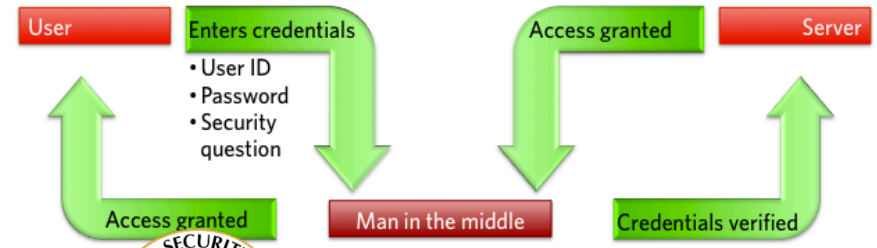
securosys

Data Governance Event

Geneva

February 6, 2018

Motivation



Motivation GDPR – Article 32

(1) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(2) In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

(3) Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

(4) The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

- Words are important
- Measures must evolve over time
- Combination of
  - Technical measures
  - Organizational measures
- Encryption is the only technical measure mentioned in the law

Encryption is not enough

- Encryption is paramount to protect your data and your customer
- Encryption is only half of the solution – you also need to protect your keys
  - Don’t leave them on the table
  - Only use good keys (and passwords)
- Moreover, you also want to have authentication!

Agenda

- Motivation
- What is a HSM?
- Use cases
  - GDPR
  - Microsoft
  - Crypto Assets
- Why Securosys

HSM
Hardware Security Module
—
Digital Key Vault

What is an HSM?

- HSM: Hardware Security Module
  - Secure generation of cryptographic keys
  - Central and secure storage of cryptographic keys
  - Controlled and regulated access to keys
  - Cryptographic algorithms
  - Tamper proof – fail safe system

- Secret (private) encryption keys are only in the HSM

Importance of good encryption keys

- Encryption keys are an easy way for backdoors
  - User cannot verify that a 256 bit key has only 40 bits of randomness
- Generation of encryption keys is of utmost importance
  - Software is deterministic and cannot generate good encryption keys
  - True random number generators are required
    - Physical noise sources like thermal noise or diode noise
    - Quantum noise sources (superset of above)
  - Guardrails to ensure proper random bit generation
    - A very cold thermal noise source is not that random anymore
- Backdoor examples:
  - RSA Security random number generator Dual_EC_DRBG
  - Random number generators inside Intel CPUs
  - Fast Prime in Infineon Smart Cards

How to connect to a HSM: Application Examples (API)

ORACLE DATABASE

transparent database encryption (TDE)

PKCS#11

API to cryptographic tokens

Microsoft

Certificate Authority

Windows Server 2012 R2

CNG

Cryptographic Next Generation

Cloud Service

CLOUD ACCESS SECURITY BROKER

JCE

Java Cryptographic Extension

Securosys Primus HSM

Primus - The Swiss HSM

- Tamper proof keystore
- Tamper resistant 19" box
- Hardware true random number generators
- Redundant, hot-pluggable power supplies
- Grouping for load balancing & failover
- JCE/JCA, PKCS#11, MS CNG Interfaces
- Configuration, monitoring, logging, firmware & software updates
- Secure transport and storage (3 years)
- Multiple-partitions/users (100+)
- Large key/certificate storage (1M+)
- Secure from Spectre and Meltdown

Long term maintenance and support

Supported Algorithms:

- RSA 2048-8192
- Diffie-Hellman
- ECDSA 256,512
- SHA-2, SHA-3
- AES 128, 256
- Camellia

Use Cases:
GDPR
Microsoft
Crypto Assets

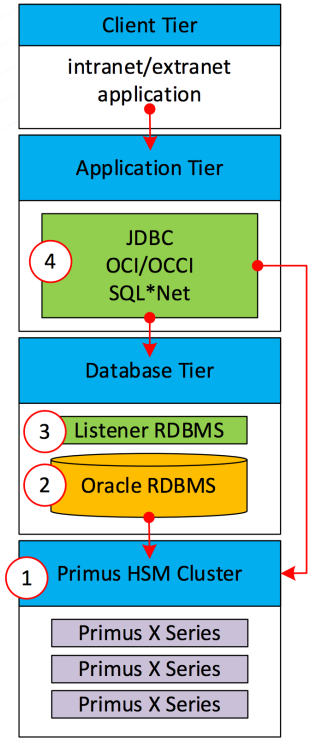
GDPR: Where is my data? How can I encrypt it?

- Customer data on-site:
  - Spreadsheets (Excel, etc.)
  - Databases (Oracle, MS SQL, mysql, etc.)

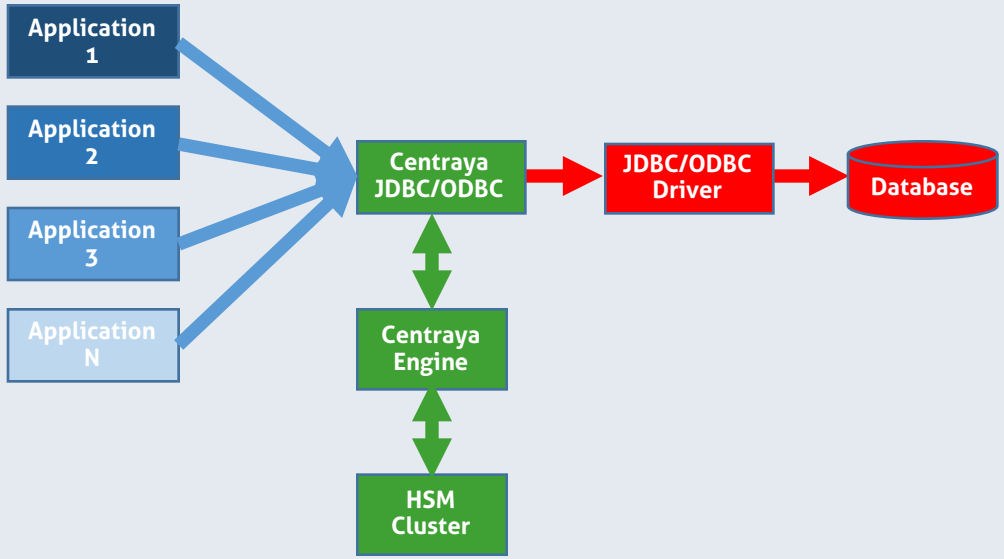
- Customer data in the cloud:
  - Dropbox, Box, etc.
  - Salesforce, Sage, etc.
  - Office365
  - Etc.

Database Encryption

- Option 1 (Oracle, MS SQL): TDE
  - Transparent Database Encryption with keystore

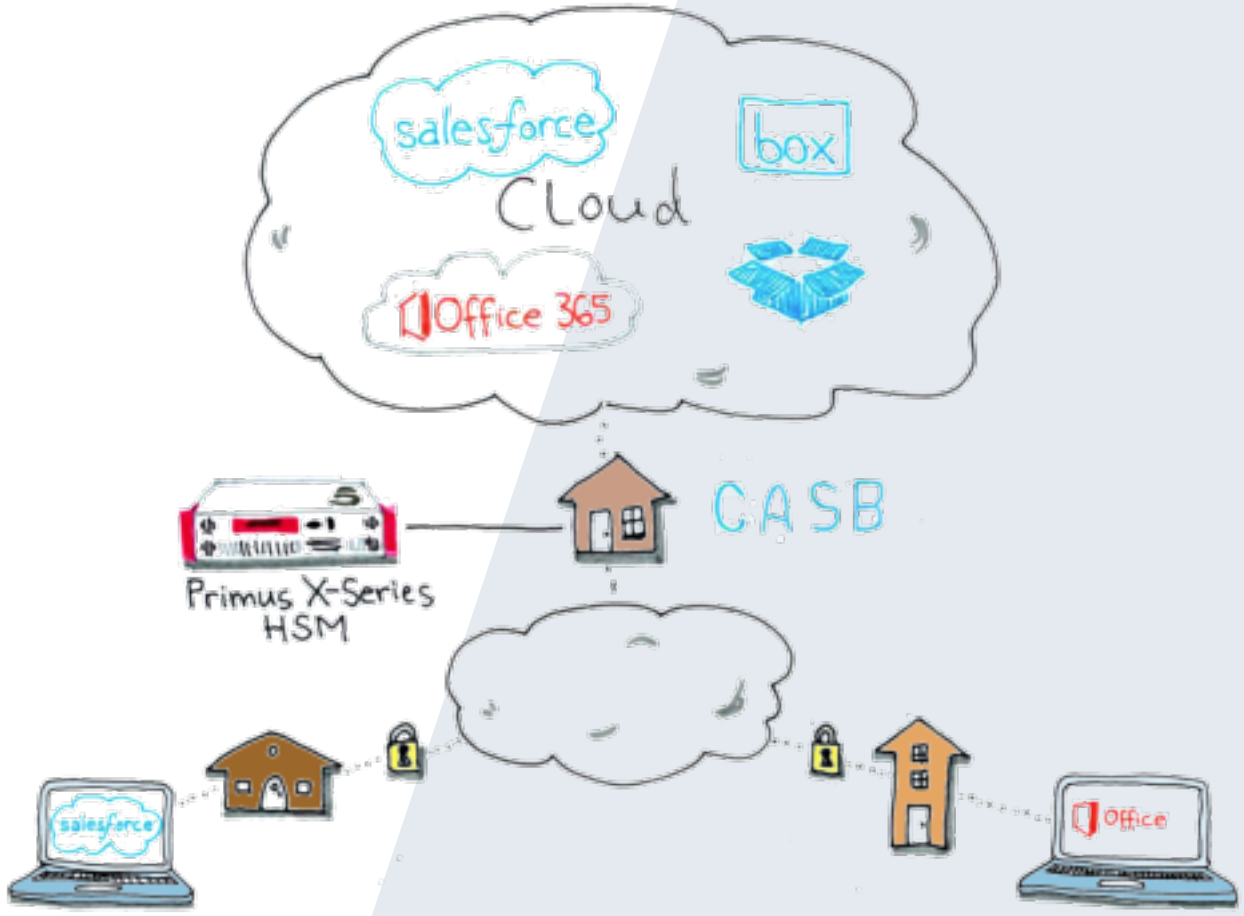


- Option 2 (any DB): jdbc, odbc wrapper with keystore



Cloud Encryption: CASB

- CASB: Cloud Access Security Broker (e.g. from ELCA)

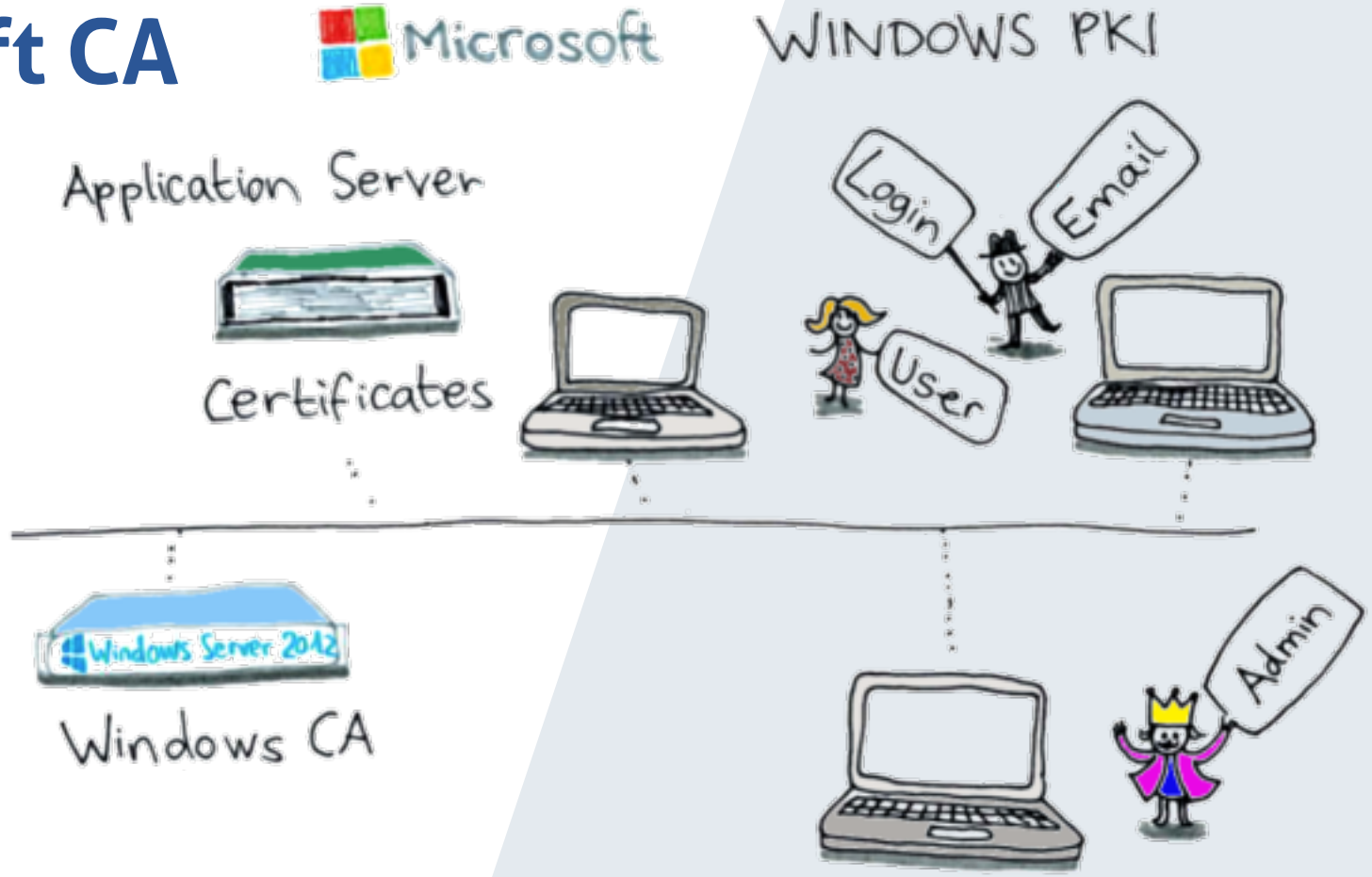


What is the benefit of using HSM?

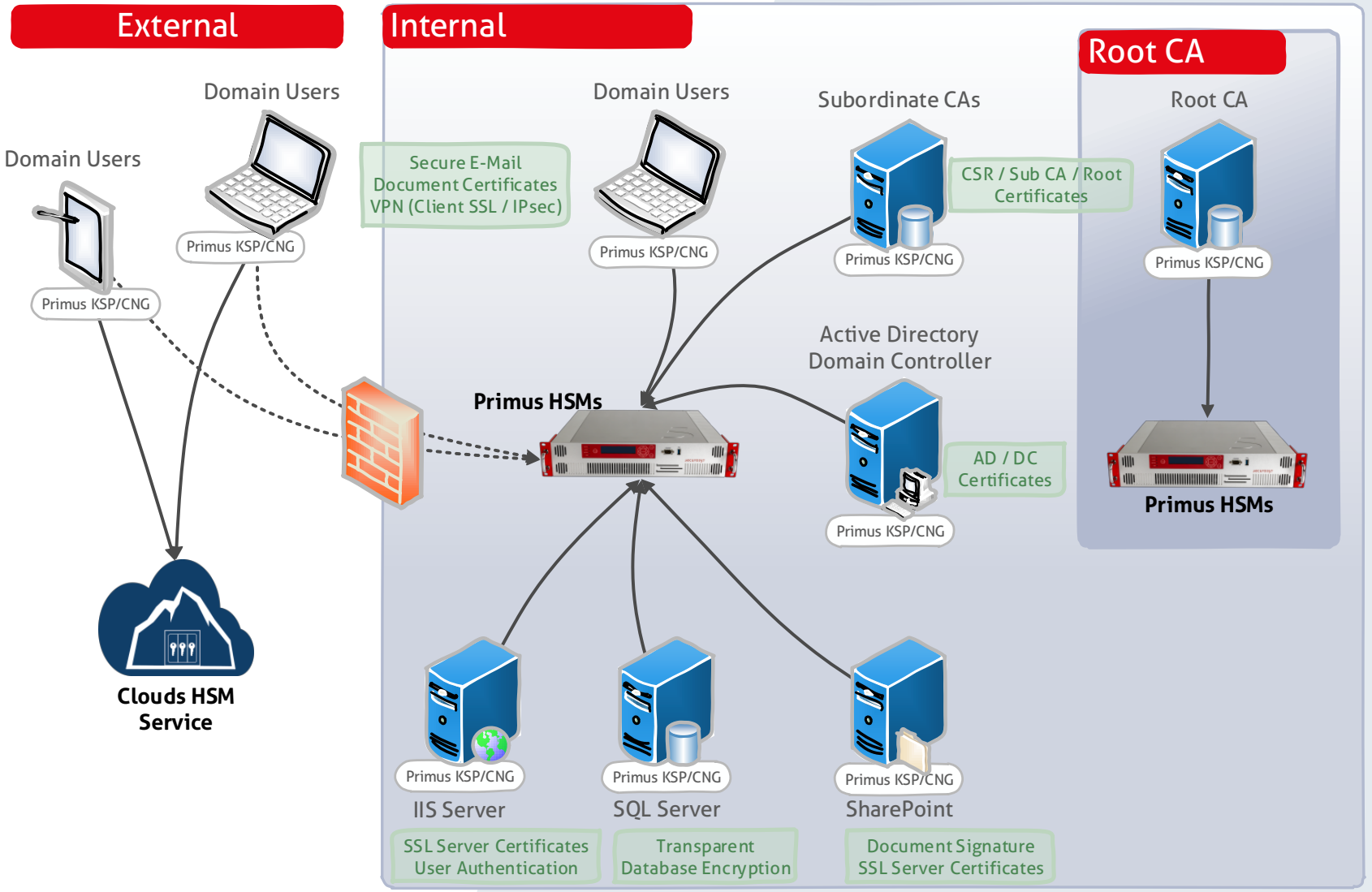
- Protect your customer data
  - If database is stolen, it is encrypted
  - Key is only in HSM
- Right to forget
  - Customer data can be erased by removing customer key in one place, from HSM
- Duty to inform on a breach
  - An infected laptop has only an encrypted version of the data
  - Access to the keys can be removed
- Setup and enforce policies and mechanisms

Microsoft Windows Server

Microsoft CA

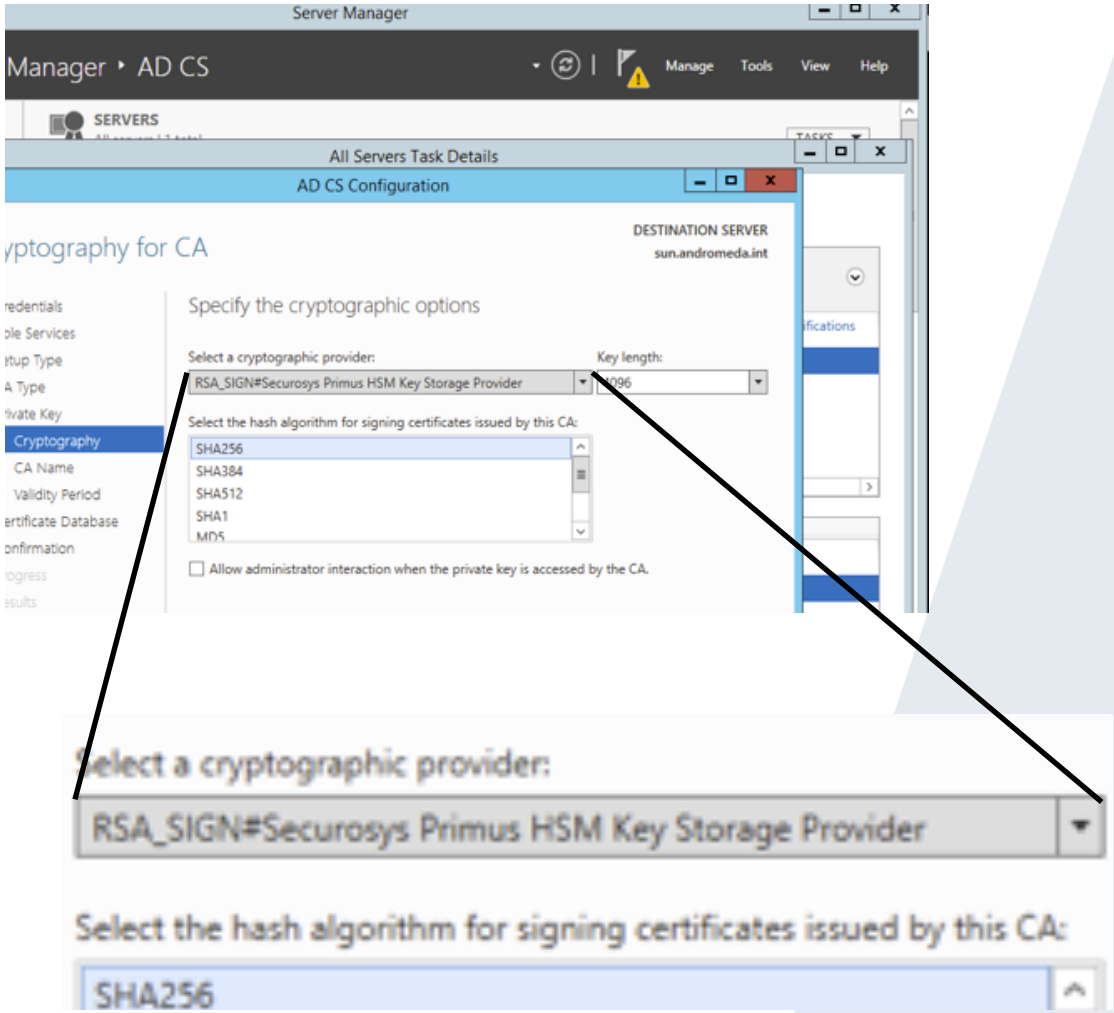


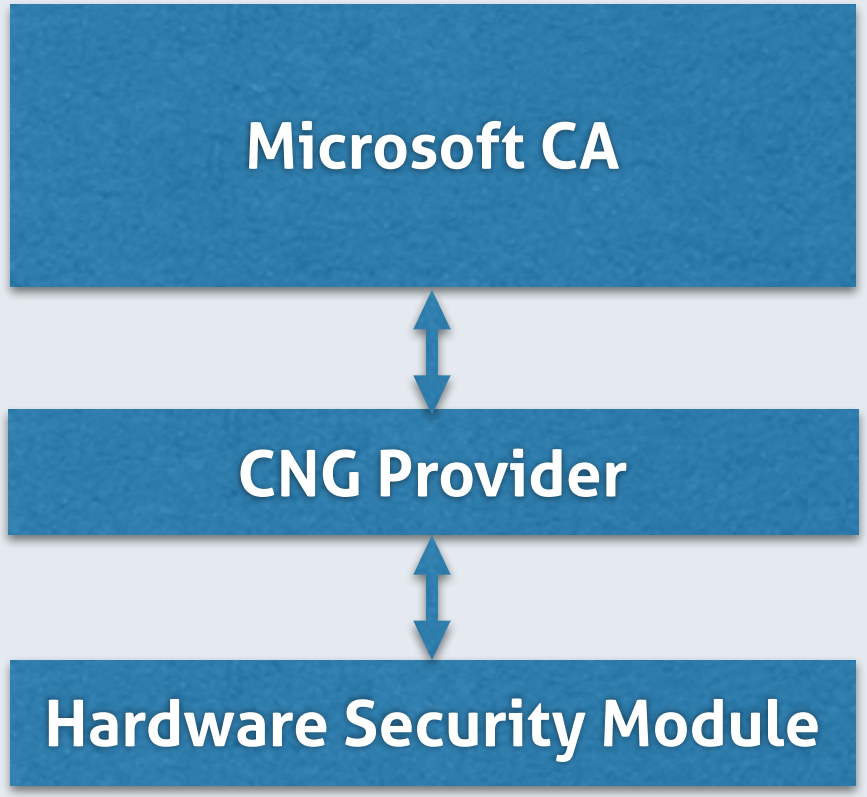
Integration with Microsoft – Complete Solution



Microsoft Partner

MS Certificate Authority (CA)



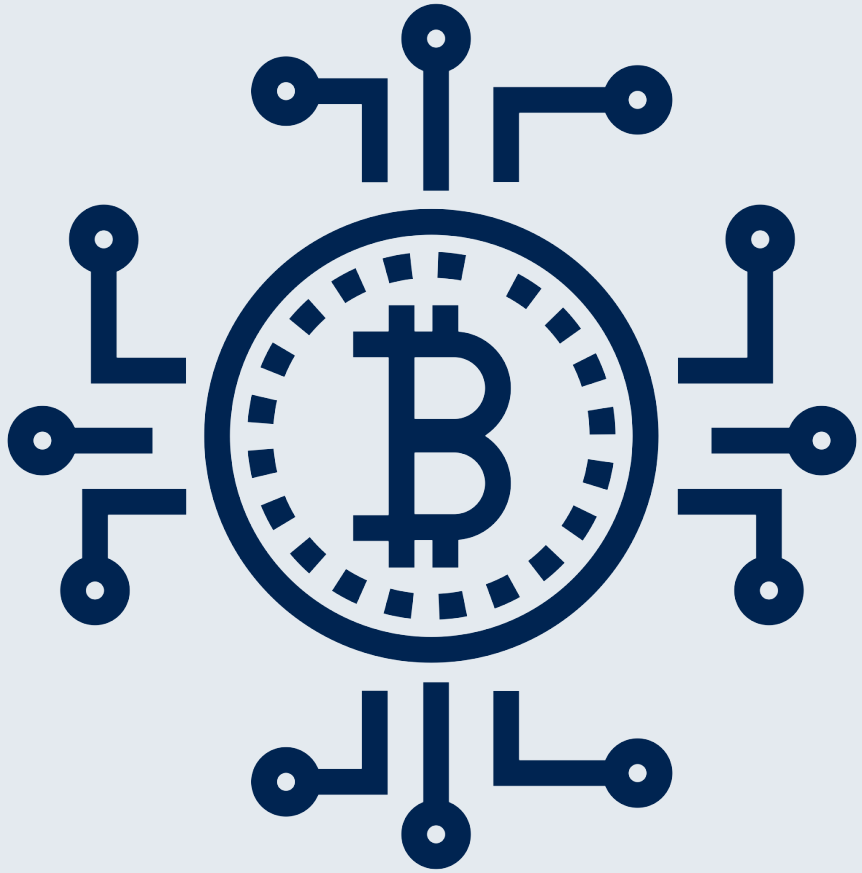


Crypto Finance – Digital Currency – Blockchain

- Crypto currencies are build on cryptography
- The private key corresponds to your money
- Cold storage: Offline storage of crypto assets (savings account)
  - Paper printout
  - USB key

- Enterprise solution for institutional investors (banks, funds, etc.):

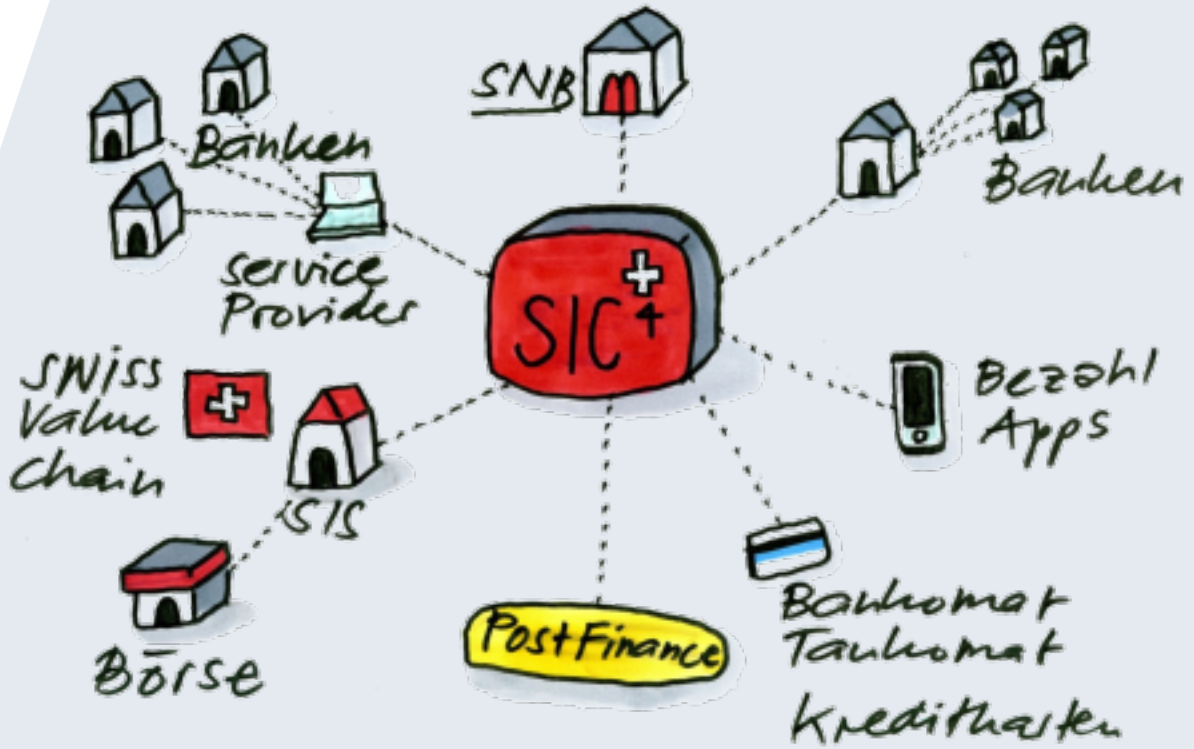
  => Cluster of HSMs



Why Securosys?

Reference

- Securosys HSM protect the Swiss Banking Place (SIC and SECOM)
  - Over 100 Billion Swiss Francs per day
  - Up to 700 transactions per second
  - 10 year maintenance & support agreement



Trustworthy.

- Modern Product-Platform
  - "Military grade security"
  - Designed for Enterprise Customers
  - Industry-Standard Algorithms
- Developed and produced in Switzerland
  - Trustworthy supply chain
  - Independent and neutral
  - No backdoors
- Company Information
  - Founded early 2014
  - Ownership: Founders and independent Swiss investors
  - Headquarters in Zürich, Switzerland

HSM for any Requirements

RSA 4096 per second (log scale)

1000
500
200
100
50


Primus X1000


Primus EP700 (**)


Primus X700


Primus X400


Primus S500 (*)


Primus X200


Primus E150


Primus E60


Primus E20


CloudsHSM-ECO

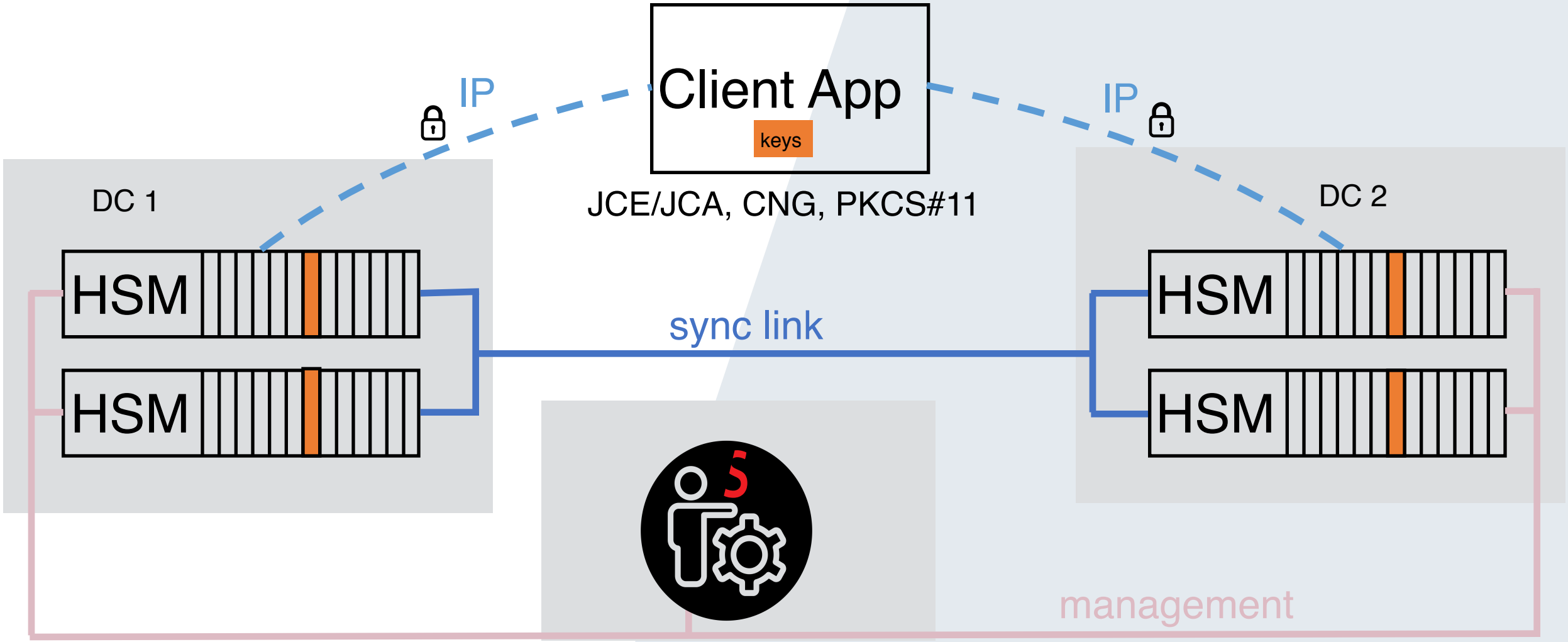

CloudsHSM-ES

(*) Primus S500: SIC and SECOM only
(**) Primus EP700: Securosys Clouds HSM only

Securosys Clouds HSM Overview

- Geo-redundant datacenters
- Tier-1 Internet connectivity
- Dual-homed Internet connection
- ISO27001-certified datacenters
- Swiss DC locations
- Administered by Securosys Experts
- Up to 4-way redundant key storage
- Highly secure Primus HSM (FIPS-140-2 Level 3 conform)
- AES256 protected connection between business App - HSM

Clouds HSM Detail-Architecture



Conclusions

- Protection of your data and your customer
  - Solutions for Databases, Cloud, Microsoft, etc.
  - Partner-Network with Swiss integrators and providers
- Encryption is the first half of the solution
- Key management is the second half of the solution
  - Generation of keys
  - Access to the keys
- HSM is paramount to protect your keys
  - Securosys HSM are developed and produced (operated) in Switzerland
  - Trusted supplier – free of contaminating influences

Q&A