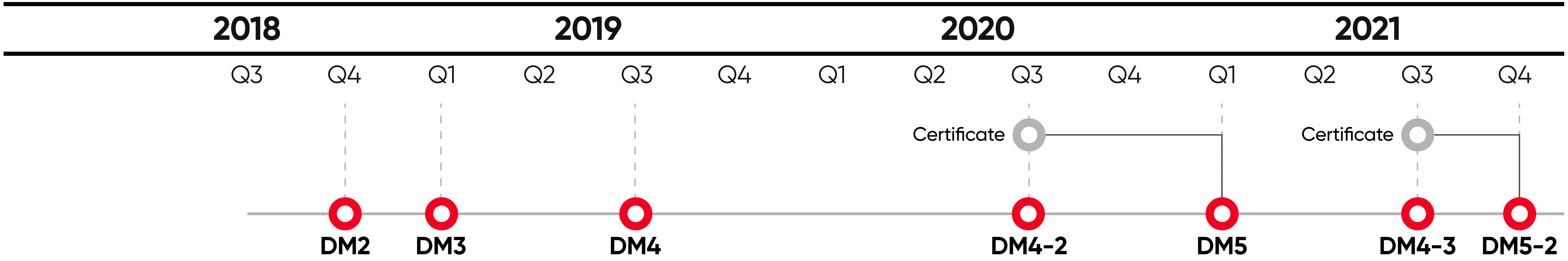
MVP (minimum viable product) for the BC-CA HSM to enable cold storage solution, multi-signature, and crypto currency functionality for the top 20 crypto currencies.

DM1-x

Updated versions of the BC-CA HSM.

The above represents the best possible timeline Securosys will deliver these products and services.

Product Development: Trusted Execution Platform HSM



Development Milestones (DM#):

DM2

MVP for the TEP HSM that can serve as blockchain node for lite nodes and execute smart contracts.

DM3

MVP for the TEP HSM that can also serve as a lightning node.

DM4

MVP for TEP HSM that can also serve as a PoS blockchain node.

DM4-x

Updated versions of the TEP HSM.

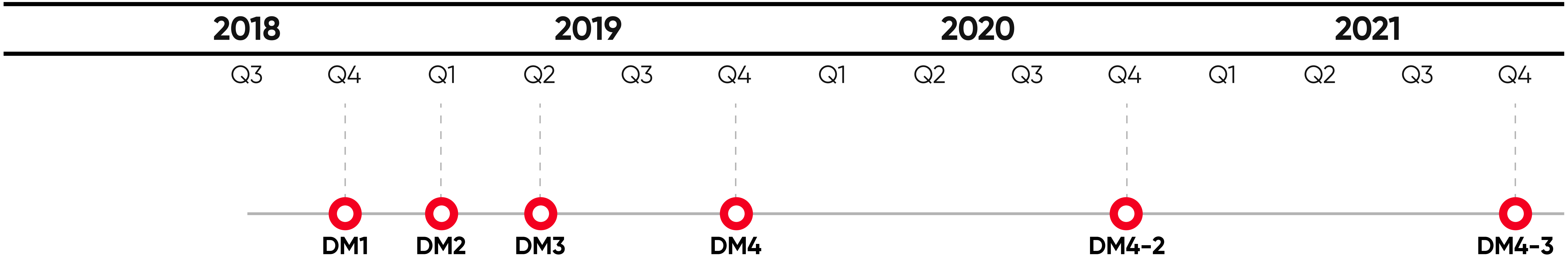
DM5

For those distributed ledger-based business applications that require certification of the underlying hardware, **Securosys** aims to certify the devices in accordance to FIPS 140-2 Level 3 and Common Criteria EAL 4+. This certification will be a costly and time-consuming endeavor[6].

The above represents the best possible timeline Securosys will deliver these products and services.

[6] Many applications used in regulated systems require these kinds of certifications. They typically take between 12-24 months and cost from $100,000 up to $250,000.

Product Development: Clouds HSM



Development Milestones (DM#):

DM1

MVP (minimum viable product) for the BC-CA HSM to enable cold storage solution, multi-signature, and crypto currency functionality for the top 20 crypto currencies.

DM2

MVP for the TEP HSM that can serve as blockchain node for lite nodes and execute smart contracts.

DM3

MVP for the TEP HSM that can also serve as a lightning node.

DM4

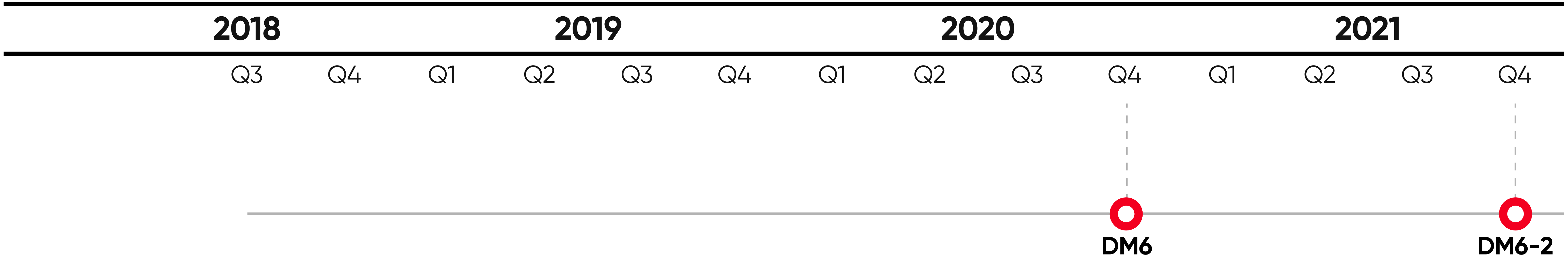
MVP for TEP HSM that can also serve as a PoS blockchain node.

DM4-x

Updated versions of the TEP HSM.

The above represents the best possible timeline Securosys will deliver these products and services.

Product Development: Key Management Server HSM



Development Milestones (DM#):

DM6

MVP for the Key Management Server HSM targeted at IoT.

DM6-x

Updated versions of the TEP HSM.

The above represents the best possible timeline Securosys will deliver these products and services.

Enabling Developers and New Applications in the Blockchain Community

Since mid-2015 **Securosys** is running a developer system. This system consists of a Securosys HSM safely located in a rack in our offices and is connected to the Internet. Upon request developers can get their own partition on this HSM with access credentials. This allows developers to test out their applications with Securosys HSMs immediately without having to setup their own system or going over lots of bureaucratic hurdles.

The same development platform is going to be used to give external application developers early access to the new BC-CA HSM, TEP HSM, and Key Management Server HSM.

Market Entries

A step-by-step introduction into the different markets is planned. In a first step, essentially any new MVP will be tested with a small group of pilot customers. This could include individuals who run their own blockchain nodes for a specific currency, small businesses that operate crypto asset management funds, companies that perform ITO/ICO services or even crypto exchanges.

In a second step we are going to engage the larger community with targeted marketing. This involves social marketing, using our own channels and channels of our partners, advisors, and SET Token holders. This will allow us to offer our products to retailers who want to operate lite nodes to verify transactions as well as to individuals who want to run their own nodes, whether to be part of the blockchain or to provide lightning node services.

Side by side to these efforts, we will write case studies and deliver white papers that explain the functionality of our new BC-CA HSM and TEP HSM in detail. On top of that, application notes will guide users and developers through the exact steps to setup and operate these devices.

At the same time, we will reach out to the large players in the crypto field directly. This includes the big exchanges, miners, ICO service providers, and large banks starting in the crypto asset market. It will also include the large nodes in lightning networks.

Strategic Partnerships

Securosys has already entered into strategic partnerships with several companies to push its technology forward and improve the economics and security of blockchain und crypto-finance transactions.

While some of these partnerships are confidential, the following can be disclosed at this time:

ITO Service Provider: A leading technology company has already started integrating Securosys HSMs into its system to provide higher security and to simplify operations.

Token exchange: Lykke has started exploring ways to integrate Securosys HSM into the existing Lykke Exchange.

Blockchain Valley Ventures (BVV), is a leading incubator, investor and ICO advisor in Switzerland. BVV uses Securosys HSMs to store and manage private keys as well as crypto currencies.

Cold Storage: Crypto Storage AG, part of the Crypto Finance AG group, is currently operating a cold storage solution for crypto assets on Securosys HSMs.

Lykke

BLOCKCHAIN
VALLEY
VENTURES

CRYPTO FINANCE

06

Background on Securosys SA

Company Story

Andreas Curiger and Robert Rogenmoser founded **Securosys** in **2014** (Swiss registry of commerce ID CHE-464.234.583). **Securosys** is a private limited shareholder company ("Aktiengesellschaft") falling under Swiss law. The company is fully owned by **Securosys** management, **Securosys** employees, and Swiss private investors.

Securosys' first years were highlighted by several honors and awards, as well as the development and delivery of the first HSMs to protect the Swiss banking infrastructure.

In June **2016**, **Securosys** was chosen as one of three finalists for the high-tech/biotech innovation award at the **Swiss Economic Forum** in Interlaken, Switzerland. In the same year Red Herring Europe recognized **Securosys** as the winner of its **Top-100 Award**.

Furthermore in **2017** the Swiss Economic Forum granted **Securosys** the SEF.High-Potential quality label, exclusively reserved to SMEs with proven growth potential. In May **2018**, **Securosys** and the Institute of Microelectronics and Embedded Systems at University of Applied Sciences of Eastern Switzerland in Rapperswil, Switzerland won the FUTUR Price for their research project on side channel attacks [2], [3].

Mission:

Protecting Digital Assets in Finance Systems

Securosys' success is based on technically superior, security-wise most trusted, and financially competitive products for hardware, software, and related services. These values enable **Securosys** to be the preferred partner of globally acting enterprises, public authorities, and industries for paving the way to cyber security in a fully connected digital world. The company puts its focus on protecting financial assets in blockchain and crypto systems as well as legacy finance systems.

Product Story

Securosys started out with the development, production and delivery of the **Primus S500 HSM** to protect the Swiss banking infrastructure. The **Primus S500 HSMs** are used in the Swiss interbank clearing and settlement system SIC operated by SIX Group AG under the supervision of the Swiss National Bank (the Swiss “Fed”). All banks in Switzerland process their financial transactions in the daily amount of over 100 Billion USD on this system.

- The development and production of the **Primus HSMs** started in the second half of 2014.
- Securosys' highly skilled and experienced team delivered a first prototype to SIX in April 2015.
- First customer shipment (FCS) of the dedicated product for SIC was in December 2015.
- Since September 2016 Securosys HSMs protect all SIC and SBX transactions.
- To fulfill this order the company first had to establish the infrastructure and business processes to comply with the requirements put on a permissioned vendor of the Swiss government. This certification was granted in April 2016.
- Secondly the company needed to establish a quality management system according to the norm ISO9001. The corresponding certificate was issued in August 2017.

SWISO

ISO 9001:2015

Securosys SA
CH-8005 Zürich
Qualitätsmanagement Zertifikat
gemäss **ISO 9001:2015**

- The **Primus S500 HSM** was then modified for general application as the Primus X-Series HSM, released in December 2016.
- The **Primus E-Series**, a lower-performance, cost-effective, and software compatible version, was released in May 2017, while the HSM as a service (the Securosys Clouds HSM) went into operation in April 2018.

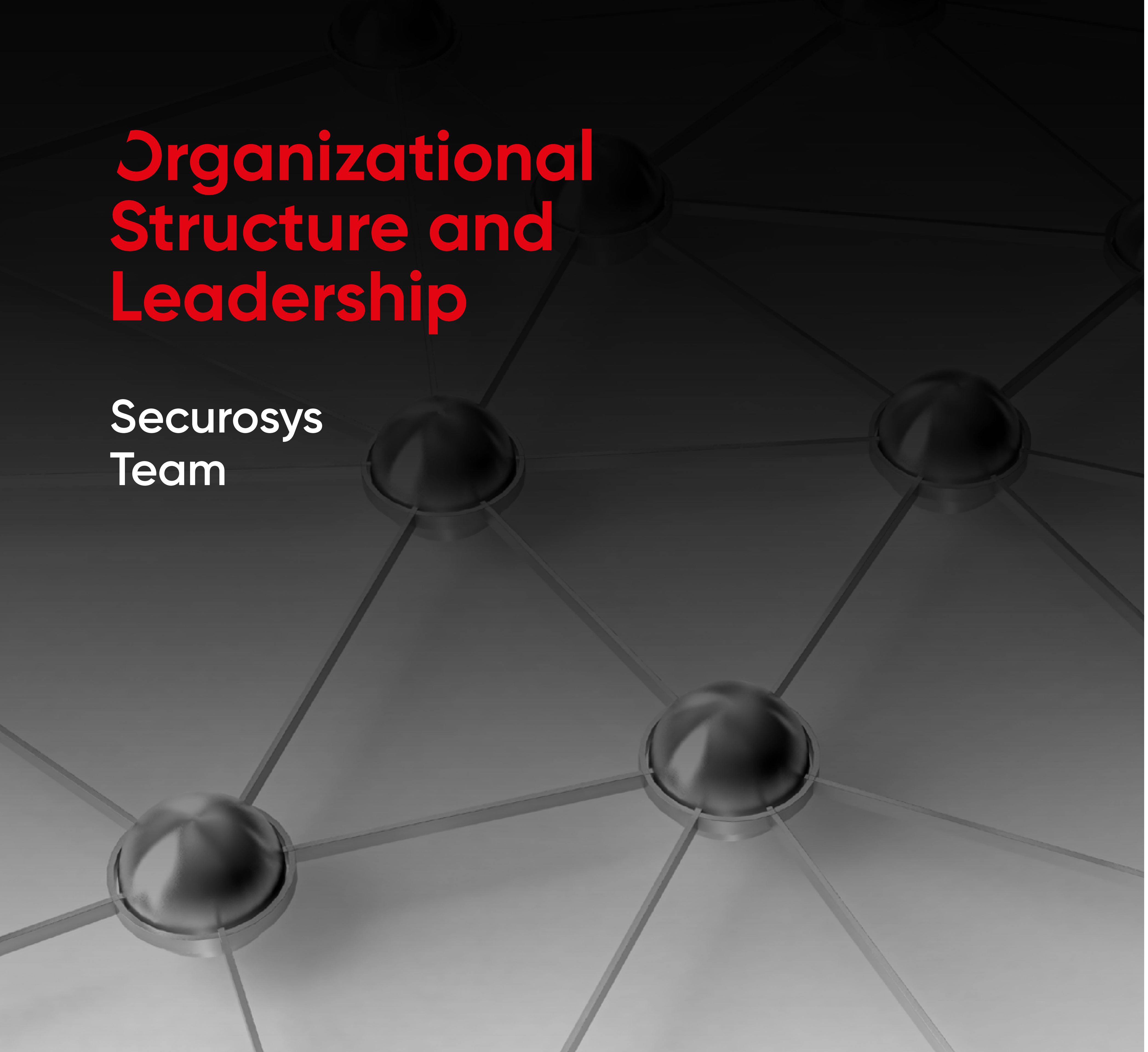
Research Activities

During the development of the Primus S500 Hardware Security Module, the company started its engagement in applied cryptographic research, working together with the University of Applied Sciences of Eastern Switzerland. In the first project, methods to protect against side channel attacks were researched [2], [3].

In the second project, which is still ongoing, important contributions concerning secure implementation of cryptographic algorithms in the post-quantum era are being developed [4].

The Commission also recognized our research effort as a success story for Technology and Innovation CTI (recently renamed to “Innosuisse”) [5].

CTI is the federal agency responsible for encouraging science-based innovation in Switzerland.



Organizational Structure and Leadership

Securosys Team

Securosys strongly believes that trusted encryption systems are the right answer to protect companies’ and individuals’ privacy and assets. Our team has the expert knowledge and competency to deliver, operate, and support the basic structure of such systems. As of today, **Securosys** employs 17 people and 4 in-house contractors in Zurich, Switzerland. The core development team consists of six highly qualified and experienced security hardware and software engineers. We are rapidly expanding our team.

Management

Dr. Robert Rogenmoser

CEO

A 17-year Silicon Valley veteran, has experience in building up companies and products from scratch

LinkedIn Profile

Dr. Andreas Curiger

CTO/CSO

Cryptographic expert with over 20 years of industry experience, manages technology

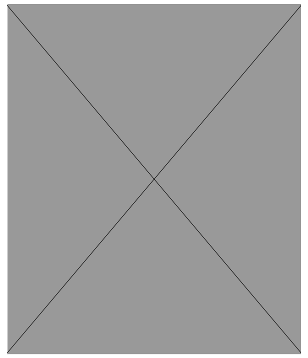
LinkedIn Profile

Marcel Dasen

Head of Engineering

With over 20 years of experience in building embedded products, leads our product development

LinkedIn Profile



Reto Stäuble

Head of Services and Biz Dev

With over 10 years of experience in cryptographic products, leads the Securosys Clouds HSM development

LinkedIn Profile

Christian Willemin

Head of Sales

Leads customer acquisition

LinkedIn Profile

Geraldine Critchely

Head of Marketing

Digital marketing expert with over 15 years experience in product marketing

LinkedIn Profile

Board of Directors

Dr. Andreas Curiger

President of the Board, CTO

Cryptographic expert with over 20 years of industry experience, manages technology

LinkedIn Profile

Dr. Robert Rogenmoser

Member of the Board, CEO

A 17-year Silicon Valley veteran, has experience in building up companies and products from scratch

LinkedIn Profile

Andrea Schlapbach

Member of the board and successful entrepreneur

Contributes valuable operational and financial advice

LinkedIn Profile

Hans-Jörg Bärtschi

Member of the board and financial expert

Contributes valuable financial and strategic advice

LinkedIn Profile

Team

Experienced Software Engineers[7]

form the core of embedded developers for the Securosys HSM extensions and are active in the blockchain community as well

Security Engineers[7]

for the HSM network appliances and Clouds HSM

Rest of the team

Besides management and engineering additional team members cover product management and application engineering, support, marketing and sales, operations including billing and shipping, and office management.

[7] For security reasons, a part of the key team members involved in the development of technical solutions will be kept anonymous in order to mitigate potential security threats.

Suppliers

In addition, we are working with many external partners. This involves experts in embedded system, hardware, and software development for specific parts and subsystems, as well as accounting and legal services.

The production of the HSMs is outsourced to two vested Swiss-based electronic manufacturing service contractors.

enics

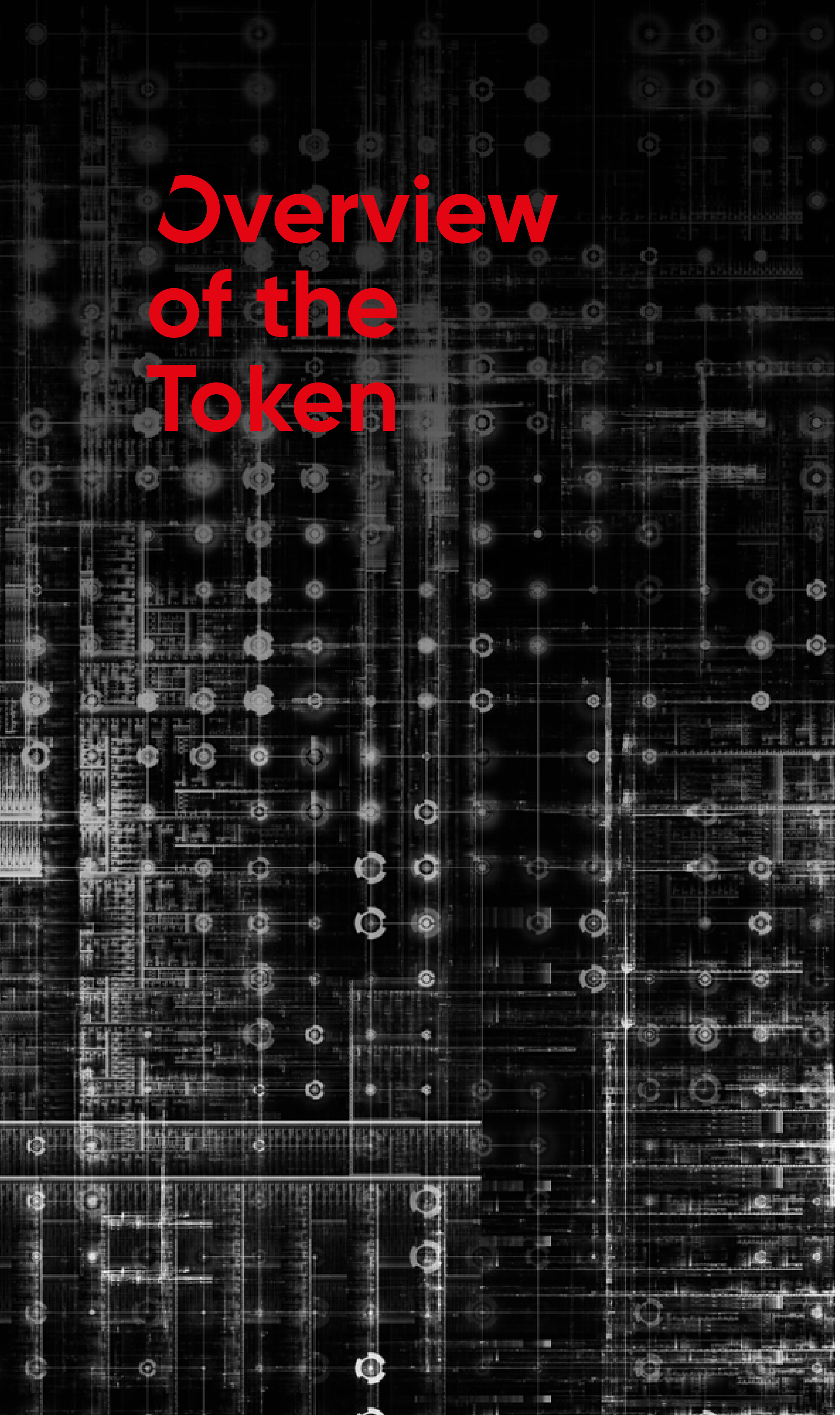
CCS Group

07 /

Token and Token Sale

Synopsis

Securosys will issue the **Securosys Token (SET)** as a security token. The following gives an overview on the Token itself, distribution, profit sharing and investor rights provided by SET Tokens.



Overview of the Token

The Securosys Token (SET) is a security token. The SET Token corresponds to **Securosys** shares. It gives the holders the same proprietary rights as if they would hold the corresponding shares. In particular, holders have a right to an equivalent share of profits made by **Securosys** in accordance with the description below (see “Payment of profit share”).

During the ITO a total of 4’691’300 SET are minted. This corresponds to 25% of the total shares of **Securosys** on a diluted basis (The shares relating to the SET Tokens are not issued until the holder of SET Tokens requests the conversion thereof. Corporate action is in place to facilitate this). This corresponds to 46’913 shares of nominal value of CHF 1.00 (i.e. the arbitrary value assigned for balance sheet purposes, this does not express the share's market value). **Securosys** general assembly authorized to issue these shares on June 12, 2018.

The SET Token holder can request the conversion of their SET Tokens into **Securosys** shares. Packets of 50,000 SET tokens or more will be converted into regular shares, smaller packets will be converted into non-voting shares (participation certificates)[8]. In limited circumstances (e.g. liquidation and exit events), as described in the SET Token Sales Terms, the SET Tokens must be exchanged into **Securosys** shares. The exchange rate therefore is 100 SET to one **Securosys** share of CHF 1.00 nominal value.

[8] https://www.admin.ch/opc/en/classified-compilation/19110009/index.html#a656a

Any exchange requested by a holder will be executed within three months after the reception of the SET Token conversion request and sufficient holder information.

Of the 4,691,300 SET Tokens minted for the ITO, 65% of all SET Tokens (3,049,345 SET) will be offered for sale. 30% of the SET will go into the **Securosys** reserve for future funding and employee compensation. 5% of the SET Tokens will be used to cover the costs of the SET ITO. Any SET Token not sold in the initial sale will be assigned to **Securosys** for later sale.

Token qualities:

- SET Tokens are considered securities under Swiss law
- SET Tokens are planned to be listed on regulated exchanges[9]
- SET Tokens do not confer any voting rights in the company

Overview Summary

Role of the token	SET tokens can be converted into shares. The tokens entitle to an annual dividend-linked participation per token. The conversion rate is 100 tokens to one **Securosys** share of CHF 1.00 nominal value. The dividend-linked participation is a cash payment by **Securosys** in CHF, tokens, or Ether. The amount of participation per token equals 1% of the amount dividend paid per **Securosys** share.
Ticker	SET
Token type	ERC20
Hard Cap	3’049’345 SET Token
Pre-Money Valuation	CHF 49’259’350 (accounting for discounts)
PPT (Price per token)	CHF 5.00

[9] As of today there are no agreements with exchanges in place. Although **Securosys** may list the SET Tokens on several cryptocurrency exchanges, there can be no assurance that such exchanges will accept the listing of SET Tokens or maintain the listing if it is accepted. There can be no assurance that a secondary market will develop or, if a secondary market does develop, that it will provide SET Token holders with liquidity of investment or that it will continue for the life of the SET Tokens.

Payment of Profit Share

Once every year, after receiving the audit report of the last financial year, the **Securosys** board will make a proposal on the amount of dividends to be distributed. Subsequently the general assembly of **Securosys** approves, modifies, or rejects the proposal. The board and the general assembly of **Securosys** will not only take financial results but also the general financial health of the company into account, before allowing the issuance of dividends. In the four years of existence, **Securosys** has not issued any dividends yet.

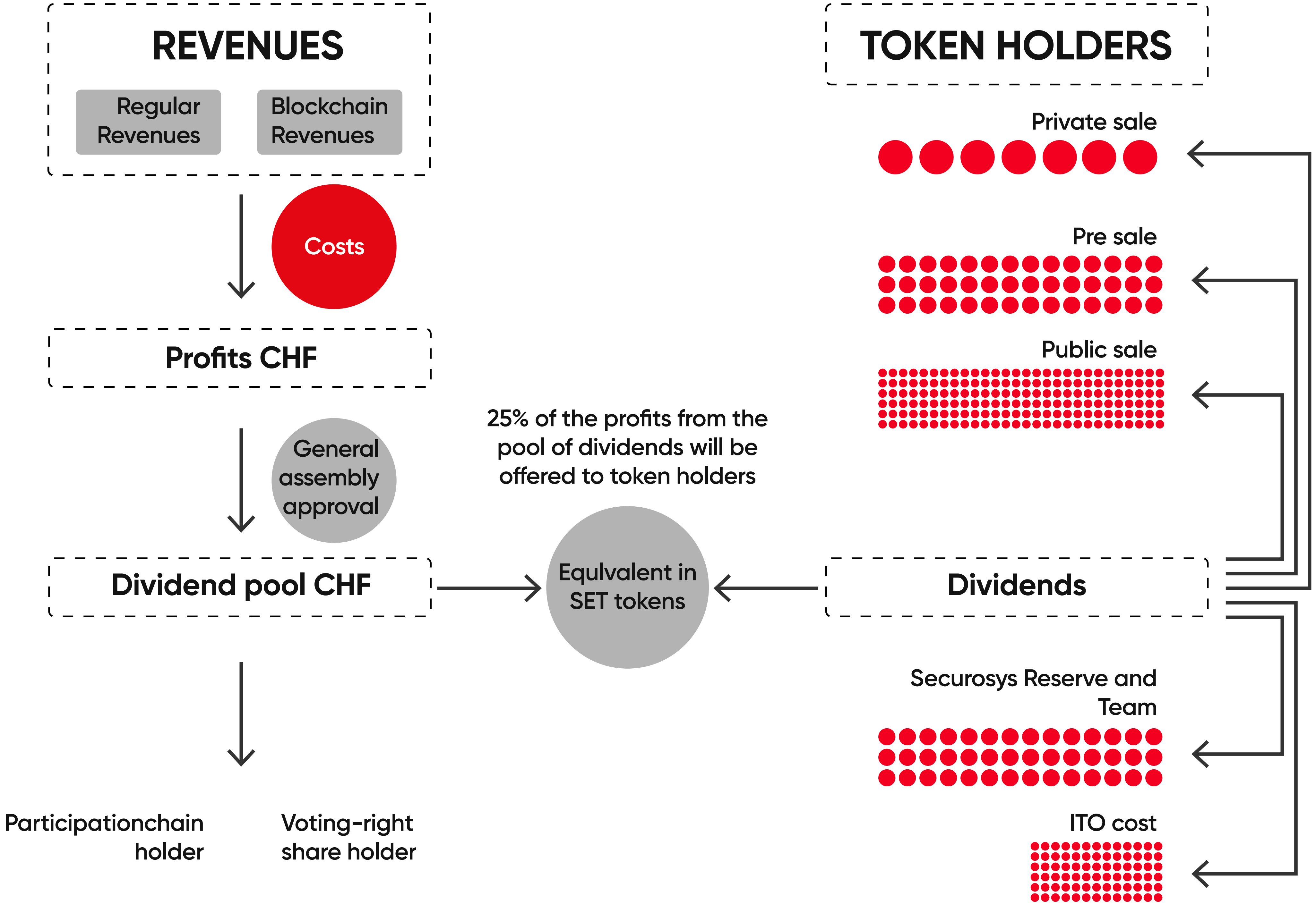
The amount of participation by the SET Token holders will be calculated based on 25% of the total dividend paid to the **Securosys** shareholders (as the total amount of SET Tokens corresponds to 25% of the total shares of **Securosys** on a diluted basis). If any SET Token are converted to shares, the total dividend amount for SET Token will be reduced accordingly. The participation by the SET Token holders can be paid out via smart contract as SET Tokens (if available in the **Securosys** reserve), ETH, or as fiat cash payment in CHF.

The amount of SET Tokens or ETH token will be calculated at the exchange rate (market price) of SET Tokens or ETH on the day, the dividend was approved.. Dividend payments in SET Tokens will come from the **Securosys** reserve or through market buy of SET Tokens. The latter is however upon **Securosys** sole discrection. In the event of the sale of a subsidiary of **Securosys**, the same procedure applies. The full terms of the SET Tokens will be included in the Token Sale Terms, to be published separately on Securosys' offering website, [website].

To receive participation, **SET** Token holders must fulfill the following requirements:

- The token holder has to hold at least 1000 **SET** Tokens at the time of the dividend distribution.
- The **SET** Tokens holder has to be registered (and verified) with **Securosys** for **Securosys** to comply with its KYC requirements and Swiss tax withholding requirements
- Any payment for **SET** Tokens not registered with **Securosys** at the date of the dividend approval or not meeting other conditions above are voided and fall back to the company.

Token Mechanics: Dividend Payments


REVENUES
Regular Revenues
Blockchain Revenues
Costs
Profits CHF
General assembly approval
Dividend pool CHF
Participationchain holder
Voting-right share holder
25% of the profits from the pool of dividends will be offered to token holders
Equlvalent in SET tokens
Dividends
TOKEN HOLDERS
Private sale
Pre sale
Public sale
Securosys Reserve and Team
ITO cost

Token Distribution

Currencies Accepted for SET Tokens Purchases

Fiat and crypto currencies will be accepted as means of payments in the ITO process. Crypto currency payments will be accepted in Ether (ETH) and Bitcoin (BTC). Also fiat currency contributions can be made, assuming we are able to engage a reliable payment service provider (there have been some issues with accepting fiat payments for ITOs in the recent past). Payments can be made through fiat wire transfers. Separate agreements can be signed for the private sale and the pre-sale. Any payment with Ether or Bitcoin will be valued at the exchange rate to CHF at the date of the transfer.

Investor Base

Within the EEA, **Securosys** will rely on prospectus exemptions, offering to less than 150 investors per member state, offering in batches of over EUR 100,000 per investor, or offering to qualified investors only. The full terms of the SET sale will be included in the Token and Token Sale Terms, to be published separately on Securosys' website, www.securosys.swiss.

For other jurisdictions **Securosys** will rely on a general representation from the investor that no securities laws and other laws are violated by the purchase of tokens/shares by the respective investor.

The SET will be offered worldwide, with the exception of the United States, Canada, China, Japan, Australia, North Korea, South Korea, Iran, Myanmar, Afghanistan, Angola, Aruba, Bangladesh, Belarus, Benin, Bhutan, Bolivia, Botswana, Brunei Darussalam, Burkina Faso, Bosnia, Burundi, Cambodia, Cameroon, Cape Verde, Central Africa republic, Chad, Comorros, Congo, Congo Democratic republic, Cuba, Cote d'Ivoire, Djibouti, Dominica, Ecuador, El Salvador, Equatorial Guinea, Eritrea, Ethiopia, Gabon, Gambia, Ghana, Guatemala, Guyana, Guinea, Guinea Bissau, Haiti, Honduras, Iraq, Jordan, Kenya, Kyrgyz Republic, Laos People's Republic, Lesotho, Liberia, Libya, Madagascar, Malawi, Malaysia, Mali, Mauritania, Micronesia, Moldova, Mongolia, Mozambique, Nauru, Nepal, New Caledonia, Nicaragua, Niger, Nigeria, Niue, Oman, Pakistan, Palestinian Areas, Papua New Guinea, Reunion, Rwanda, Samoa, Sao Tome and Principe, Senegal, Sierra Leone, Somalia, South Georgia, Sudan, Sri Lanka, Suriname, Syria, Swaziland, Tajikistan, Tanzania, Timor, Togo, Tonga, Tunisia, Turkmenistan, Uganda, Uzbekistan, Venezuela, Western Sahara, Yemen, Zambia, Zimbabwe or any jurisdiction into which the same would be unlawful.

Lockup Periods Will Be Set Accordingly to the Investment Ticket

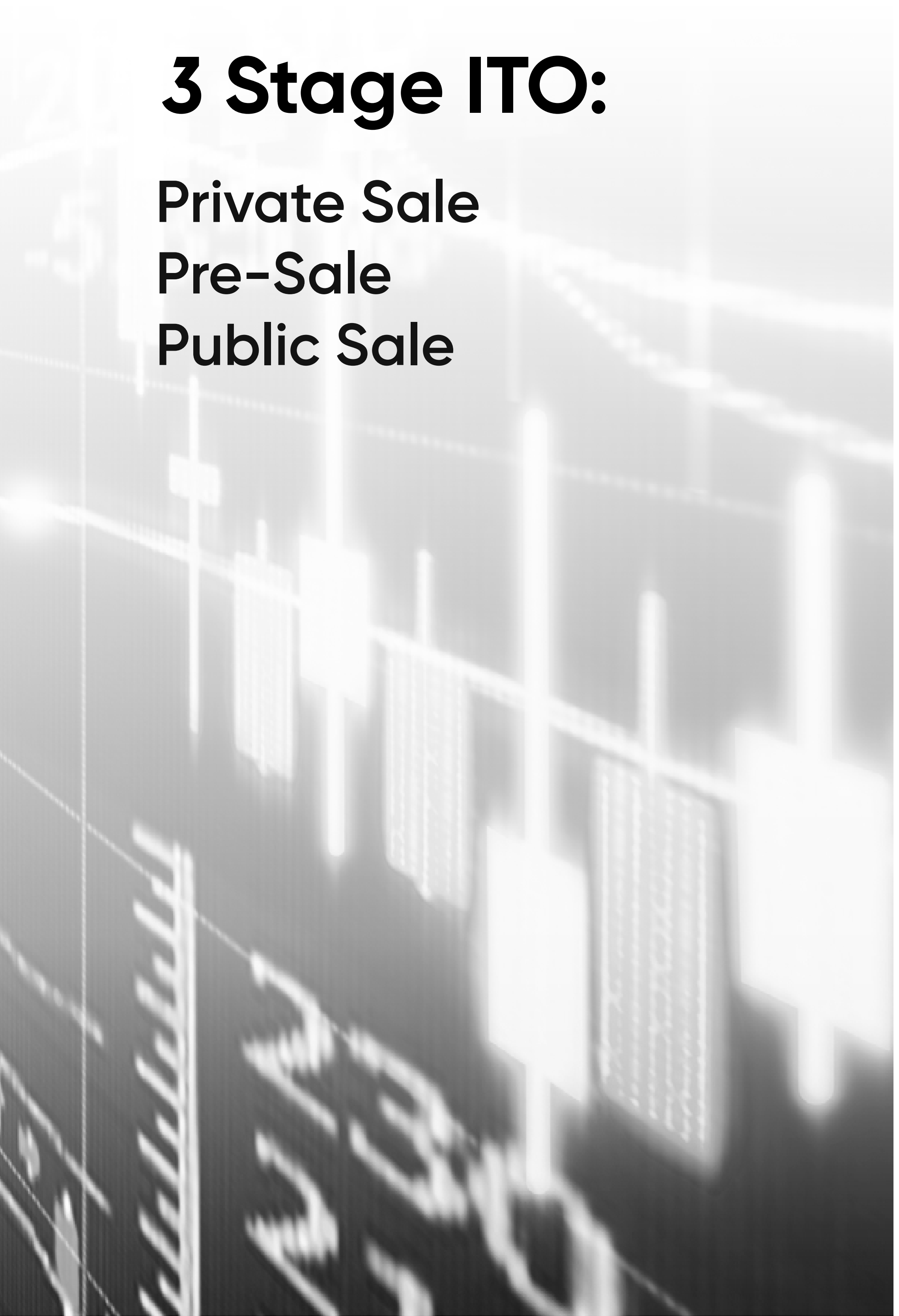
Depending on the type of investment, the lockup periods differ. The Tokens in the **Securosys** reserve will be locked-up for 24 months from the ITO date before they can be sold. The Tokens held by investors will be locked depending on the investment tickets. For the private sale investors, the lockup period will be 6 months, for the pre-sale the lockup period will be 3 months, while for the public sale investors there will be no lockup period.

The Token Distribution Will Be Spread Across Public Sale, Reserve, Employees, Operating Expenses, ITO Costs

From the total amount of SET Tokens 65% will go to the private, pre-sale and public sale. 22% will be allocated in the reserve, 8% will be used to incentivize employees and 5% will be reserved to cover ITO costs. The SET Token distribution looks as follows:

The following SET Token distribution is planned:

	Percentage of tokens	Lockup period	Comments
ITO	65% of total tokens	0, 3, 6 months	Depending on the investment size.
Securosys Reserve	22% of total tokens	24 months	Used for payment of dividends, for future fund raising, for strategic partnerships.
Securosys Employees	8% of total tokens	—	Distributed over 3 years.
ITO costs	5% of total tokens	—	Other PR, Marketing, Operational costs for ITO. If not fully used, will go to Securosys reserve.



3 Stage ITO:

Private Sale
Pre-Sale
Public Sale

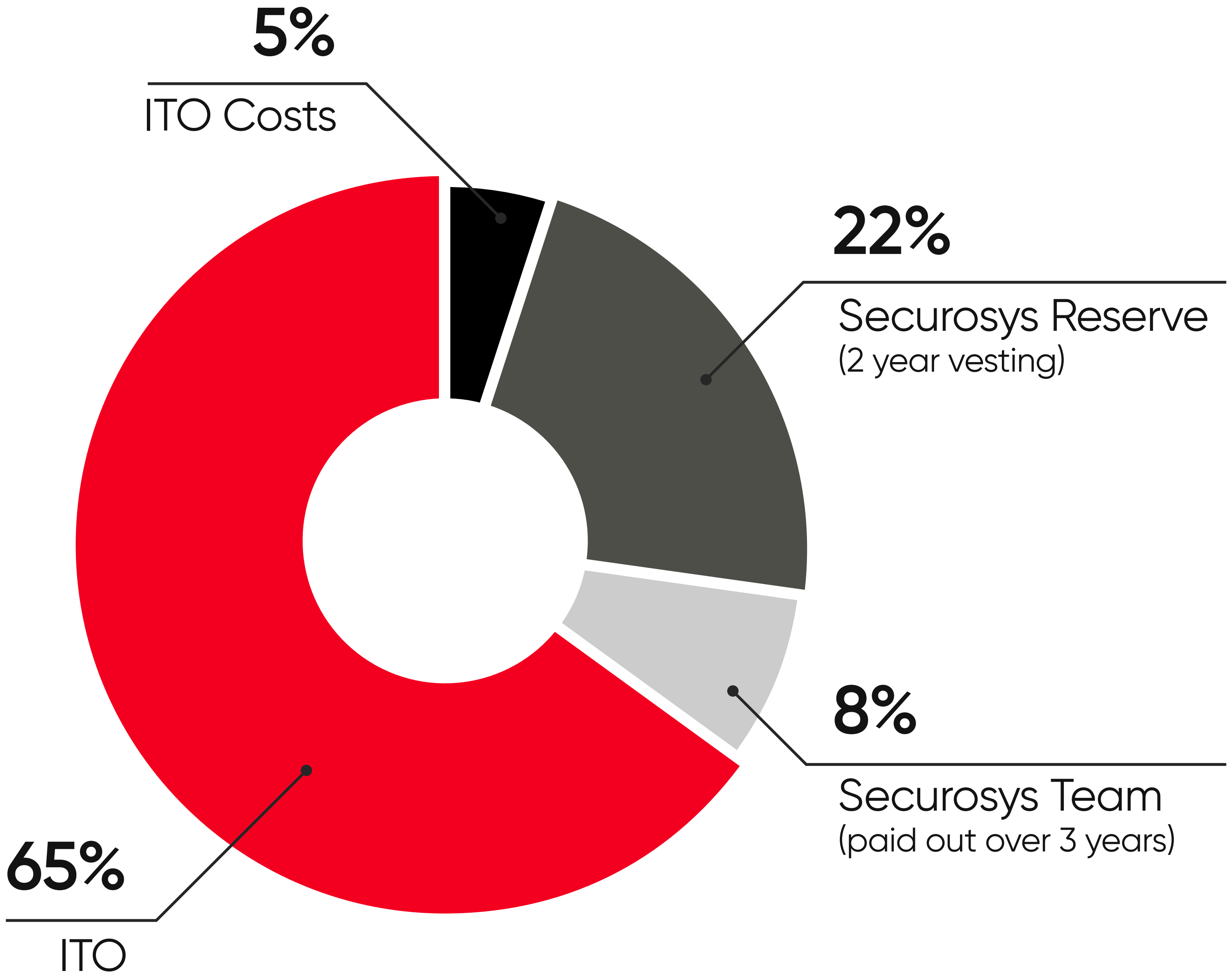
		Discount	Ticket size	Lockup period
Private sale[10]		30%	CHF 1 Mio. +	6 months
		25%	CHF 0.5 Mio. – CHF 1 Mio.	
Pre-sale	Stage 1	20%	CHF 50k – CHF 500k	3 months
	Stage 2	15%		
	Stage 3	10%		
Crowd sale	Stage 1	15%	CHF 5k – CHF 50k	-
	Stage 2	10%	CHF 1k – CHF 50k	
	Stage 3	0%		

We will have a private sale, pre-sale, and an open sale for investors registered with **Securosys**. During the token distribution 65% of the total number of SET Tokens will be sold in three steps that vary by the amount of investment and by the discount offered:

Target Schedule[11]	Begin	End
Stage 1	06.11.2018	27.11.2018
Stage 2	28.11.2018	07.12.2018
Stage 3	08.12.2018	14.12.2018

[10] Private Sale ongoing until end of Token Sale

[11] Schedule may move by a few days



Registration

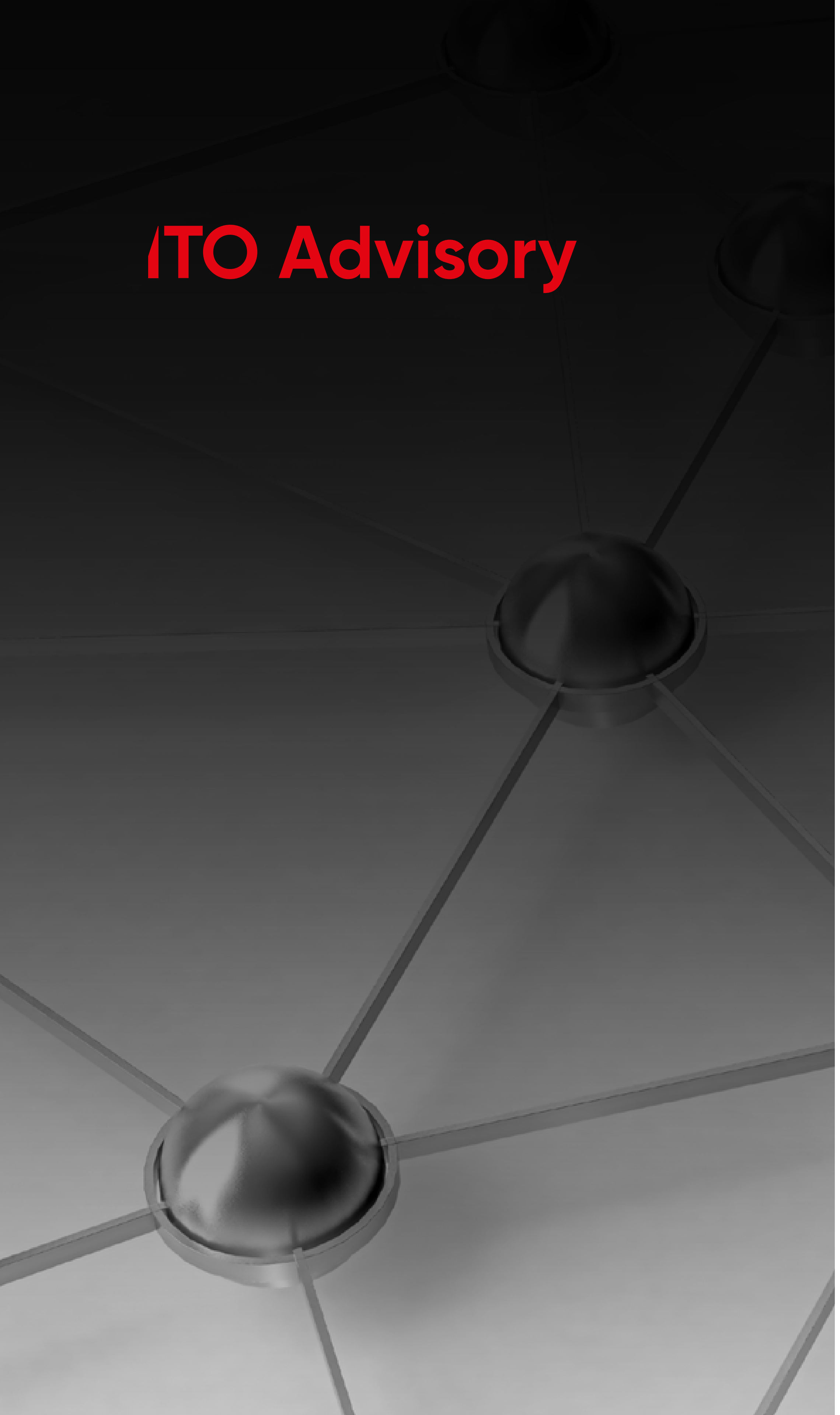
To participate in the SET Token sale, the investors have to register for whitelisting and commit the amount of money they would like to contribute in the sale. The investor can participate in the sale after having received a written confirmation from **Securosys**.

Securosys reserves the right to offer special conditions to very large investors (over CHF 1.5 Mio.).

08

/ MTO Advisory

ITO Advisory



Michael Guzik

ITO Advisor

Blockchain Valley Ventures (BVV)

LinkedIn Profile

Ronald Kogens

Legal & Regulatory Counsel

Froriep Legal Ltd.

LinkedIn Profile

Yannick Zehnder

ITO Advisor for Community Building and Management and Investor Relations

LinkedIn Profile

Bibliography

[1] Graz University of Technology, “Meltdown and Spectre – Vulnerabilities in modern computers leak paswords and sensitive data.” https://meltdownattack.com/.

[2] Dorian Amiet, Andreas Curiger, and Paul Zbinden. “Flexible FPGA-Based Architectures for Curve Point Multiplication over GF(p).” In 2016 Euromicro Conference on Digital System Design, DSD 2016, pages 107–114. IEEE Computer Society, 2016.

[3] Roman Willi, Andreas Curiger, and Paul Zbinden, “On Power-Analysis Resistant Hardware Implementations of ECC-Based Cryptosystems.” In 2016 Euromicro Conference on Digital System Design, DSD 2016, pages 665-669. IEEE Computer Society, 2016.

[4] Dorian Amiet, Andreas Curiger, and Paul Zbinden. “FPGA-based Accelerator for Post-Quantum Signature Scheme SPHINCS-256,” https://tches.iacr.org/index.php/TCHES/article/view/831. Accepted for publication at the IACR Conference on Cryptographic Hardware and Embedded Systems (CHES) 2018, Amsterdam, The Netherlands, September 9–12, 2018.

[5] Commission for Technology and Innovation. “Hack um Hack zu mehr Sicherheit im Zahlungsverkehr.” https://www.kti.admin.ch/dam/kti/de/dokumente/ErfolgsgeschichtenundPublikationen/SuccessStories/SuccessStories_FuE/Erfolgsgeschichte FuE Securosys.pdf.download.pdf/Success_Story_F&E_Securosys_dt_170720_lowres.pdf, July 2017.

[6] Andrew Norry, “The Hinstory of the Mt Gox Hack: Bitcoin’s Biggest Heist,” Nov 29, 2017, https://blockonomi.com/mt-gox-hack/.

[7] Yuji Nakamura and Hideki Sagiike, “The $500 Million Heist Hit High-Minded Cryptocurrency: Quick Take.” Feb 1, 2018, https://www.bloomberg.com/news/articles/2018-02-01/hackers-in-500-million-heist-targeted-obscure-cryptocurrency.

[8] The Element Group, “Next Year in Crypto – 11 predictions for 2018,”, Dec 30, 2017, https://hackernoon.com/next-year-in-crypto-11-predictions-for-2018-7ac0e87cf18.

IMPORTANT INFORMATION

Nothing in this White Paper shall be construed as an offer to sell or buy securities in any jurisdiction, or a solicitation for investment, or an investment advice. The White Paper does not regulate any sale and purchase of SET Tokens (as referred to in the White Paper). The purchase of SET Tokens (or "Tokens") is subject to the Token Sale Terms and Conditions.

This White Paper describes the current operation of Securosys SA's existing business and its development intentions. While Securosys SA intends to attempt to realize the next development steps, please recognize that such intention is dependent on quite a number of factors and subject to quite a number of risks. It is entirely possible that the realization of the intentions as set forth in this White Paper will be impossible, or that only a portion thereof will be realized, or that the intentions will not gain as much as attention as expected. Securosys SA will try to update its community as things grow and change, but undertake no obligation to do so. Becoming a leading company for secure enterprise-grade key management for crypto assets and blockchain systems is a very ambitious undertaking that may never succeed.

Securosys SA do not guarantees or warrant any of the statements in this White Paper regarding the future outlook of its business, because it is based on its current beliefs, expectations and assumptions, about which there can be no assurance due to various anticipated and unanticipated events that may occur.

SET Tokens represent blockchain-technology based convertible dividend-linked share rights. The tokens can be converted into company shares. The tokens entitle to an annual dividend-linked participation per token. This dividend-linked participation is a cash payment by Securosys in CHF, tokens, or Ether. The amount of participation per token equals 1% of the amount dividend paid per Securosys share. The dividend for one year, if any at all, must be approved by Securosys'

! This White Paper is provided by Securosys SA (**"Securosys"**)
for informational purposes only.

shareholders meeting held in that year for the past business year. The conversion rate is 100 tokens to one Securosys non-voting share (participation share) of CHF 1.00 nominal value. The full details are listed in the section Overview of the Token.

Blockchain-technology is in its infancy and will be subject to many challenges, competition and a changing environment. Due to the retrospective nature of regulatory action or guidance, we can make no guarantees regarding the legality of the SET-Token and the SET-Token launch in any given jurisdiction. SET-Tokens may not be available in certain countries. SET-Tokens are non-refundable and are not for speculative investment. No promises of future performance or value are or will be made with respect to SET-Tokens, including no promise of inherent value, no promise of continuing payments, and no guarantee that SET-Tokens will hold any particular value.

This White Paper may be updated or altered, with the latest version of the White Paper prevailing over previous versions and we are not obliged to give you any notice of the fact or content of any changes. The latest version of the White Paper in English is available at the website https://www.securosys.swiss/whitepaper. While we make every effort to ensure that all data submitted in the White Paper is accurate and up to date at the point in time that the relevant version has been disseminated, the proposed White Paper is no alternative to consulting an independent 3rd party opinion.

The White Paper does not constitute an agreement that binds Securosys SA. Securosys SA, it's directors, officers, employees and associates do not warrant or assume any legal liability arising out of or related to the accuracy, reliability, or completeness of any material contained in the White Paper. To the fullest extent permitted by any applicable law in any jurisdiction, Securosys SA disclaim all liability to you and everyone else in respect of the content of this White Paper, whether under any theory of tort, contract or otherwise and whether in respect of direct, indirect, consequential, special, punitive or similar damages. Persons who intend to purchase SET-Tokens, should seek the advice of independent experts before committing to any action, set out in the White Paper.

! This White Paper is provided by Securosys SA (**"Securosys"**) for informational purposes only.

securosys

Securosys SA, Förrlibuckstrasse 70
CH-8005 Zürich
Switzerland

securosys.ch
cloudshsm.com
www.securosys.swiss

ico@securosys.ch

Member of

ISSS Information Security Society Switzerland

Information Security Society

Switzerland (ISSS) www.isss.ch

SWISS FINANCE STARTUPS

Swiss Finance Startups

https://swissfinancestartups.com/

Crypto Valley Member

Crypto Valley Association

https://cryptovalley.swiss/