"T.I.S.P. Community Meeting 2022"

Berlin, 09.-10.11.2022

Hardware-Sicherheitsmodule in der Cloud – kann das sicher sein?

Tom Schiekel & Ulf Seifert / Softline AG

WER SIND WIR ?

Tom Schiekel // Dipl. Inf.

2008 – 2010	**Snom Technology AG** *Softwareentwickler*
2010 – 2018	**Nexus Technologies GmbH** *IT-Consultant // Presales Engineer*
2018 – 2022	**Softline Solutions GmbH / Softline AG** *Senior Berater // Team Lead // T.I.S.P.*

E-Mail: tom.schiekel@softline-group.com
Web: https://www.softline-solutions.de
Informationssicherheit und IT-Sicherheit

Ulf Seifert // Dipl. Ing. Elektrotechnik

2001 – 2010	**PC-WARE Technologies GmbH** *Team Lead // IT-Security Principale*
2010 – 2022	**Softline Solutions GmbH / Softline AG** *Senior Berater // Team Lead // CISO // T.I.S.P.*

E-Mail: ulf.seifert@softline-group.com
Web: https://www.softline-solutions.de
Informationssicherheit und IT-Sicherheit

EINFÜHRUNG & GRUNDLAGEN

WAS IST EIN HSM UND WARUM BENÖTIGT MAN ES?

- Ein HSM ist ein manipulationssicheres Gerät, das dafür ausgelegt ist,
  - Schlüssel sicher zu erzeugen,
  - Schlüssel sicher zu speichern,
  - Kryptooperationen sicher auszuführen.

- Ein HSM enthält einen echten Zufallszahlengenerator (TNRG).
- Der Zugang zu den Schlüsseln kann durch Kartensätze und Passphrasen geschützt werden.

EINFÜHRUNG & GRUNDLAGEN

EINSATZGEBIETE EINES HSM

- PKI – CA-Schlüssel / OCSP
- Blockchain
- Website-Zertifikate (TLS)
- Application-Layer Encryption
- Code-Signatur / Datenbankverschlüsselung
- Key Injektion / Transaktionsabsicherung / Tokenization

- Absicherung von Cloud-Diensten / BYOD / HYOK
- IoT / Finanzsektor / …
- eIDAS Vertrauensdienste
  - Zeitstempel
  - Qualifizierte Signatur / Fernsignatur / Siegel

EINFÜHRUNG & GRUNDLAGEN

ZERTIFIZIERUNGEN FÜR HSM

- FIPS 140-2 Level 2 - 4
- Common Criteria Certified EAL4+
  - CEN EN 419 221-5 - Protection Profiles for TSP Cryptographic Modules
  - CEN EN 419 241-2 - Protection Profile for QSCD for Server Signing
- Payment Card Industry (PCI) Data Security Standard (DSS)
  - PCI-PTS (PIN Transaction Security)
- DUAL Random Number Generator (TRNG (AIS.31) and PRNG (FIPS))
- VS-NfD Zulassung

EINFÜHRUNG & GRUNDLAGEN

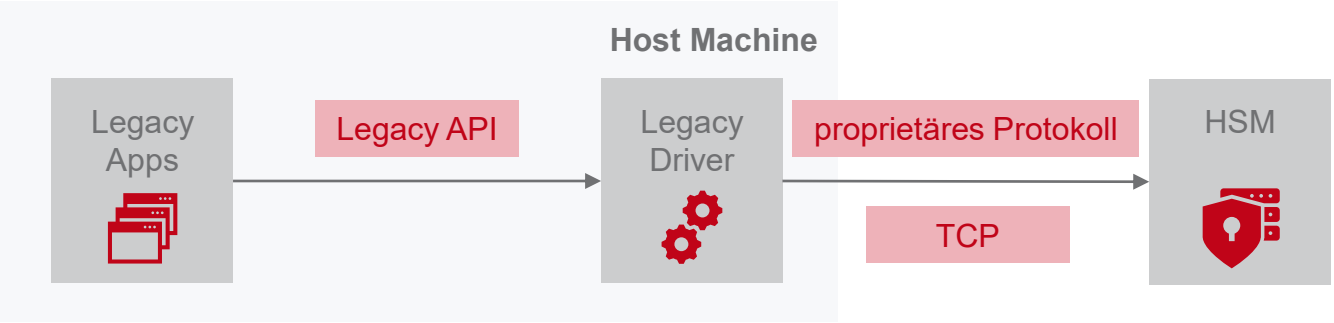
HSM-SCHNITTSTELLEN

Legacy-APIs

- PKCS#11
- Microsoft CNG (Cryptography API: Next Generation)
- Microsoft EKM (Extensible Key Management)
- Nicht „cloud-fähig“
- HSMs bieten keine Cloud-APIs an

Cloud-APIs

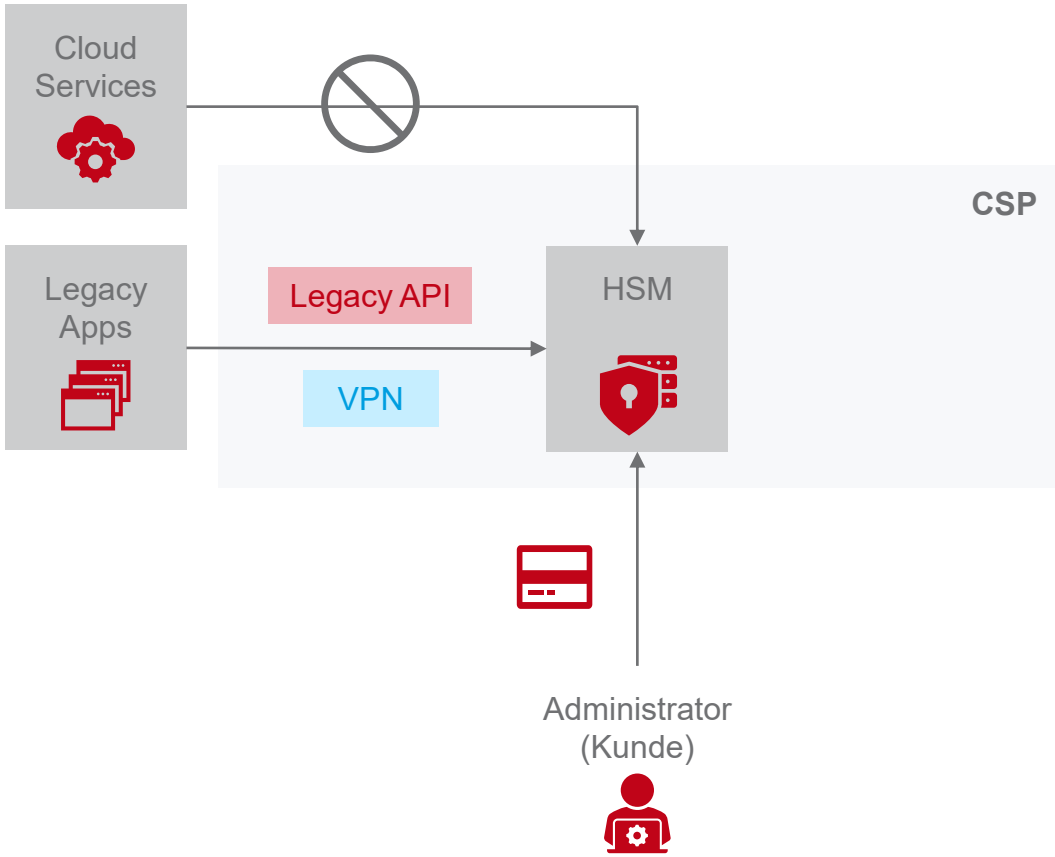
- Ermöglicht es Cloud-Diensten, untereinander zu kommunizieren
- Protokolle: REST, SOAP, JSON-RPC
- Transportsicherheit mittels TLS



BETRIEBSMODELLE

HSM ALS IAAS-DIENST

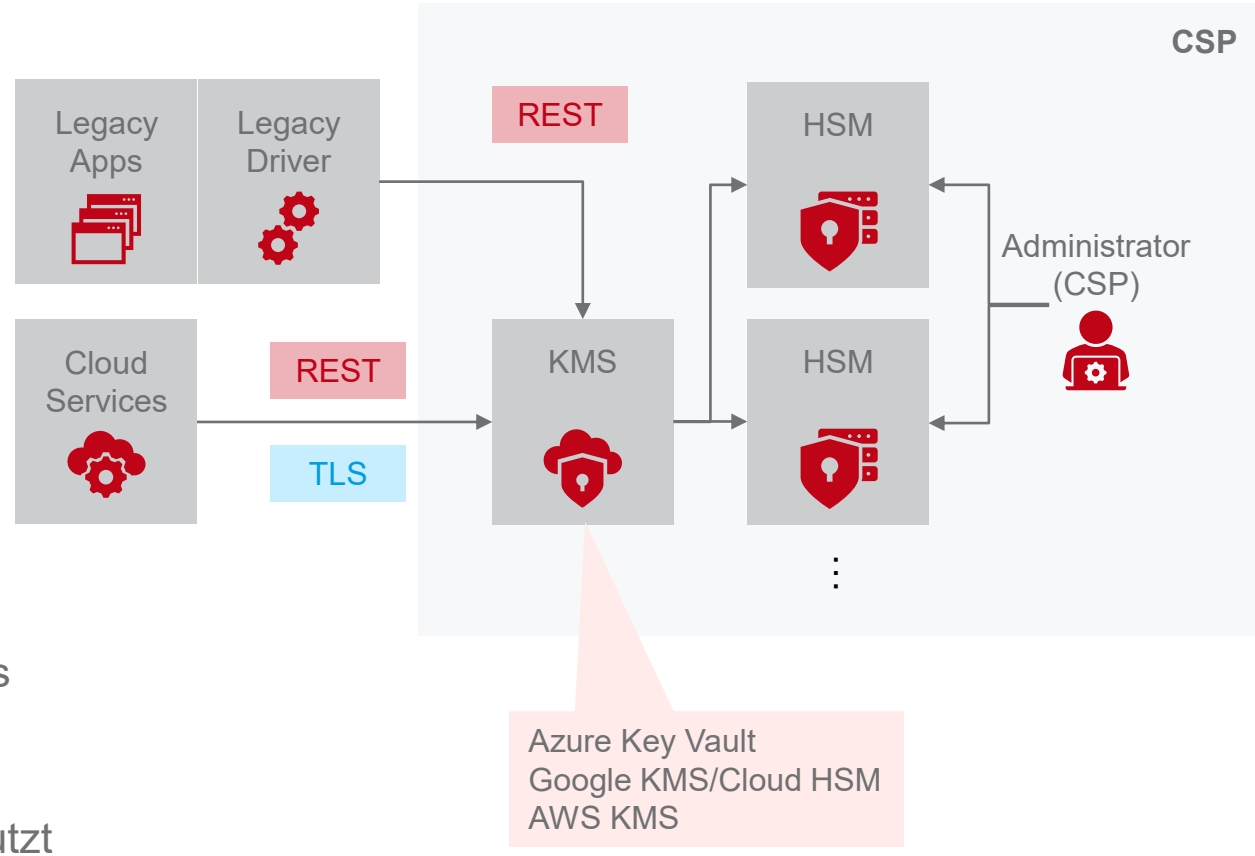
- HSM befindet sich im Rechenzentrum des CSP
- HSMs werden kundenseitig administriert
- HSM „gehört“ dem Kunden
- Legacy API (CNG, EKM, PKCS#11)
- Unzureichende Möglichkeiten der Integration von Cloud-Anwendungen
- Ggf. Vendor Lock (hängt von CSP ab)
- Zugriffsverwaltung obliegt dem Kunden – Zugriff durch CSP grundsätzlich nicht möglich
- CSP hat physischen Zugriff, aber keine logischen



BETRIEBSMODELLE

HSM ALS PAAS / SAAS

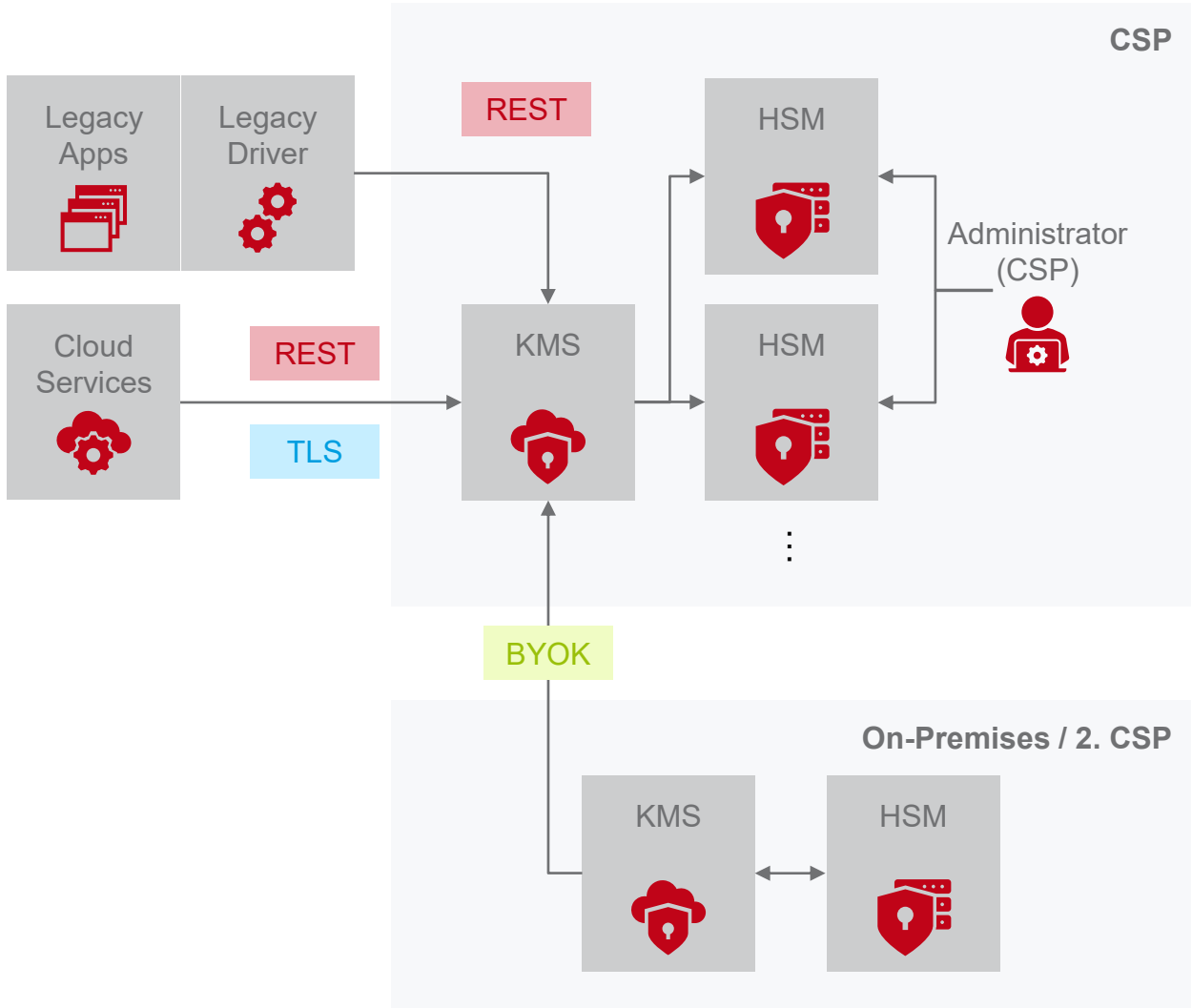
- HSM „gehört“ dem CSP
- Administration und Zugriffsverwaltung erfolgt durch CSP
- CSP hat physischen und logischen Zugriff auf das HSM
- Serverless – Zugriff wird durch ein Cloud Key-Management-System (KMS) ermöglicht
- Legacy-Treiber ermöglichen Integration mit Legacy APIs
- Vendor-Lock – HSM-Modelle sind vorgegeben
- I.d.R. werden die HSMs von mehreren Mandanten genutzt
- KMS APIs sind proprietär und maßgeschneidert für das CSP-Ökosystem
- Kunde verfügt über keine Schlüsselhoheit → BYOK



BETRIEBSMODELLE

HSM ALS PAAS / SAAS

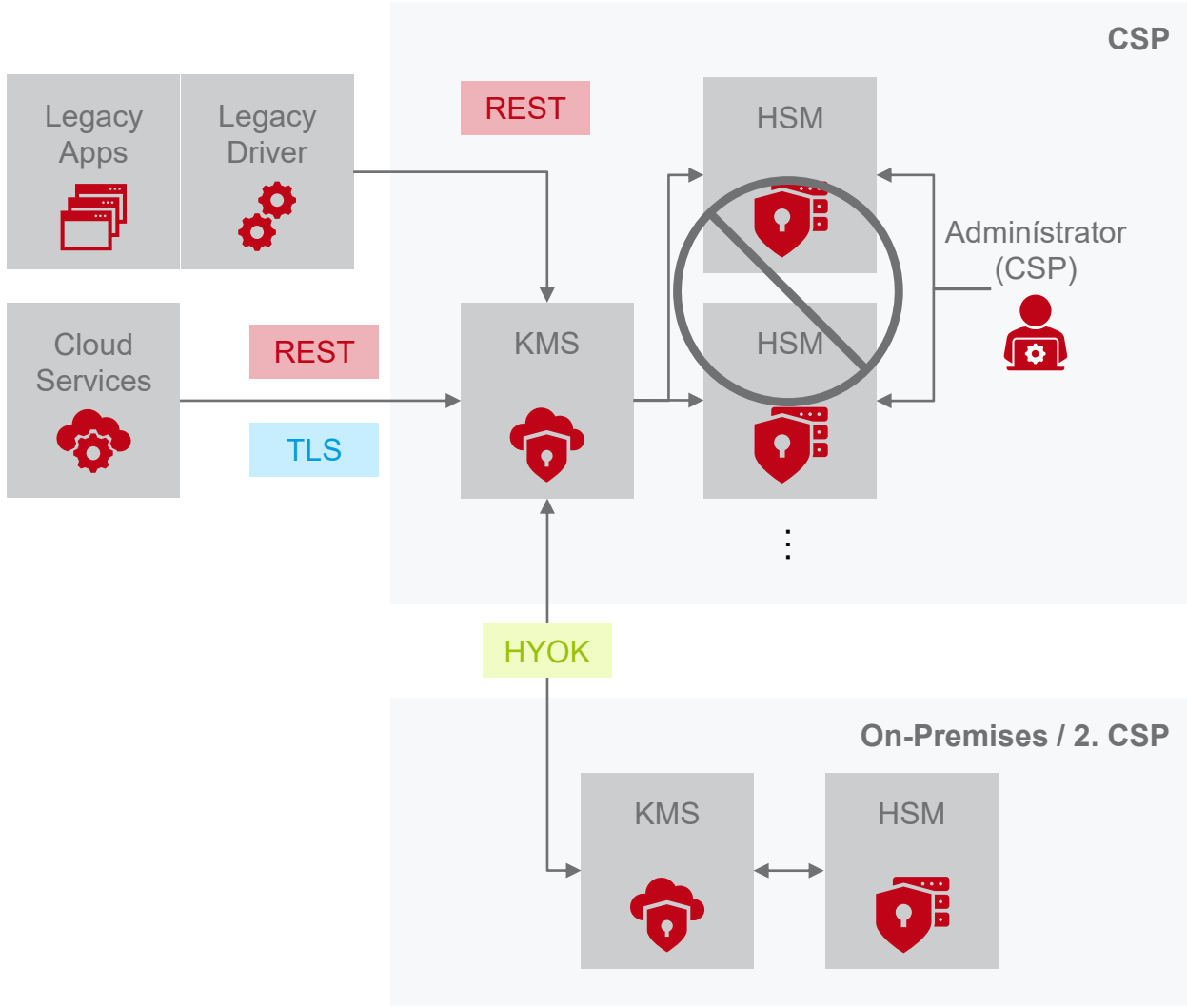
- Bring-Your-Own-Key (BYOK)
  - Keys werden kundenseitig erzeugt
  - Der CSP und der Kunde verfügen über das Schlüsselmaterial
- Alleinige Kontrolle der Schlüssel → HYOK



BETRIEBSMODELLE

HSM ON-SITE

- Hold-Your-Own-Key (HYOK)
- Volle Schlüsselkontrolle
- Eingeschränkte Unterstützung bei Cloud Diensten, z.B. Office 365:
  - Data Loss Prevention
  - Transport Rules
  - eDiscovery
- Vendor-Lock – HSM Hersteller müssen für jeden CSP die API implementieren
- eigene HSM Infrastruktur muss betrieben werden



RESÜMEE

HARDWARE-SICHERHEITSMODULE IN DER CLOUD – KANN DAS SICHER SEIN?

Die Art und Weise wie HSMs in der Cloud betrieben werden ist komplex hängt von einer Vielzahl von Aspekten ab.

Welche Schnittstellen müssen bedient werden?

- Legacy, Cloud (REST)

Welche Zertifizierungen werden benötigt?

- FIPS 140-2 L3, eIDAS CC, …

Welche Schutzbedarf strebe ich an?

- Volle Kontrolle / Zertifizierungen

Kann ich eine eigene Infrastruktur aufbauen?

- HYOK / BYOK

Muss ein HSM Vendor-Lock vermieden werden?

Muss die Lösung multicloud-fähig sein (keine Abhängigkeit von einem CSP)?

Die Sicherheit hängt von den eingesetzten HSMs und vom Betriebsmodell ab.

Nur 2 Verfahren garantieren die volle Schlüsselkontrolle:

- HSM als IaaS
- HYOK

Je nach Betriebsmodell sind funktionale Einschränkungen hinzunehmen.

Von pauschalen Aussagen hinsichtlich des Betriebs und der Sicherheit von HSM in der Cloud ist Abstand zu nehmen.

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

Tom Schiekel & Ulf Seifert

PHONE // +49 (341) 24051-236 & +49 (341) 24051-139
E-MAIL // tom.schiekel@softline-group.com & ulf.seifert@softline-group.com