

Konnektor im Feld ...Fertig?

Die Telematikinfrastuktur kommt!
Chancen und Herausforderungen – eine unabhängige Betrachtung



Konnektor im Feld ...Fertig?

.... natürlich nicht. Jetzt beginnt für alle anderen Teilnehmer die Zukunft.

- **Hersteller von TI-Komponenten:**
 - Kontinuierliche Weiterentwicklung von Terminals und Konnektoren
 - Einführung neuer Funktionen und Fachdienste
- **Medizingerätehersteller:**
 - Müssen ihre Systeme in die TI integrieren
 - Betriebs- und Wartungsschnittstellen müssen koexistent zur TI sein
 - Neue Anwendungen sind möglich (Online Steuerung von Wearables, Patient@home)
- **Integrierte Versorgung**
 - Vernetzte Anwendungen müssen auf Interoperabilität mit der TI angepasst und geprüft werden

Ausgangspunkt

- Zunächst werden **zwei Anbieter** am Markt für die Verbindung der Leistungserbringer mit der TI sorgen
 - ✓ Anbieter muss für die Daten- und Betriebssicherheit seiner Installation Gewährleistung übernehmen
- **Aktuell kein geregeltes Verfahren zur Untersuchung der Wirkung der TI auf Bestandssysteme außerhalb der TI und des KV-Safenet**
- **Die gematik bietet wenig Möglichkeiten zur Begegnung mit der TI**
 - ✓ vorwiegend auf die Grundanwendungen der TI optimiert
- **Anbieter von vernetzten Produkten/ Software, zur Unterstützung der integrierten Versorgung, benötigen Zugang zu Testmitteln und Verfahren**
 - ✓ Beratungsleistung zur Bewältigung der viele tausend Seiten starken Dokumentation der TI ist gefragt

Ausgangspunkt

- Man benötigt eine hochverfügbare Test-TI, die für jeden Kunden exklusiv verfügbar sein muss, damit:
 - a) Seine speziellen Konfigurationswünsche nicht auf andere Benutzer übertragen werden
 - b) Seine Manipulationen an den Komponenten nicht auf andere Benutzer übertragen werden
 - c) Seine Erkenntnisse nicht den Mitbewerbern zugänglich sind

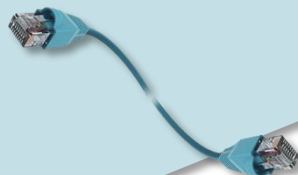
- Als wichtiger Seiteneffekt wird auch die **Interoperabilität** zwischen den Anwendern gefördert und die Spezifikationen von Auslegungsspielräumen befreit

Basis Telematikinfrastruktur



Vernetzte Praxis

Leistungserbringer



Basis Telematikinfrastruktur



Vernetzte Praxis

Leistungserbringer

Telematikinfrastruktur

eHealth
Konnektor

PKI

QES

VSDM

Service &
Maintenance

Zentrale Dienste

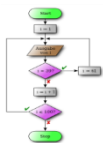
End-to-End Security?

Welche Enden müssen betrachtet werden?



Geschäftsverbindungen:

Kunde – Dienstleister – Zahlungsmittel



Geschäftsvorfälle:

Kartenadministration -
Aktualitätsprüfung/Update



Infrastruktur:

Komponenten, Datenleitungen, etc.

Zertifikate

X509 PKI -
eGK/HBA/
SMC-B

CVC PKI -
eGK/HBA/
SMC-B
gSMC-K/KT

X509 PKI –
gSMC-K/KT

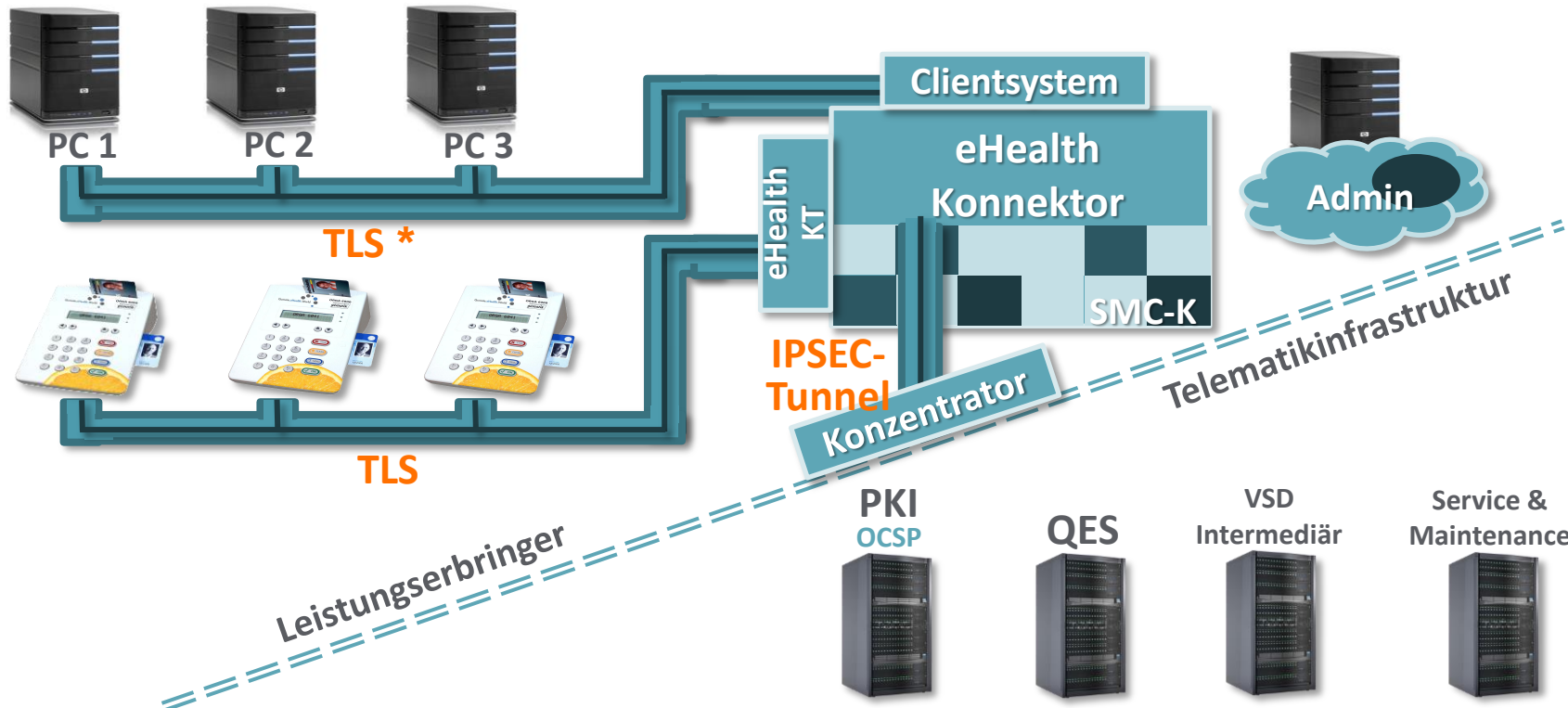
X509 PKI –
Konzentrator
(TI/SIS) -
Dienste

Bedingungen:

- 1) CA MUSS in der TSL sein
- 2) TSL Signatur MUSS mit dem x509 Zertifikat:
DF.Sicherheitsanker / EF.C.TSL.CA_1 der
gSMC-K verifiziert werden können

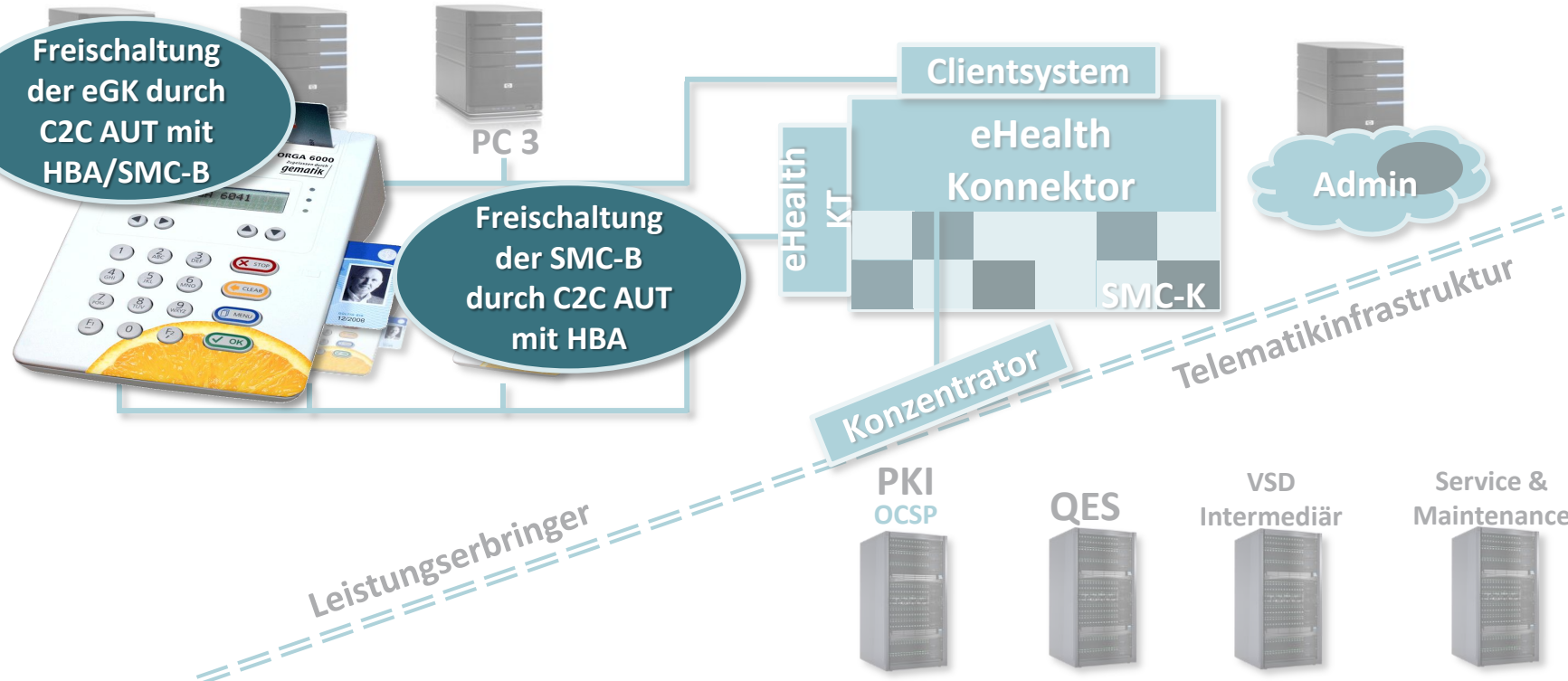
Basis Telematikinfrastruktur - Stufe 1 (BTI-S1)

Grundsicherung Kommunikation



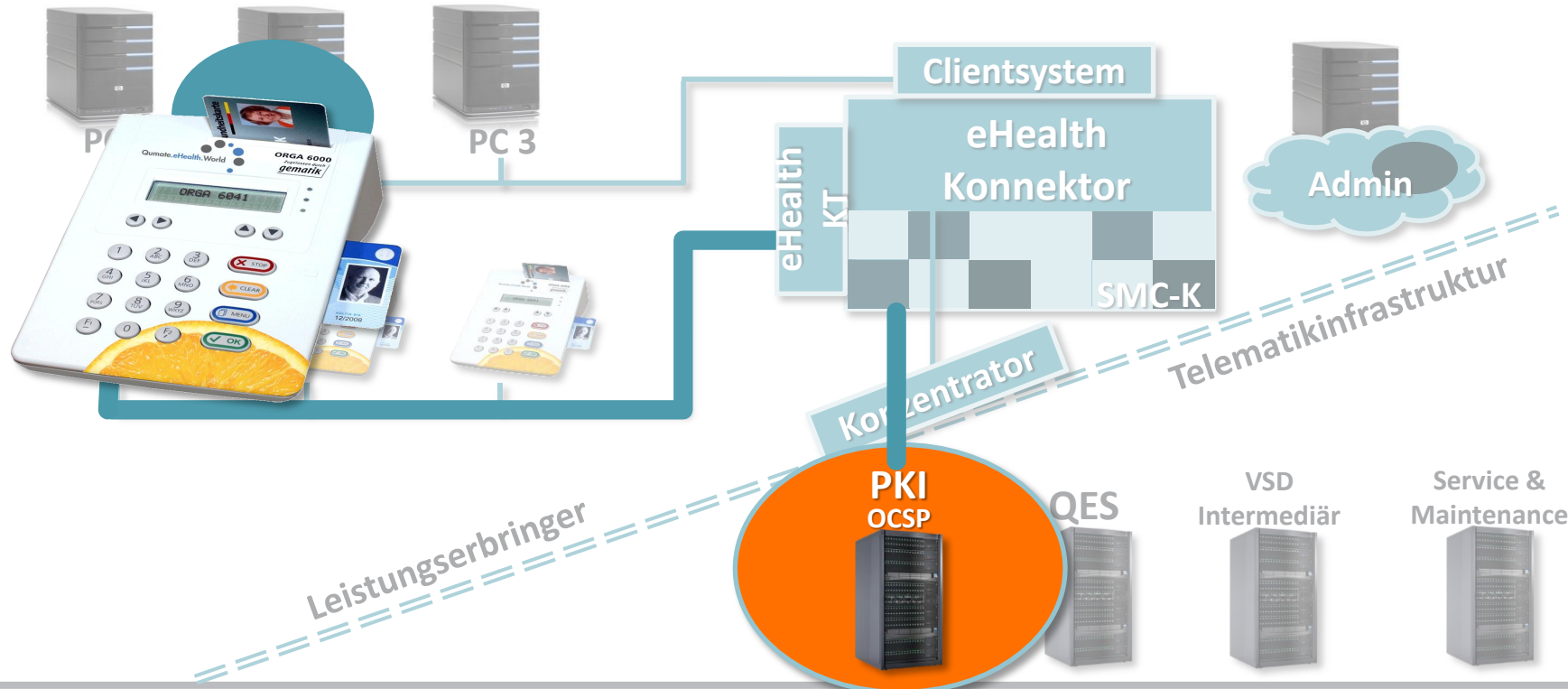
Basis Telematikinfrastruktur - Stufe 1 (BTI-S1)

Grundsicherung Kartenauthentizität



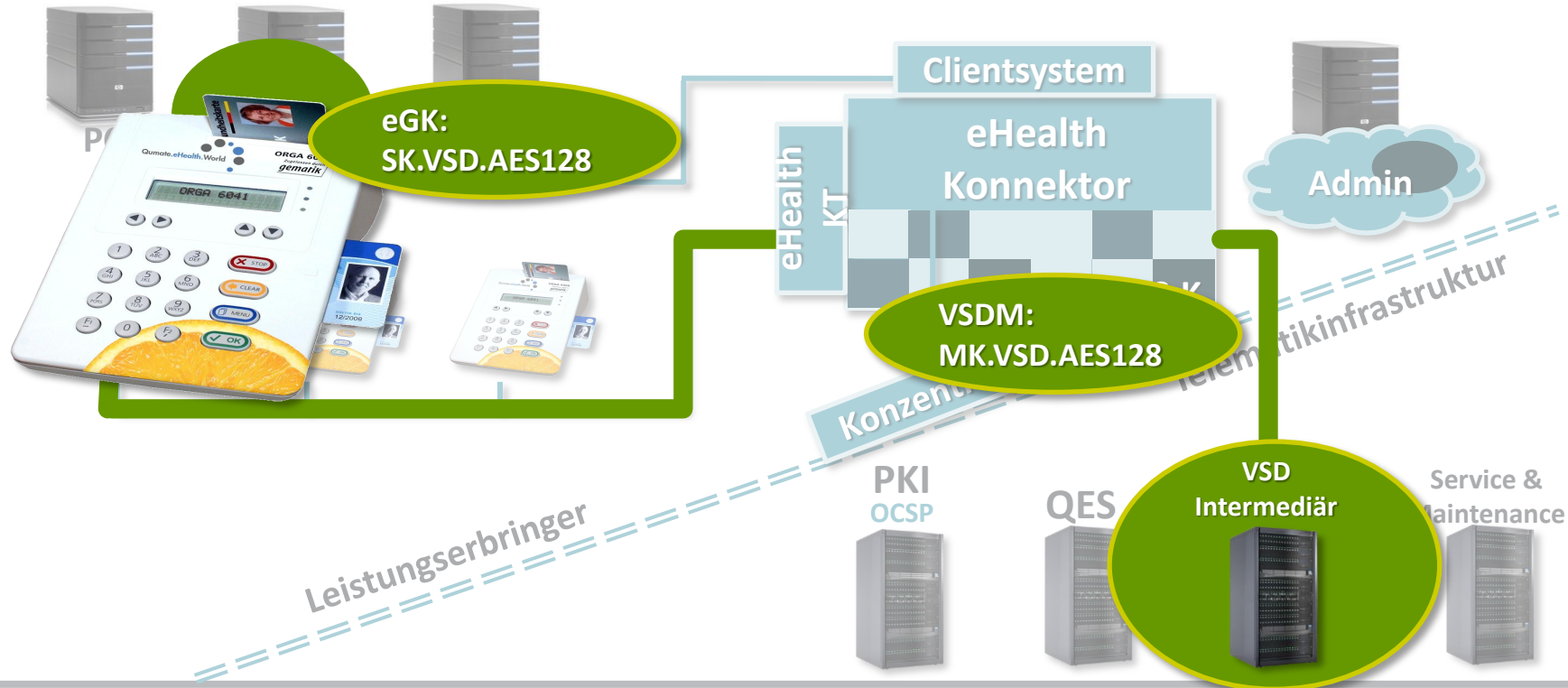
Basis Telematikinfrastruktur - Stufe 1 (BTI-S1)

Grundsicherung Kartengültigkeit



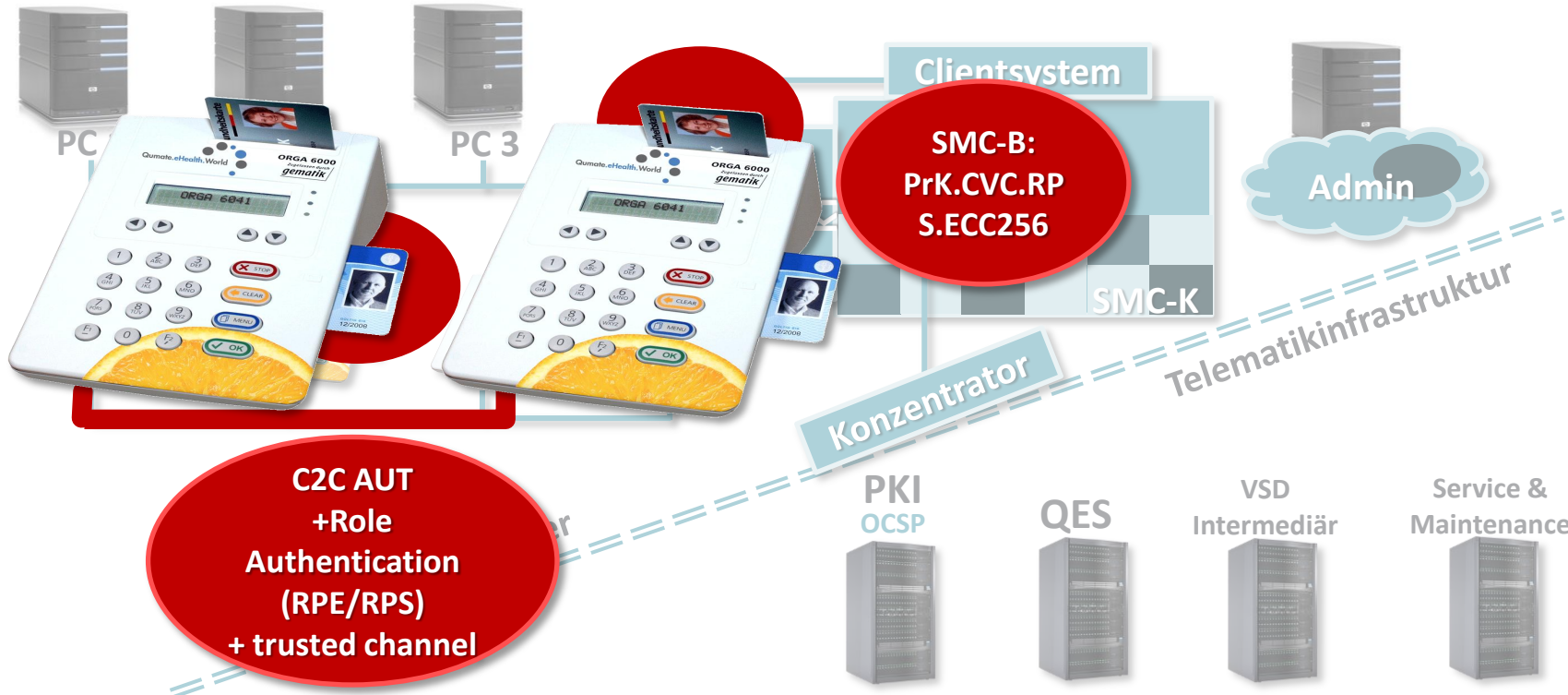
Basis Telematikinfrastruktur - Stufe 1 (BTI-S1)

Grundsicherung VSDM – Update



Basis Telematikinfrastruktur - Stufe 1 (BTI-S1)

Grundsicherung Remote-PIN



Basis Telematikinfrastruktur - Stufe 1 (BTI-S1)

Grundsicherung Remote-PIN



Qumate.eHealth.World – 2018

achelos beabsichtigt, mit Partnern aus Forschung und Industrie ein **Interoperabilitätslabor** zu errichten

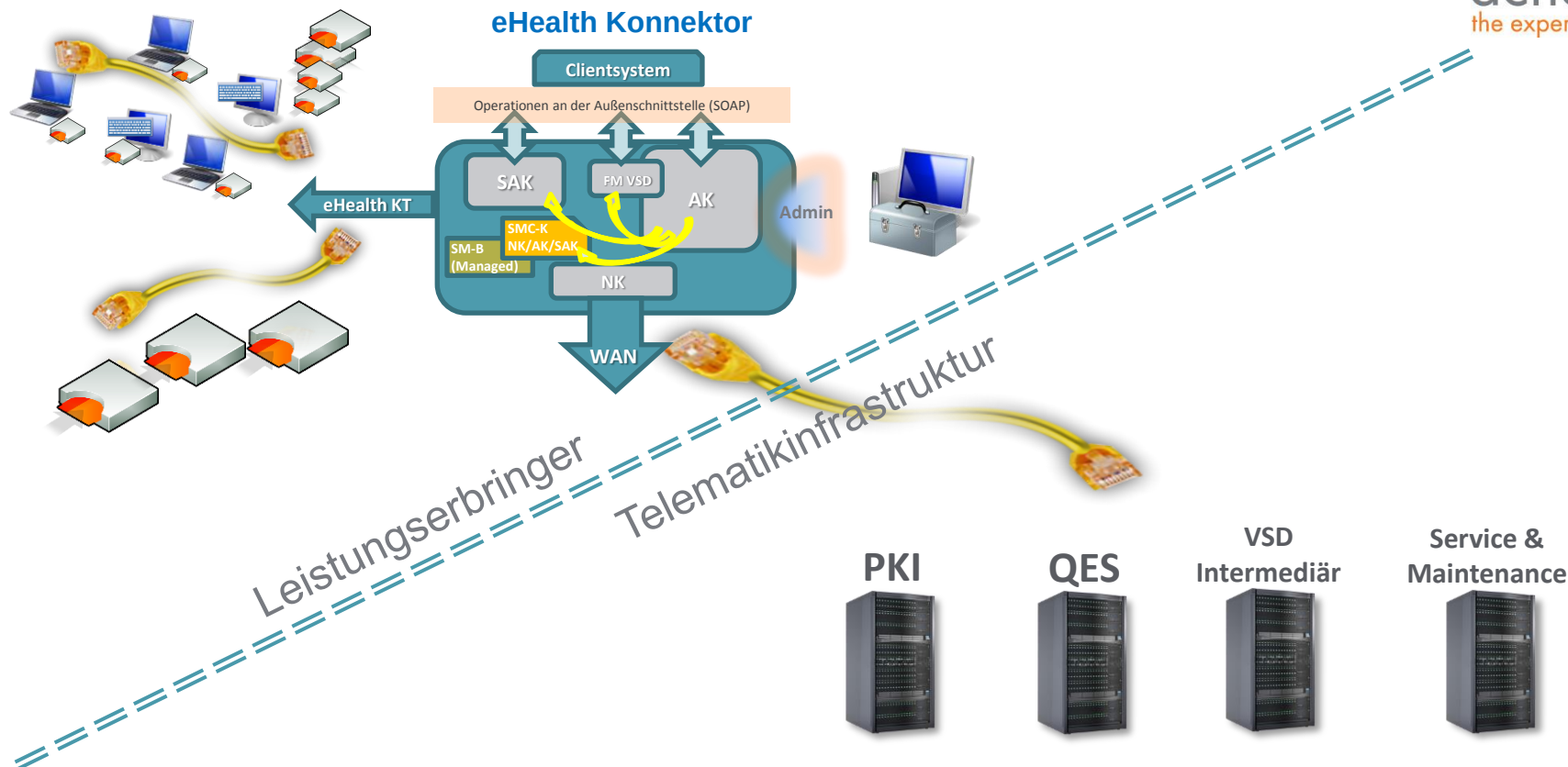
Warum?

1. Weil die TI nicht auf „der grünen Wiese“ errichtet wird, sondern in ein gewachsenes Feld gebaut wird
2. Weil Vernetzung dem Leistungserbringer nur hilft, wenn seine Funktionen verlässlich sind
3. Weil es derzeit kaum möglich ist, die TI im Entwicklungslabor verfügbar zu haben
4. Die Koexistenz von vernetzten Produkten und Services mit der TI alternativlos ist

Für wen?

- **Hersteller und Betreiber von Komponenten** der TI können aus dem Qumate.eHealth-Portfolio von achelos die für ihren Testbedarf benötigten Komponenten und Module auswählen und benutzen
- **Softwarehersteller** können sich eine eigene Simulation der TI verfügbar machen. Damit sind entwicklungsbegleitende Tests und Anpassungen an den Betrieb ihrer Produkte im Zusammenspiel mit der TI möglich
- Ein **Umfassendes Beratungsangebot**, basierend auf detailliertem Wissen über alle Komponenten und Schnittstellen der TI, rundet das Angebot ab.
- achelos bietet jedem Kunden, der der Qumate.eHealth.World - Community beitrifft, eine **Vielzahl von Werkzeugen und Testmitteln** an, mit denen man sein Produkt entwickeln und testen kann. Alle Werkzeuge sind im **Umfeld des ORS-1** entstanden und verwendet worden. Alle achelos Produkte werden mit den **Releases der gematik** aktuell gehalten

Basis Telematikinfrastruktur - Stufe 1 (BTI-S1)





Testsuite Host



Testsuite.Konnektor

Eine eigene TI für jeden!



achelos
the experts in eID

LAN-Simulation



Sim Server

DNS/DHCP

10.60.4.0/24
Steuerungsnetzwerk

Proxy

10.60.5.0/24
Steuerungsnetzwerk

WAN-Simulation

TI-Konzentrator

DNS Server
(Master)
<ltest.>

Hash&URL-
Server

Registration
Service

VPN Server

CRL/TSL
Download

VSDM
Intermediate

Offene FD
172.30.0.0/24

NTP

OCSF

KSR

VSDM
Fachdienst

CCS

VSDM

VSDM

UFS

Nameserver

DNS Server
(Master)
<lekr-test.>

Bestandsnetz

Internet
10.50.0.0/24

Remote
Management

VPN Server

SIS-Konzentrator

DNS Server

Router

DHCP Server

DNS Server

Config Switch
Parallel/serial

Konnektor

LAN

WAN

eHealth Card Terminal
Simulation

virtual.card.kit
Simulation

hta
[HBA 1]
[SMCB-1] [gSMC-KT A]
KVK

ktb
[HBA 2]
[SMCB-2] [gSMC-KT B]
KVK

ktc
[gSMC-KT C]
KVK

- Simulated network of the „Konnektor“ simulation (virtualized)
- Controlling network of the simulation (virtualized)

Testsuiten für Komponenten und Schnittstellen

Auf Basis des **Qumate.eHealth.Testcenters** werden je nach Produkt folgende Testsuiten angeboten:

- Qumate.eHealth.**Konnektor**: Testfälle für den eHealth-Konnektor
- Qumate.eHealth.**Kartenterminal**: Testfälle, die Kartenterminals testen
- Qumate.eHealth.**mobKT**: Testfälle, die mobile Kartenterminals testen
- Qumate.eHealth.**Card**: Testfälle für die Prüfung von Kartenbetriebssystemen
- Qumate.eHealth.**PS**: Testfälle um ein Primärsystem zu testen
- Qumate.Security.**vpn**: Testfälle für die Sicherheitsprotokolle der ISO/OSI Schicht 3 und 4: TLS (Client und Server, IKE/IPsec)

Ergänzende Produkte und Dienstleistungen

Um die Testdurchführung weiter zu automatisieren, können verschiedene Komponenten als Simulation geladen und aus dem Testfall konfiguriert werden

- eHealth-Terminal-Simulation
- COS-Simulation - Software
- COS-Simulation - für Hardware (Kelle)
- Handhabung von Image-Sammlungen für Objektsysteme, die auf dem gematik-COS basieren
- Intermediär-Simulation (mit allen nachfolgenden Services zum VSDM)
- TI-Konzentrator-Simulation
- PKI-Komponenten
- Tools zur Anfertigung von richtigen und fehlerhaften Zertifikaten (CVC und x509, ECC und RSA)
- Man-in-the-middle features zur Überwachung von TLS-Verbindungen

- **achelos entwickelt Software für verschiedenste Produkte**
 - Sicherheitsmodule und Middleware für Smart Card Anwendungen
 - Smart Card Operating Systems
 - Firmware für eHealth-Kartenterminals
 - PKI Komponenten und Kryptofunktionen

- **Common Criteria ist unser Geschäft**
 - Lassen Sie uns Ihre CC-Dokumentation planen und erstellen
 - Wir dokumentieren und liefern Tests und Protokolle für die Zertifizierung

We provide end-to-end security for your business!



achelos GmbH

Christof Basener
Vattmannstraße 1
33100 Paderborn

Christof.Basener@achelos.de

www.achelos.de