securosys

HSM in the Cloud
Threats and Opportunities

Robert Rogenmoser,
CEO Securosys SA

SIGS Technology Conference
Datacenter Day
May 16, 2017, Regensdorf

Agenda

- How are your keys protected?
- Why do we need HSM?
- HSM as a Service — an Oxymoron?
  - Benefits and Drawbacks of a Cloud HSM
  - Securosys Cloud HSM
- Summary

Keys ?

- Encryption keys
  - asymmetric e.g. RSA, ECC public/private key pairs for wrapping
  - symmetric e.g. AES, RC4, 3DES keys
- Signature keys
  - asymmetric e.g. DSA, ECDSA public/private key pairs for signing (of object hashes)
  - hash algorithms e.g. SHA-2, SHA-3
- Certificates
  - digitally signed public keys

How are my keys protected ?

- Different OS have different strategies
  - By software encryption (but where is the encryption key stored ?)
  - Trusted platform module (just one per machine)

- Software cannot protect your keys
  - A trust anchor is required

Linux (and various Unix)

Linux

- Keys are protected by user / group file permissions
  - privileged users (e.g. “root”) can access everything
- Keys are typically stored in files, e.g. in users home directory

```
roro$ ls -al .ssh
-rw-------  1 roro   staff  1766 Jan 27  2015 id_rsa
-rw-r--r--  1 roro   staff   400 Jan 27  2015 id_rsa.pub
```

Microsoft

- Keys are stored encrypted in
  - file system for standalone
  - user profile for domain
- Encryption key per user (user master key)
  - rolled over regularly
  - stored in profile encrypted with logon password and user SID.

Key type	Directory
User private	%APPDATA%\Microsoft\Crypto\Keys
Local system private	%ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\SystemKeys
Local service private	%WINDIR%\ServiceProfiles\LocalService
Network service private	%WINDIR%\ServiceProfiles\NetworkService
Shared private	%ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\Keys

Keychain on OSX

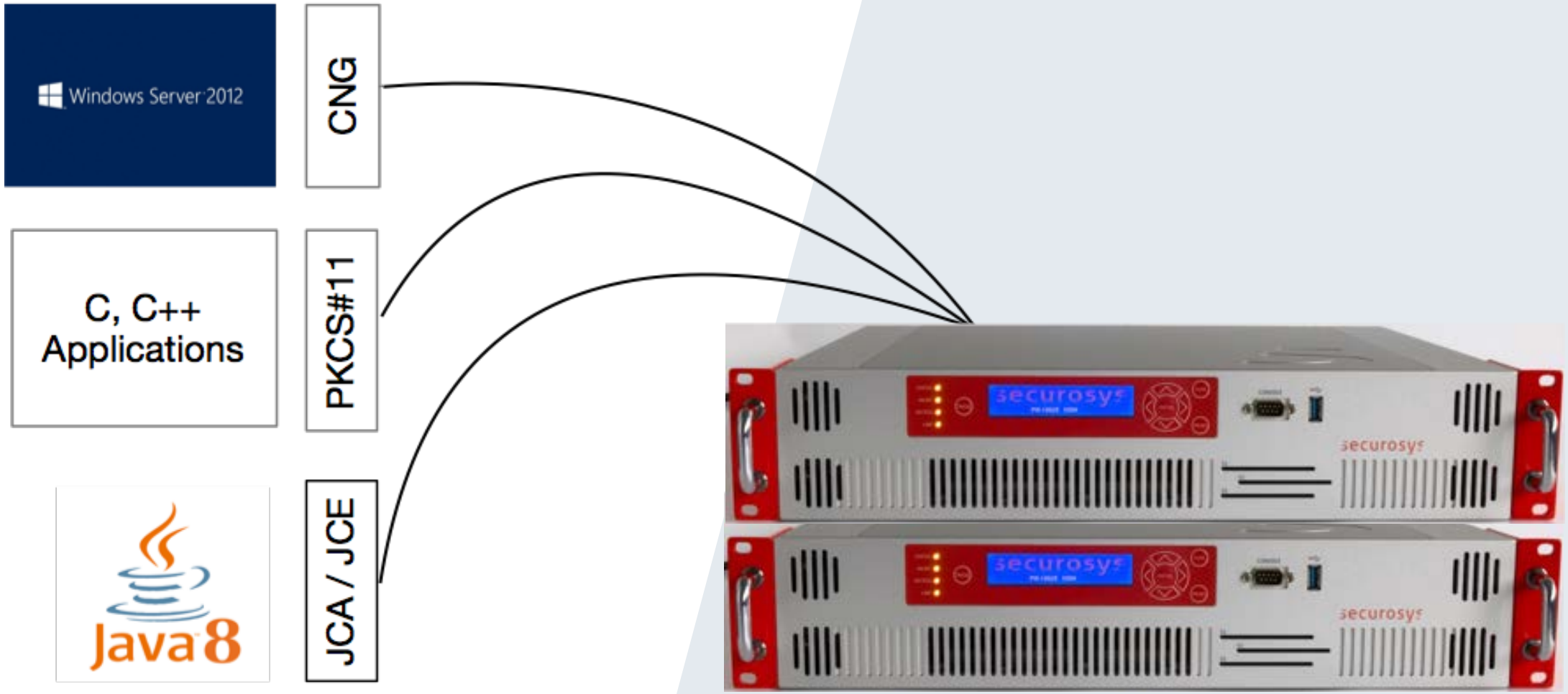
- Keys (certificates, passwords, etc.) are stored via the keychain application
- The keychain is located in the users profile directory
  - ~/Library/Keychains
- Keychains are encrypted with password derived keys
- Login key chain can be accessed with “root” privileges

The trust anchor

- HSM is a Trust Anchor
  - Generates trusted certificates and keys
  - Safeguards keys = Key storage

- Different form factors
  - Hardware security module (performance)
  - Smartcard (portability)

Integration of a trust anchor

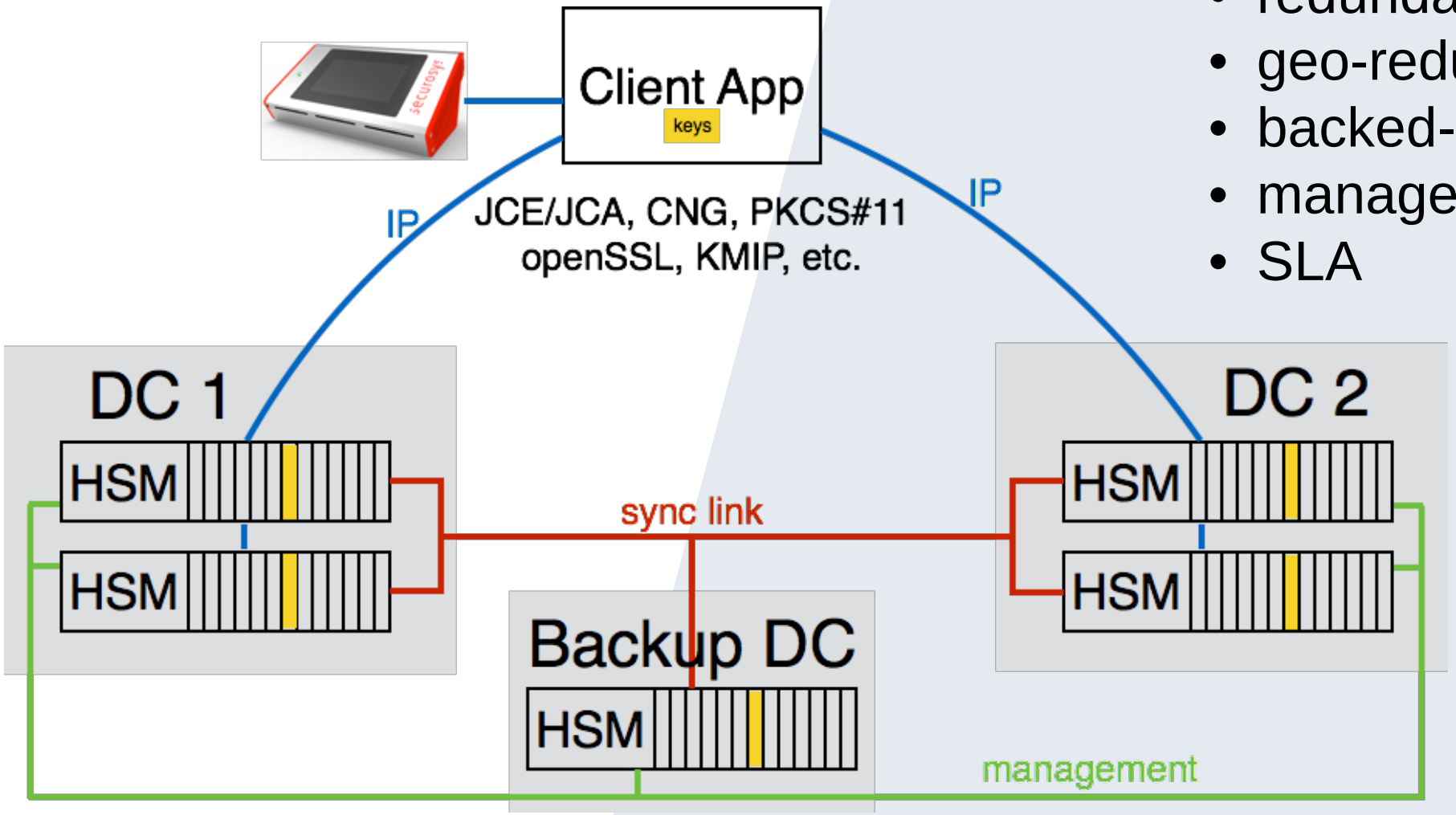


Moving the HSM to a Cloud Service

HSM as a Service - an Oxymoron?

- Availability and Redundancy
  - More than 1 HSM
  - Internet Access: Multiple providers
  - Datacenter Failover — Geo-Redundancy
- Access
  - Protection from DoS attack — Firewall, Proxy
  - Increased latency: ms instead of µs
  - Security officer functions
  - Backup
- Trust
  - Provider
  - Location
  - Move out

Securosys Cloud HSM



- Partition
- redundant
- geo-redundant
- backed-up
- managed
- SLA

Securosys Cloud HSM

- Swiss company
- Swiss datacenters
- Swiss law

- Highest Availability (Swiss Banking Standard):
  - Redundant HSM in two locations:
    - Zürich (Equinix)
    - Attinghausen (Deltalis, former Swiss Air Force Bunker)
    - Backup HSM in third location
- Dual Internet Access with Cogent and SwissIX
  - Firewall with authenticating proxy

Securosys Cloud HSM (cont'd)

- Security
  - Securosys Primus HSM — in FIPS140-2 Level 3 certification
  - Datacenters ISO27001 conform
  - Control: Security officer functions via Decanus remote device
  - Move out option: Transfer your keys to your own HSM
- Scalability & Setup
  - Adjustable SLA: Performance and key storage space
  - Quick setup: Securosys Cloud HSM ready to connect
  - Lower costs: No capital cost — pure service
- Operations & Support

Summary

- Your keys need to be protected in a trust anchor:
  - Hardware Security Module
- Moving to the cloud: control, availability, readiness
  - Who is the provider?
  - Who has access to the keys?
  - Which jurisdiction?
  - Redundant setup?
  - How much effort is it to get going?
- Securosys Cloud HSM — Primus Cloudus
  - In test operation — looking for Beta-Customers

Thank you!

securosys

Robert Rogenmoser
Technoparkstrasse 1
CH-8005 Zürich

roro@securosys.ch
www.securosys.ch
+41 44 552 31 00