Bundesministerium
für Wirtschaft
und Energie

Trusted Cloud

Architektur und Sicherheitsaspekte des Text-Mining in der Cloud

TMF-Workshop, 28. Januar 2015, Berlin

averbis
text analytics

Fraunhofer
SCAI

FAU FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG
MEDIZINISCHE FAKULTÄT

Universitätsklinikum
Erlangen

TMF

RHÖN-KLINIKUM
AKTIENGESELLSCHAFT

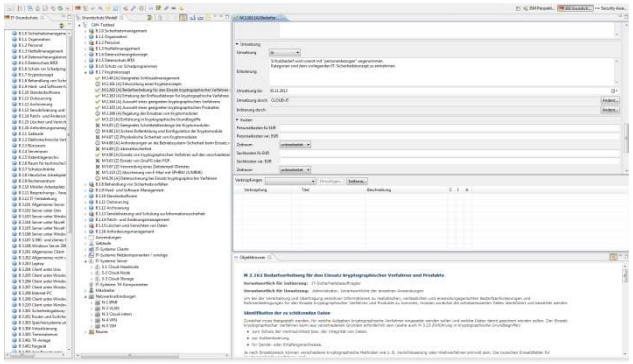
- Herausforderung: Sensible, personenbezogene Daten
  - Adressierung rechtlicher Rahmenbedingungen
  - u.a. Anlage zu § 9 Satz 1 des BDSG (techn. & org. Maßnahmen)

- Ziel: Sicherstellung von Vertraulichkeit und Integrität der Daten über den gesamten Lebenszyklus/DV-Workflow hinweg
- Ansatz von cloud4health: Ganzheitliches Sicherheitskonzept nach BSI 100-2 „IT-Grundschutz“

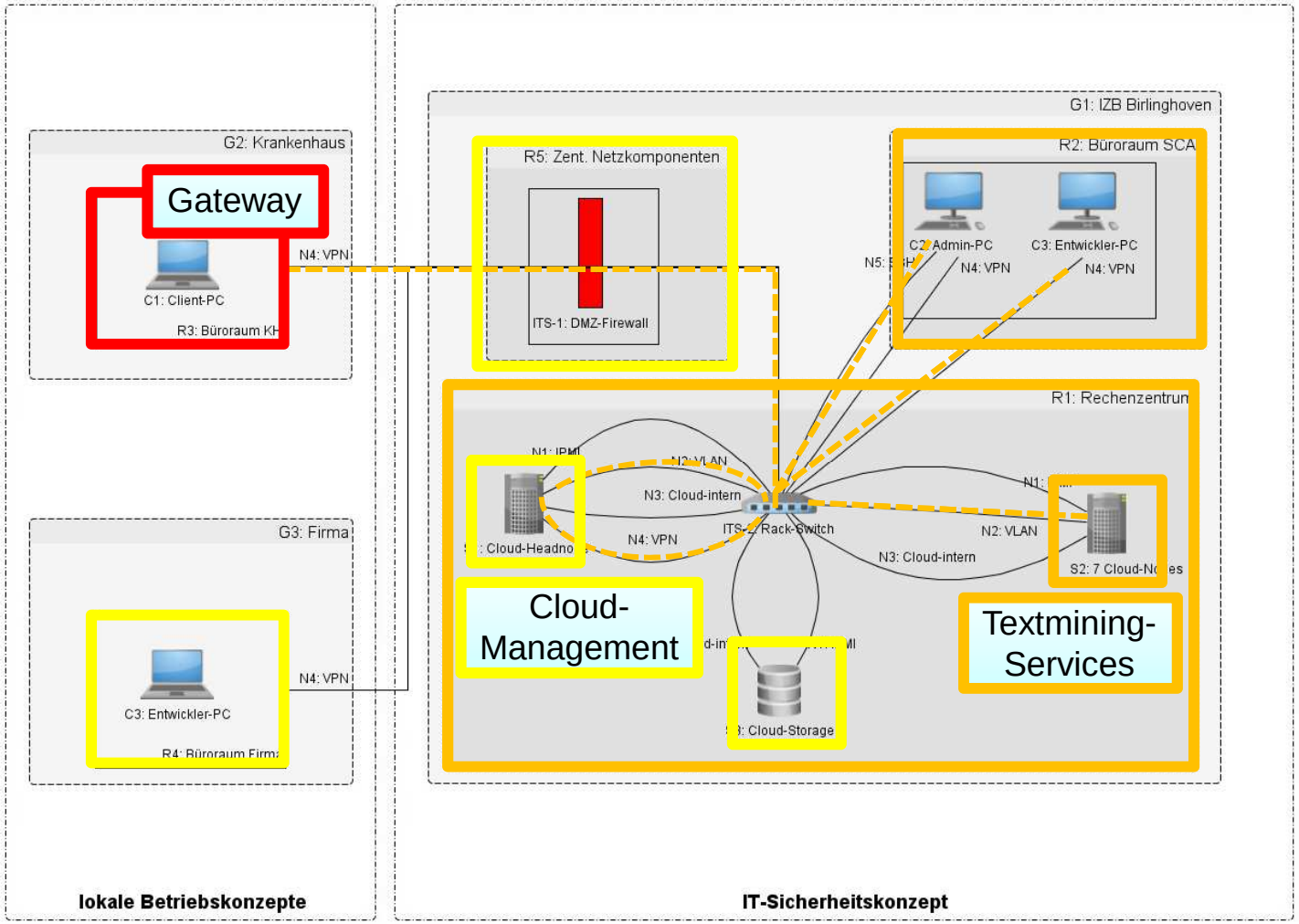
BSI 100-2: IT-Grundschutz

- IT-Grundschutz-Katalog enthält modulare Bausteine für umfassende IT-Sicherheit
  - Jeweils Auflistung möglicher Risiken und empfohlener Maßnahmen
- Umfangreiche Tool-Unterstützung
  - GS-Tool, Verinice, …
- Anerkanntes und zertifizierbares Vorgehen

Bundesamt
für Sicherheit in der
Informationstechnik



Ganzheitliches Sicherheitskonzept: Modularität

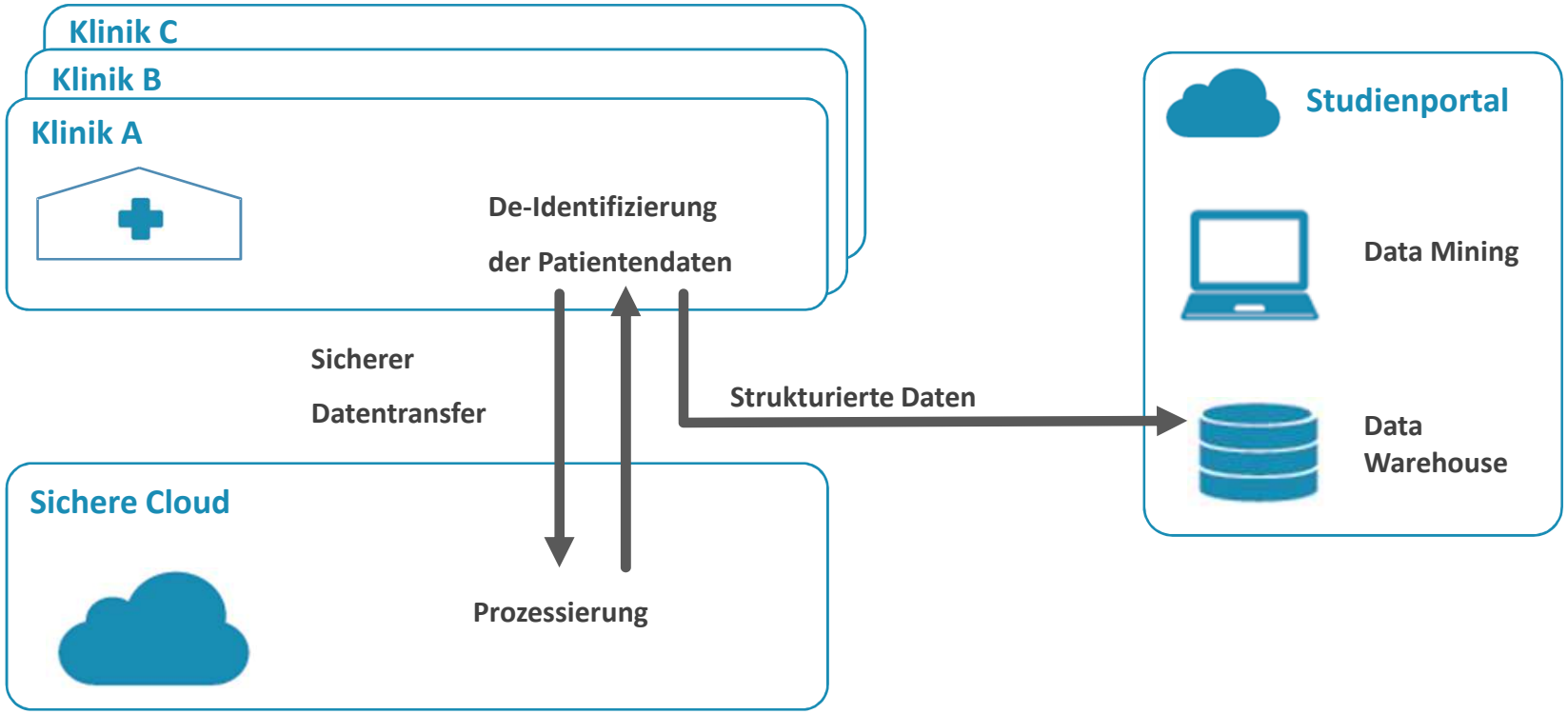


Schutzbedarf Vertraulichkeit

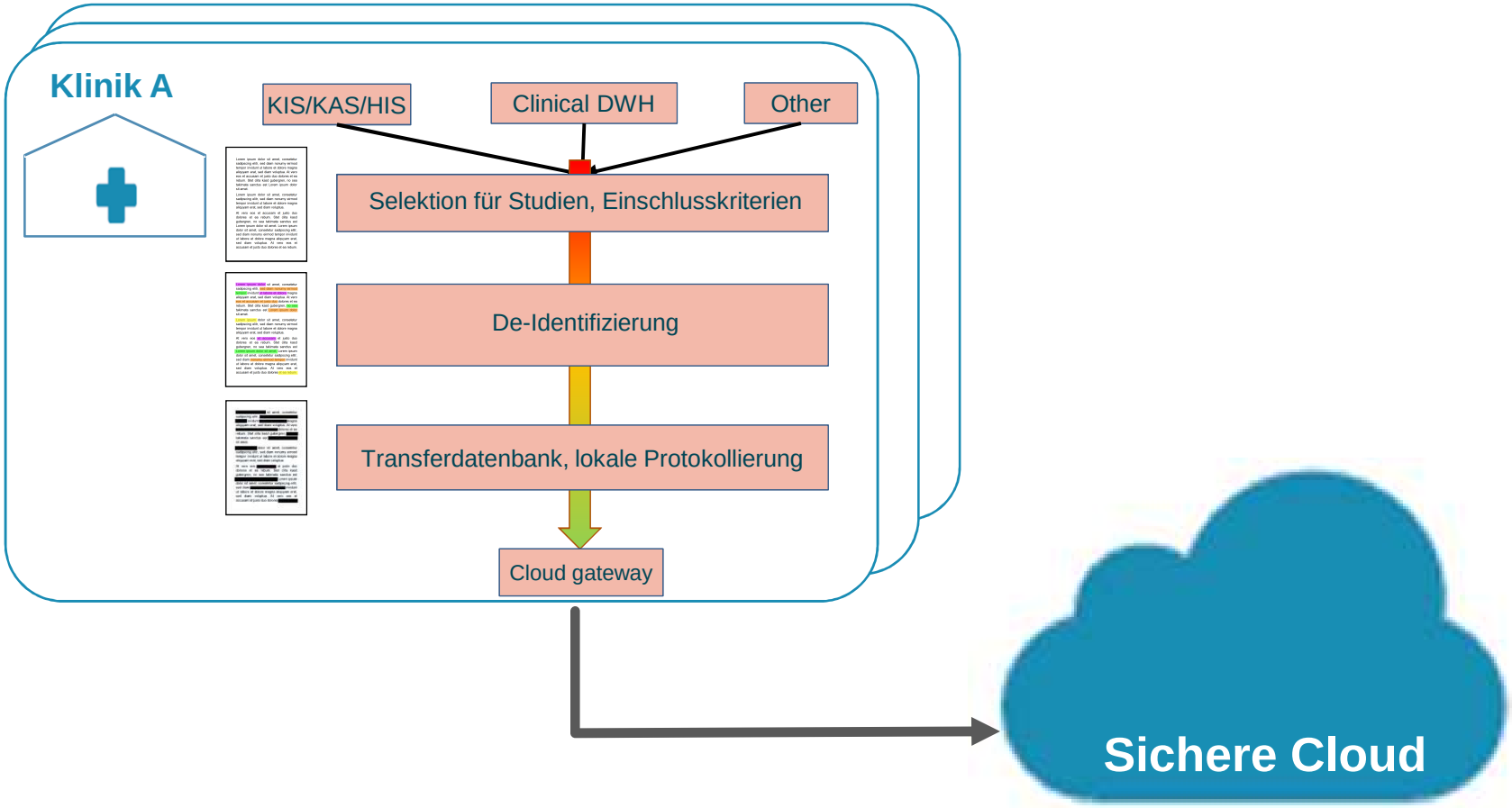
- normal
- hoch
- sehr hoch

Ganzheitliches Sicherheitskonzept: Architektur

Durchgängige Sicherheit durch abgestimmte, komplementäre Maßnahmen in Kliniken und zentraler Cloud-Infrastruktur



Klinik-interne Vorverarbeitung



Sicherer Datentransfer in die Cloud

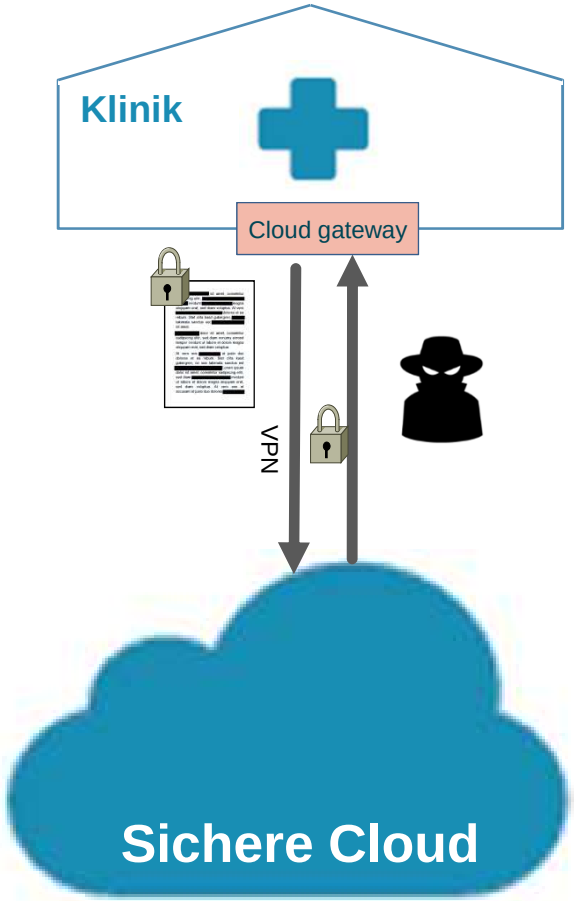
Herausforderung: Datentransfer über unsicheres Drittnetz

Ansatz auf mehreren Ebenen

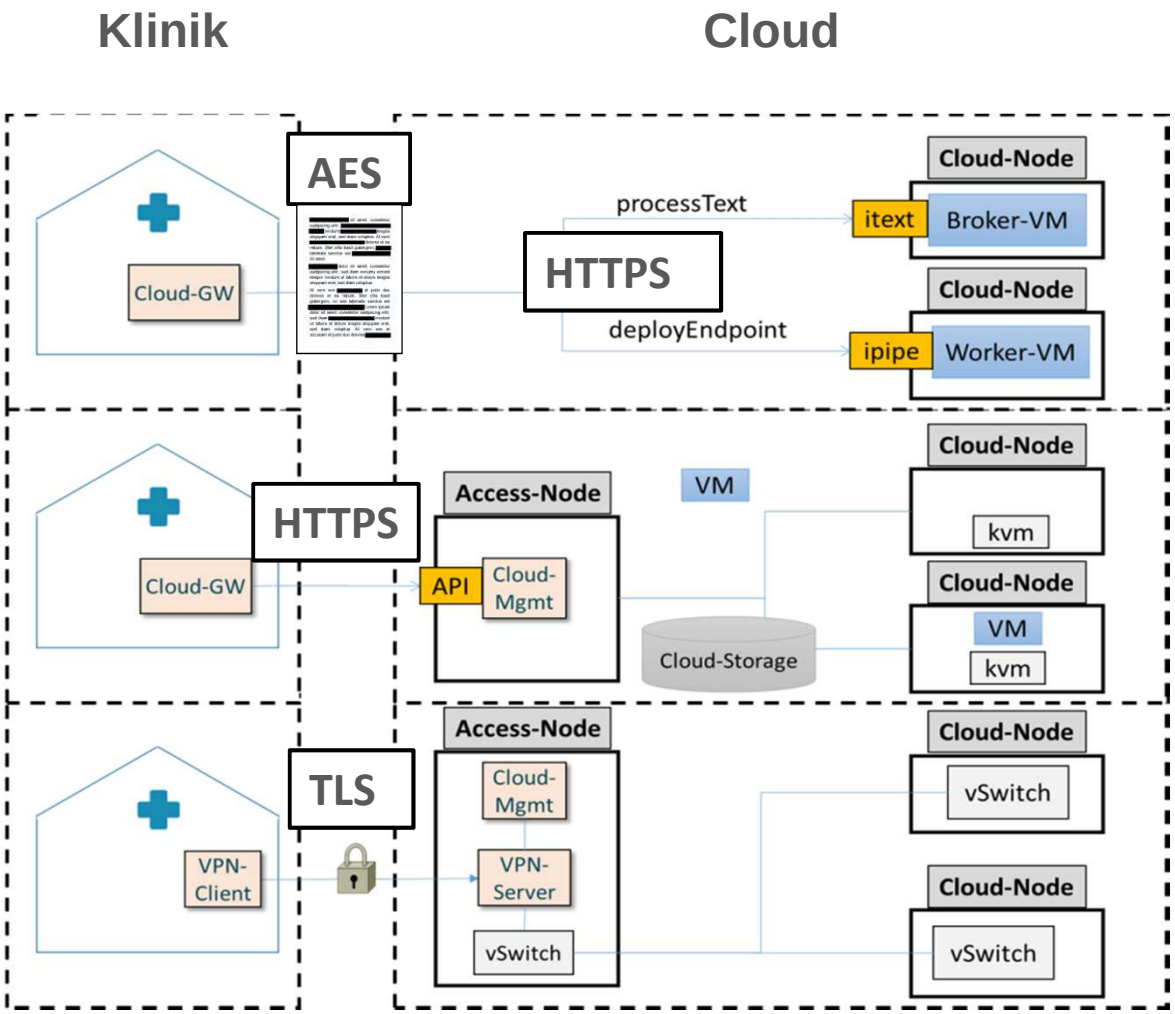
- Transportverschlüsselung (TLS)
- Anwendungsebene (HTTPS)
- Dokumente (AES)

Orientierung:

– Richtlinien des BSI (Ciphers, Schlüssellängen)



Verschlüsselung auf mehreren Ebenen



- Textmining-Services

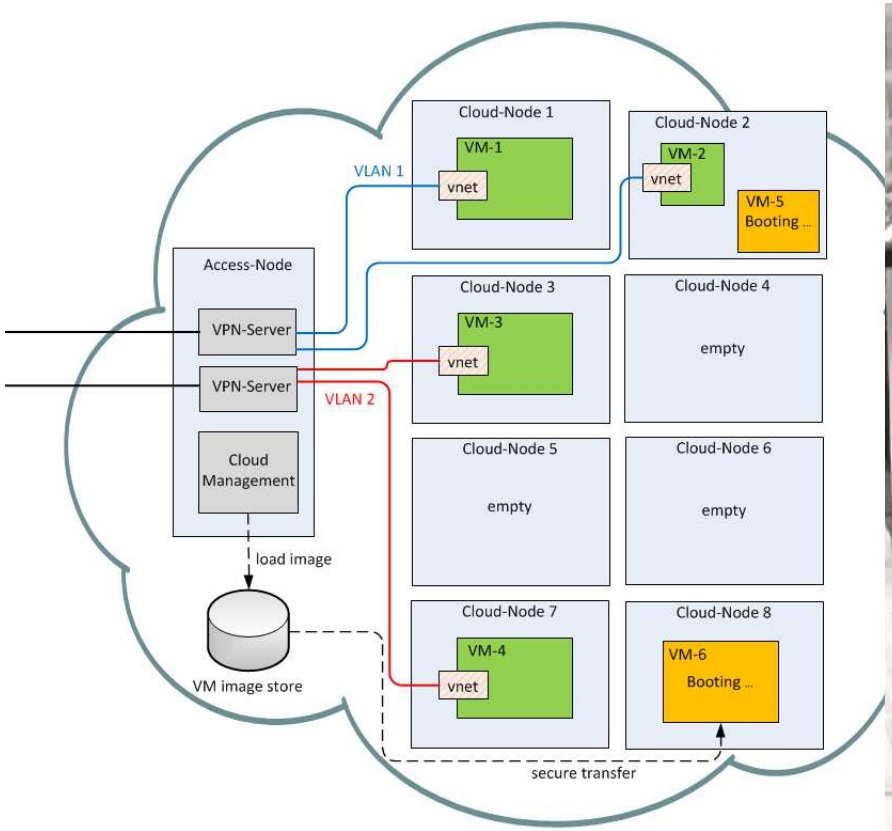
- AAA
- Initialisierung und Shutdown v. VMs

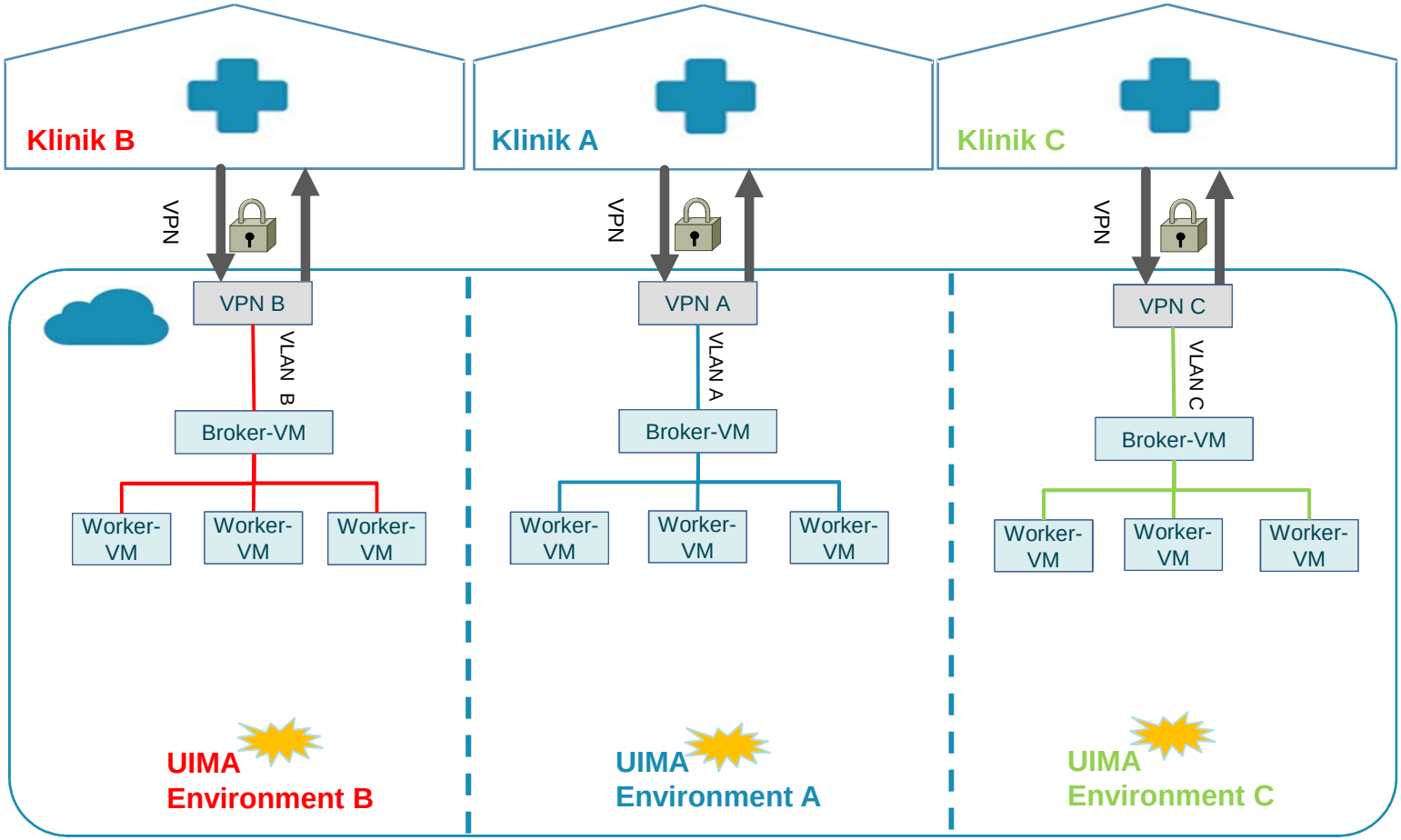
- Anbindung an Cloud-MW
- Netzintegration

Sichere Cloud @ Fraunhofer SCAI

cloud4health

Fraunhofer SCAI




Klinik B
Klinik A
Klinik C
VPN
VPN
VPN
VPN B
VPN A
VPN C
VLAN B
VLAN A
VLAN C
Broker-VM
Broker-VM
Broker-VM
Worker-VM
Worker-VM
Worker-VM
Worker-VM
Worker-VM
Worker-VM
Worker-VM
Worker-VM
Worker-VM
UIMA Environment B
UIMA Environment A
UIMA Environment C

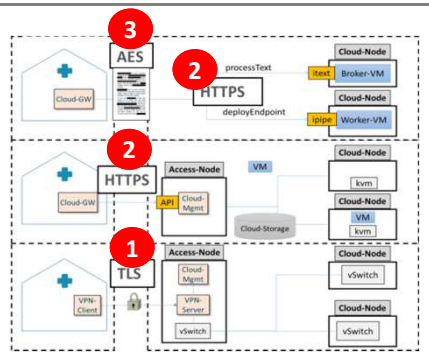
Sichere Cloud @ Fraunhofer SCAI

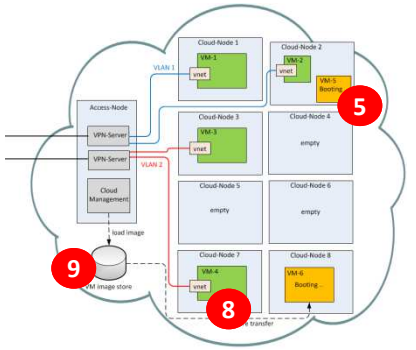
- Verschlüsselung
  - (1) Absicherung Klinik-Cloud durch VPN
  - (2) Anwendungsebene
  - (3) Einzelverschlüsselung der Dokumente

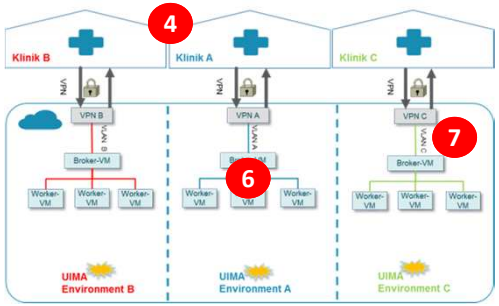
- (4) Community Cloud
- (5) Kein automatischer Datenabruf
  - Services werden vom Kunden gestartet

- Mandantentrennung
  - (6)Exklusive Textmining-Services pro Kunde
  - (7) Netzseparierung (VLAN + VPN)
  - (8) Exkl. Nutzung von Cloud-Nodes möglich
  - (9) Kein shared storage

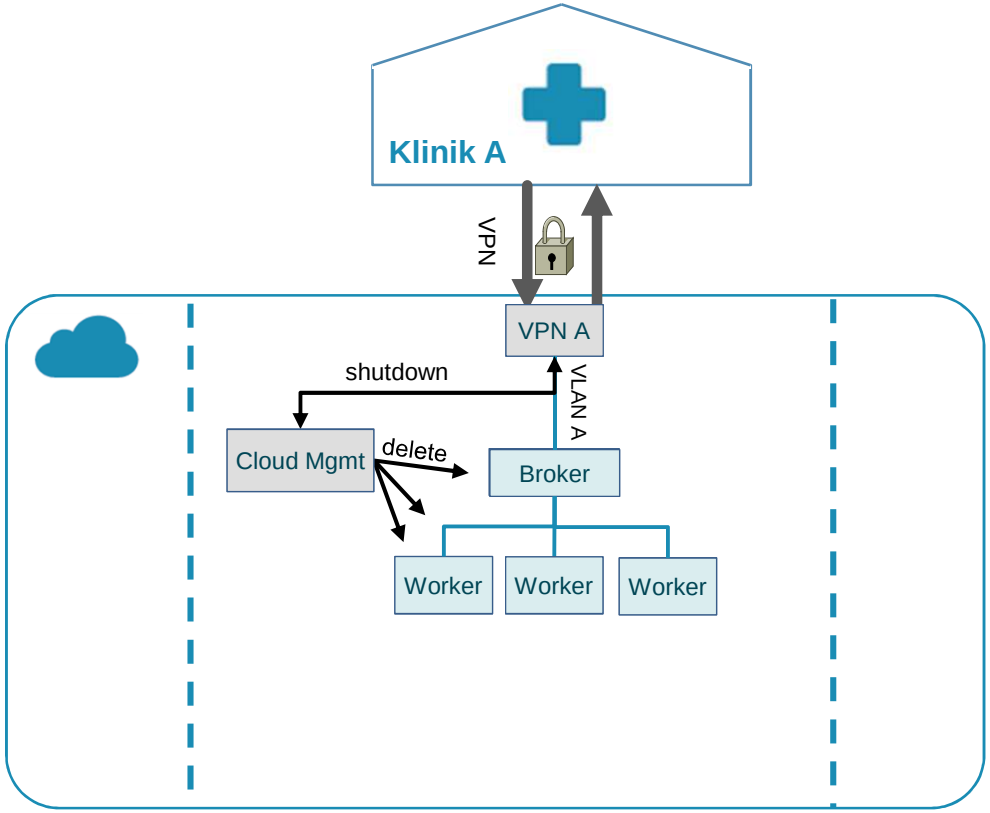
- (10) RZ am Standort Deutschland







Sicheres Herunterfahren von VMs



- Keine Persistierung von Patientendaten in der Cloud während der Prozessierung
- VM „lebt“ nur solange die Textanalyseservices benötigt werden
- Sicheres Löschen der VM-Images durch randomisiertes Überschreiben

Zusammenfassung

cloud4health

- Analyse medizinischer Daten in einer klinik-externen Cloud
  - Sensible, personenbezogene Daten
  - Sicherstellung von Vertraulichkeit und Integrität im gesamten DV-Workflow
- Zentrale Punkte des Sicherheitskonzeptes
  - Klinik-interne De-Identifizierung
  - Verschlüsselung auf mehreren Ebenen: Transportlayer + Anwendungslayer + Einzeldokumente
  - Mandantentrennung, vollständige Löschung der Daten etc.
- Basis und Orientierung des Sicherheitskonzeptes
  - Abstimmung von Cloud-Betreiber, Kliniken und Datenschützern
  - Vorgehen nach BSI 100-2 “IT-Grundschutz“
  - OH Mandantenfähigkeit, Protokollierung, Cloud
  - Internationale Rahmenwerke: ENISA, NIST, CSA …

cloud4health

Vielen Dank!

Kontakt: steffen.claus@scai.fraunhofer.de

averbis text analytics

Fraunhofer SCAI

FAU Friedrich-Alexander Universität Erlangen-Nürnberg Medizinische Fakultät

Universitätsklinikum Erlangen

TMF

RHÖN-KLINIKUM Aktiengesellschaft