OpenSSL 2025

Beyond the Filesystem:

A Robust Approach to Key Storage

Marcel Dasen | Executive VP Engineering | Securosys

About the speaker

VP Engineering Securosys SA

Swiss manufacturer for cryptographic security appliances (HSM).

Responsibilities:

Head of Software, Hardware and chip design, Product compliance and safety.

Security certifications of products: FIPS 140-3 and Common Criteria,

Background:

MS in computer science and engineering from ETH Zürich

Securing the Cloud Operation Paradigm

CI / CD Pipeline

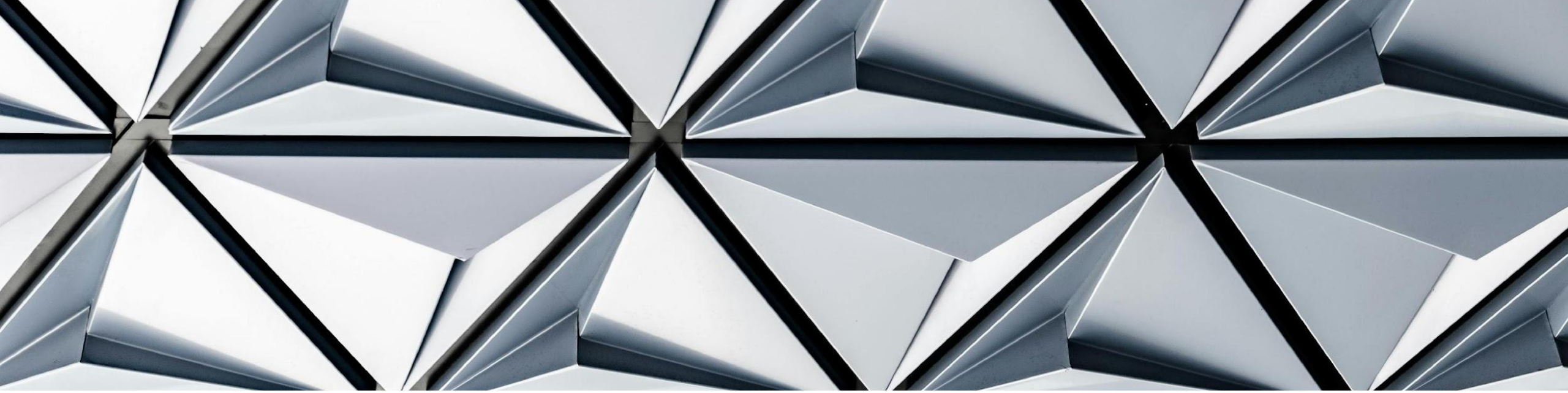
- Continuous improvement
- Continuous deployment (in-situ)
- Deployment in containers (docker)

Containerisation

- Service deployment and scalability with containers
- Microservices: One service per instance / user

Service / API orientation

- Functionality is consumed as a service (IaS, PaaS, SaaS)
- Hybrid operation: On-prem and cloud workload / services work together



01/ Cryptography - why?

Cryptography Key Drivers in IT

Compliance

- GDPR
- Industry regulation: Health, Finance, Payment
- Qualified signature

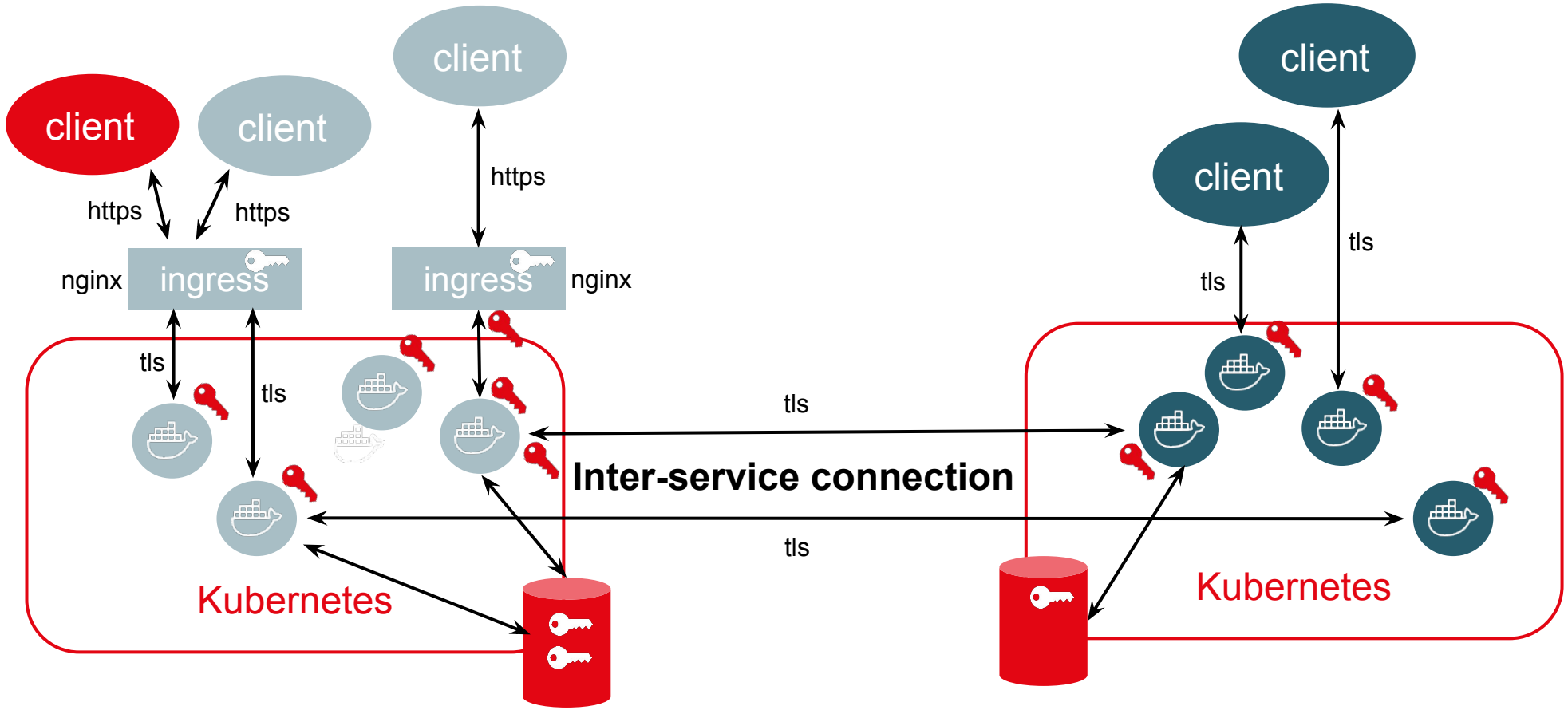
Privacy

- Confidentiality
- IP Protection
- Network encryption (TLS, VPN)
- Blockchain

Cyber Protection

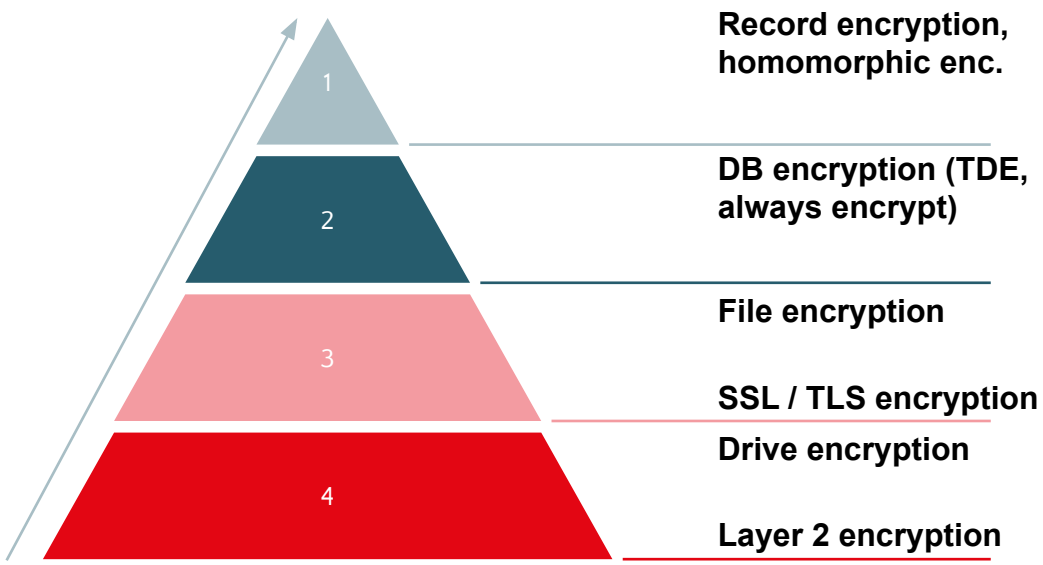
- Encryption to prevent data breaches and theft (data a rest, DB column & TDE, drive, cloud data, DKE)
- Access control (Oauth, JWT)
- Verifiable authenticity (sMIME, document signing)

Encryption is Everywhere



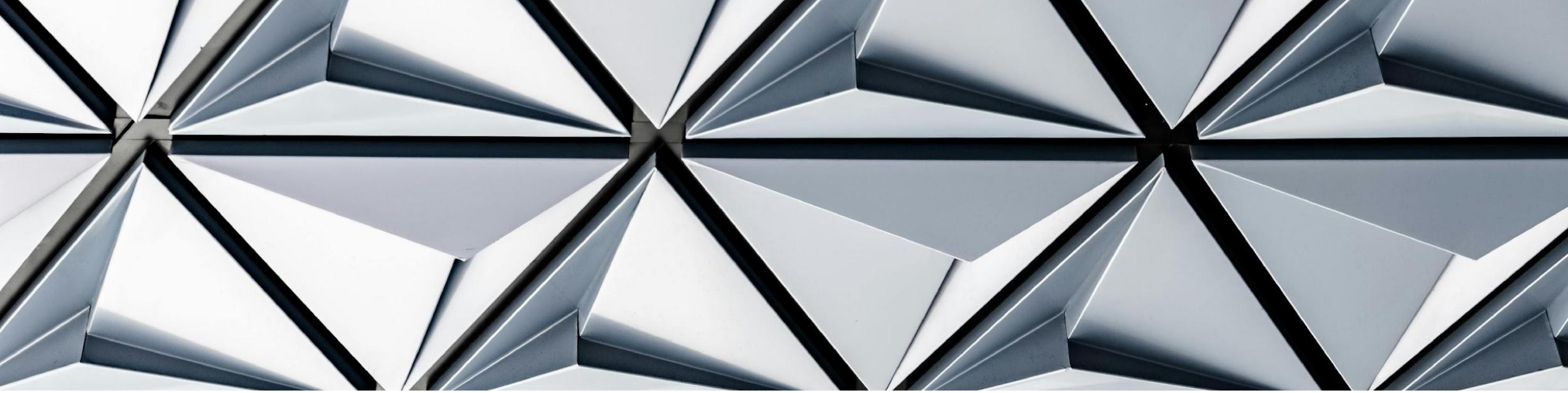
Securing the digital space

/ Encryption



/ Digital Signature

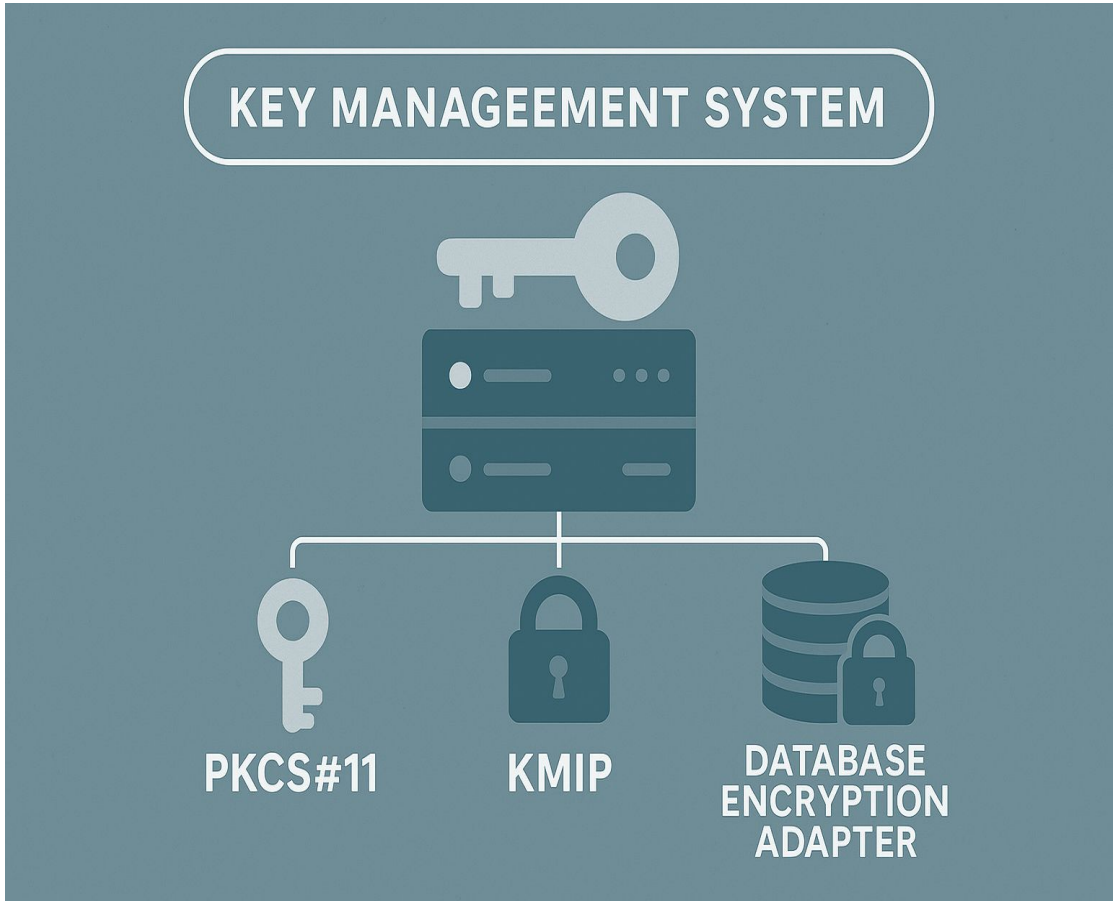
Key Management



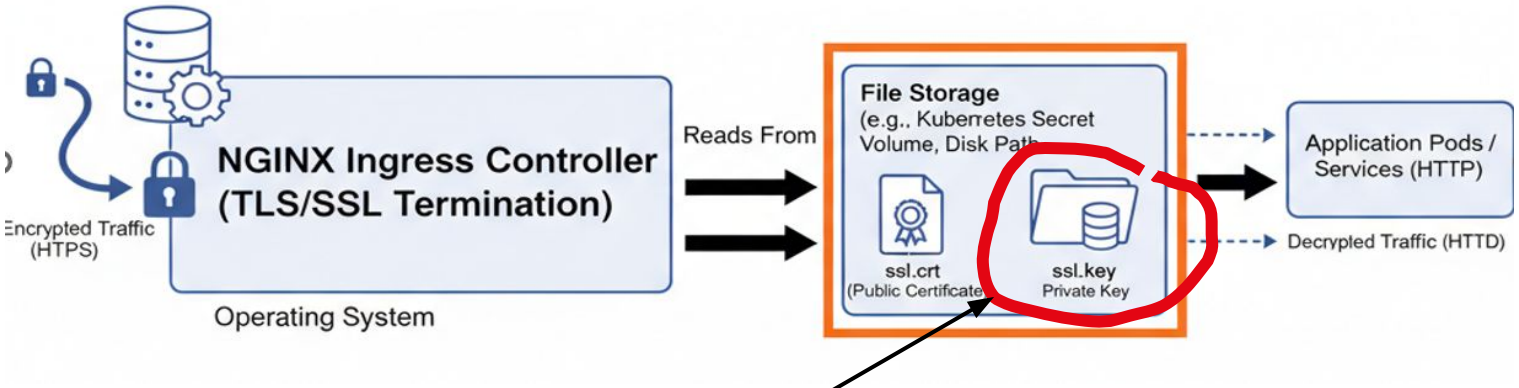
02/ **Key management**

Key Management System (KMS)

Reality Check



The simple key management system



security

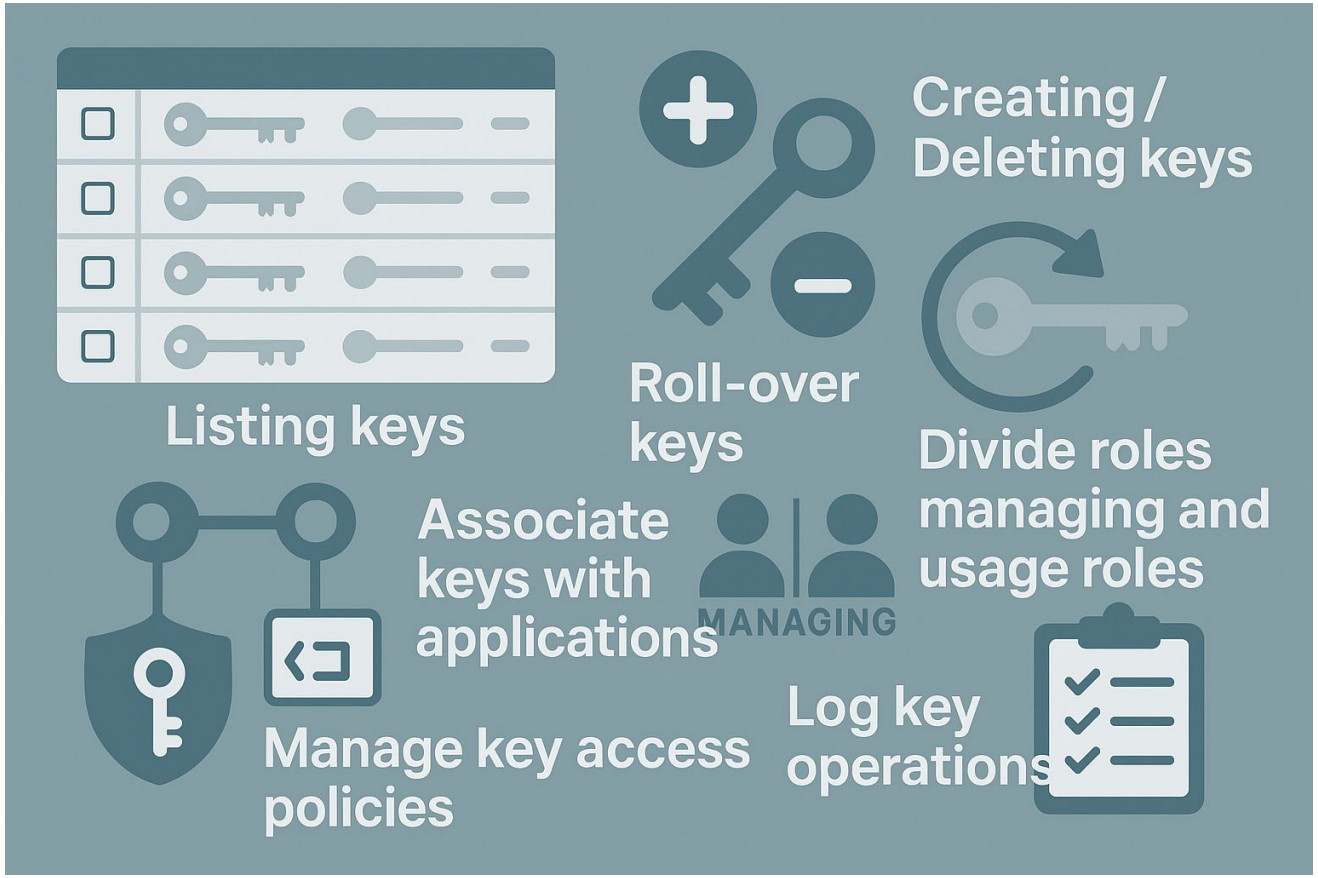
compliance

scalability

Key Storage Method	Security Level	Typical Use Case	Trend
File System	Low	Small-scale, legacy, or non-regulated deployments	Decreasing (replaced by KMS/HSM)
HSM (Hardware Security Module)	Very High (FIPS L3/L4)	Mandated compliance (PCI DSS, financial, government)	Steady/Growing (often via Cloud KMS)
KMIP/KMS (Key Management Service)	High (Hardware-backed or software)	Cloud and large-scale, distributed hybrid environments.	Rapidly Increasing

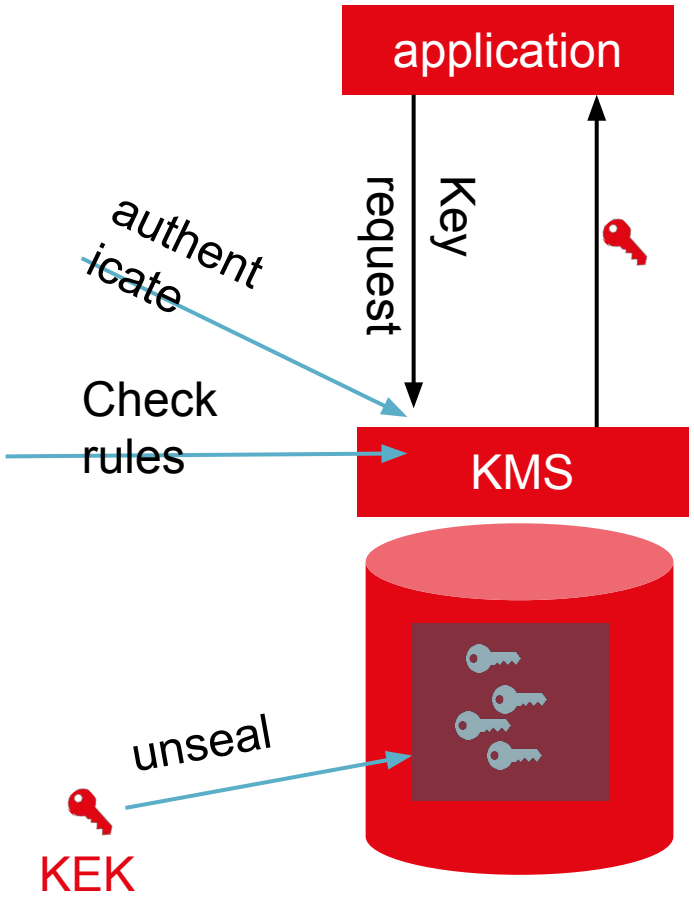
Key Management?

- Listing keys
- Creating / Deleting keys
- Roll-over keys
- Associate keys with applications
- Devide roles manging and usage roles
- Manage key access policies
- Log key operations



Accross all IT infrastructure

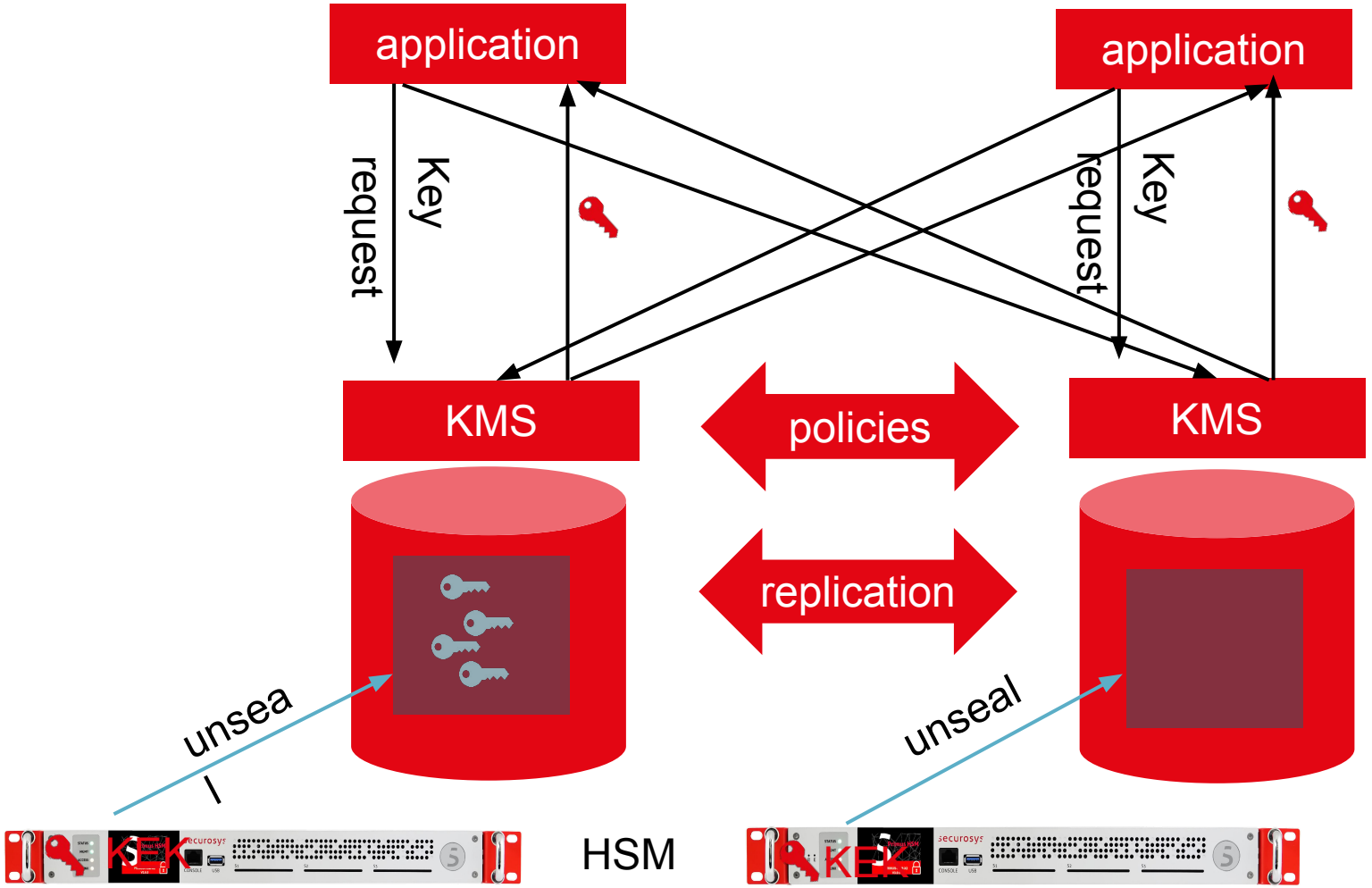
Typical operation of a KMS



Challenges

- Multiple application protocols
  - KMIP, PKCS#11, JCE, CNG, RestAPI
- Key exposure
  - None, DRAM, persist
- Key audit logging (key usage)
- Key exposure in store
  - Unseal (data@rest security only)
- KMS Redundancy
- Unseal KEK storage

The redundant KMS



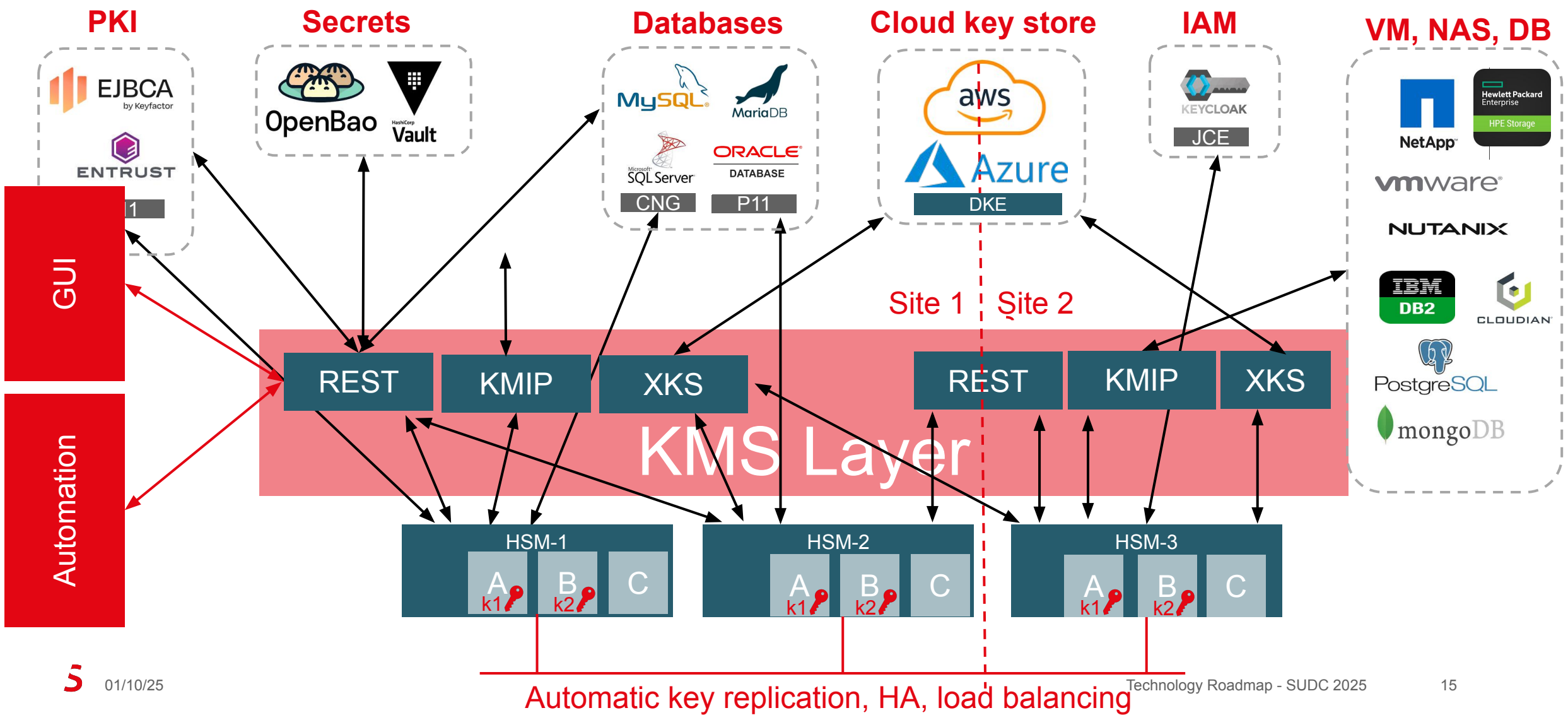
Still challenges

- Multiple application protocols
  - KMIP, PKCS#11, JCE, CNG, RestAPI
- Replication
- Secure key storage (Hardware keys)
- Key generation quality
- Statefull keys (SP800-208)
- Exensibility with other additional tools (PKI, secrets managment, …)

Turn things up side down

- Use a unified key store
  - Access control
  - Policy controls
- Any protocol can access key store
- KMS manges keys in key store
  - Not replicating protocols
  - No overlay authentication

Unified Key Store, Many Access Protocols



Key Management on the Next Level

- Fully **redundant, scalable** cross platform, for on-prem, hybrid and cloud
- Keys can be shared across platforms
- **Unified view and access control**, supporting for all interfaces, like KMIP, PKCS#11, JCE, CNG, REST/KMS, OpenSSL
- Seamlessly integrating with any PKI
- Combined with **secrets management**
- **Extensible with 3rd party tools** and easy to integrate in exsting workflows through REST API.
- **Keys created** and **stored in (**FIPS, CC **certified)** secure key store (**HSM)**

Key store (HSM) enforces Roles and policies

/ Key manager role

- create, delete, import, export, set properties, enumerate

/ Key user role

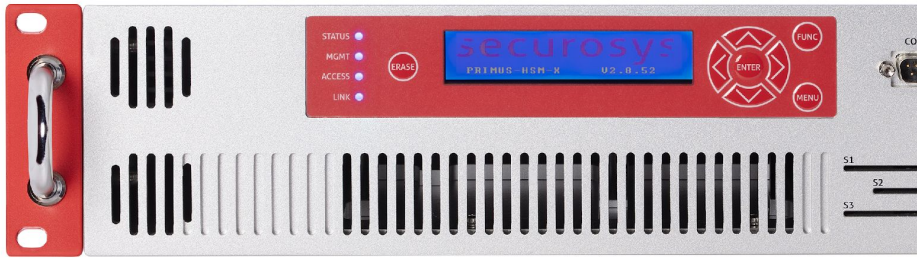
- sign, verify, encrypt, decrypt, wrap, unwrap, session key creation / deletion, enumerate

/ Key policies for user roles

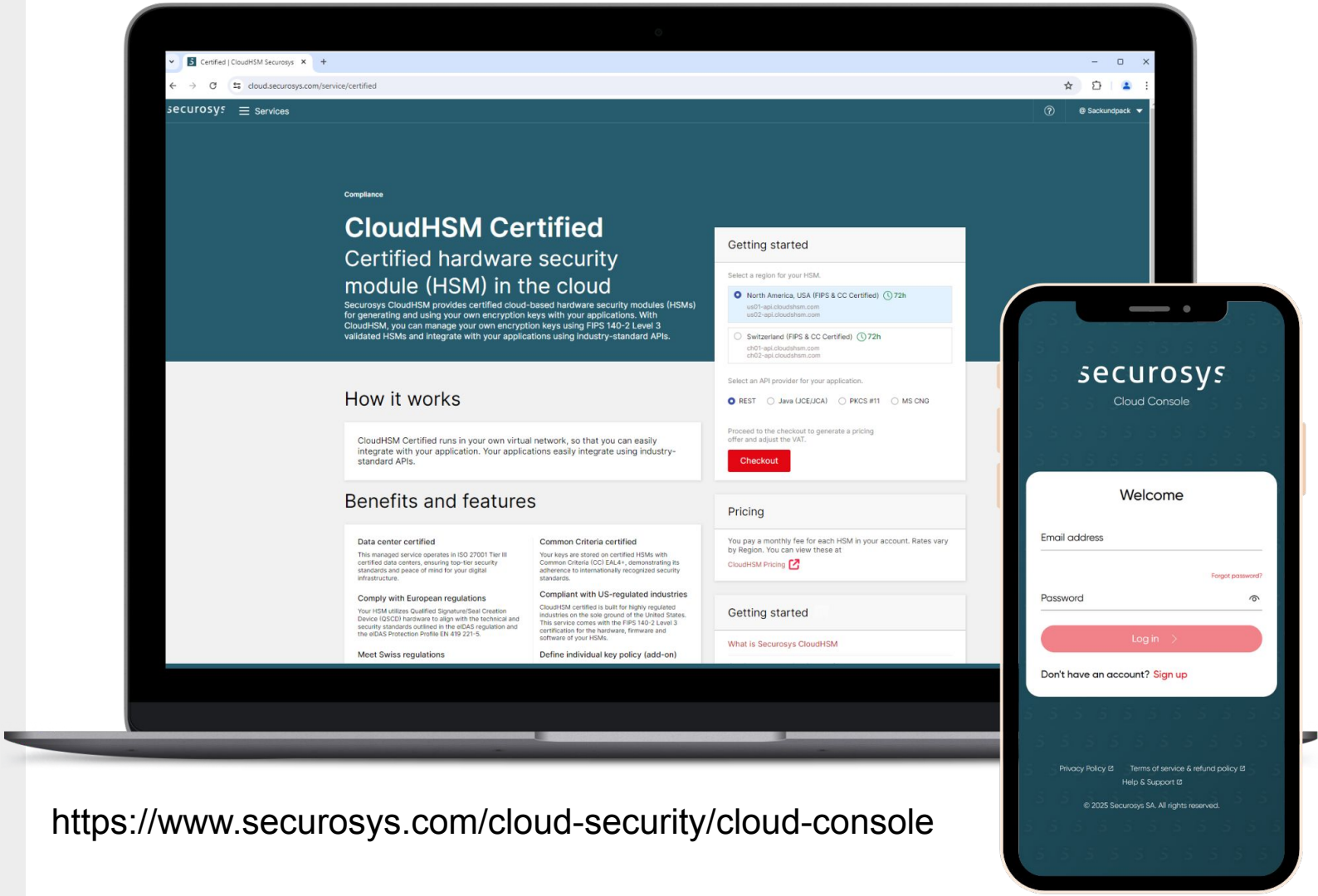
- All operations and access protocols

Key store function
Unified for any API

Primus HSM CyberVault



Try it out!
Cloud console



https://www.securosys.com/cloud-security/cloud-console

Thank you

Securosys SA
Max-Högger-Strasse 2
8048 Zurich, Switzerland

+41 44 552 31 00

info@securosys.com