



Aufbau einer hoch sicheren eHealth-Infrastruktur in Baden- Württemberg

Jörg Stadler, Jens Urmann

eHealth Infrastructure Product House

eco Arbeitskreis Sicherheit, Köln,
06.05.2009

05.05.2009 12:01

Cracker fordern 10 Millionen US-Dollar für Patientendatenbank

Kriminelle sollen **US-Medienberichten[1]** zufolge die Daten von 8 Millionen amerikanischen Schmerzpatienten vom Server des Virginia Prescription Monitoring Program gestohlen haben und nun 10 Millionen US-Dollar Lösegeld fordern. Der Server dient Ärzten zur Überwachung der Herausgabe von Rezepten für Schmerzmittel wie Opiate und soll den Drogenmissbrauch verhindern.

Nach Angaben von Brian Krebs von der Washington Post drangen die Kriminellen auf unbekanntem Weg in den Server ein, verschlüsselten die Daten, löschten die Originale anschließend auf dem Server und hinterließen den Erpresserbrief. Dieser wurde auch auf **Wikileaks[2]** veröffentlicht:

```
"I have your shit! In *my* possession, right now, are 8,257,378 patient records and a total of 35,548,087 prescriptions. Also, I made an encrypted backup and deleted the original. Unfortunately for Virginia, their backups seem to have gone missing, too. Uhoh :(For $10 million, I will gladly send along the password."
```

Der Server ist derzeit nicht mehr erreichbar. Nach Angaben des Virginia's Department of Health Professions sind die Ermittlungsbehörden bereits eingeschaltet.

(**dab[3]**/c't)

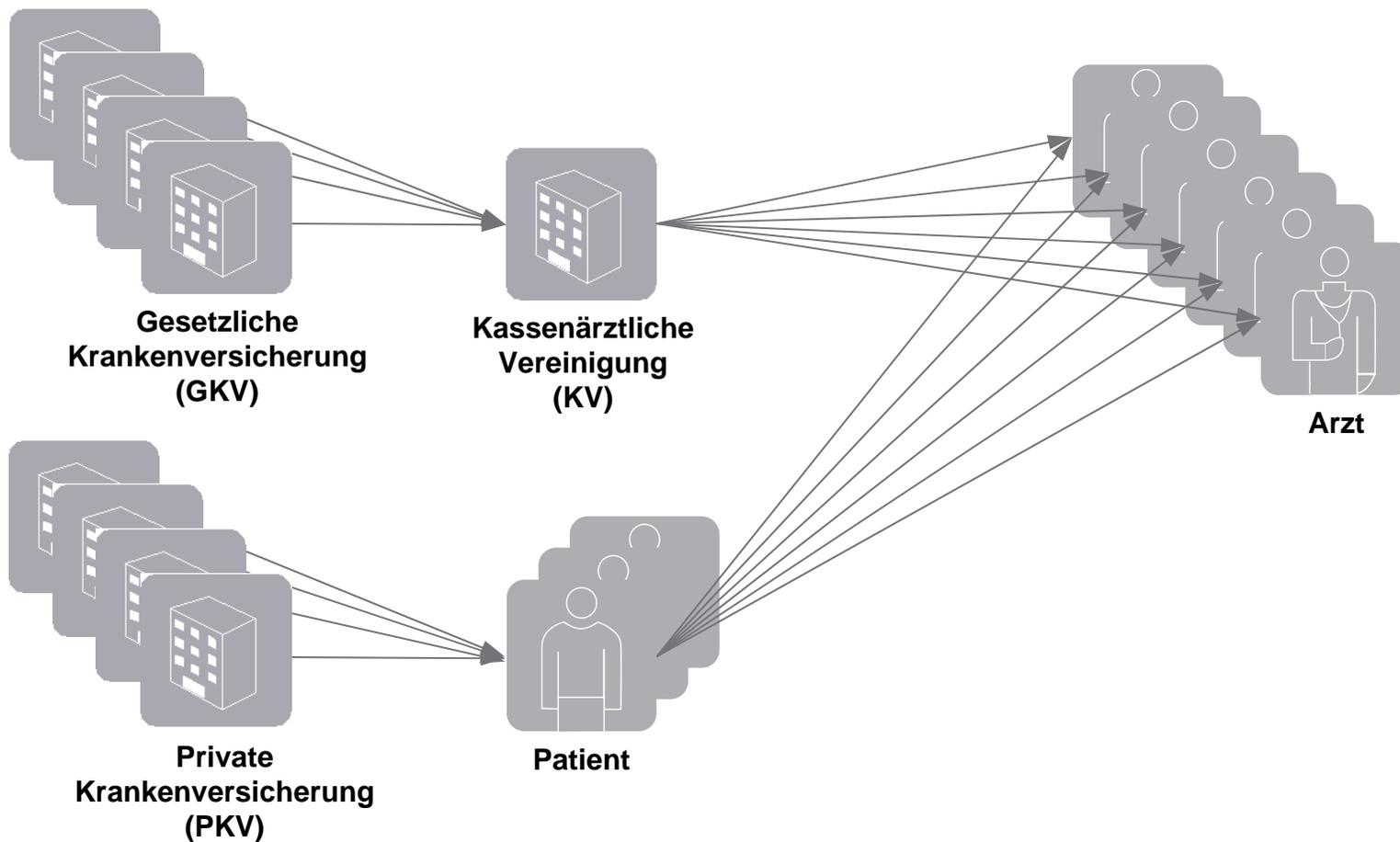
Agenda

1. Grundlagen - Vergütungssystem der niedergelassenen Ärzte
2. Hausarztzentrierte Versorgung (HZV) - Motivation und Ziele
3. Ausbau der Infrastruktur - Weitere Anwendungen
4. Sicherheitsfunktionen der HZV-Infrastruktur
5. ICW Healthcare Connector
6. HZV-Infrastruktur - Telematik-Infrastruktur der gematik
7. Lessons Learned

Agenda

1. Grundlagen - Vergütungssystem der niedergelassenen Ärzte
2. Hausarztzentrierte Versorgung (HZV) - Motivation und Ziele
3. Ausbau der Infrastruktur - Weitere Anwendungen
4. Sicherheitsfunktionen der HZV-Infrastruktur
5. ICW Healthcare Connector
6. HZV-Infrastruktur - Telematik-Infrastruktur der gematik
7. Lessons Learned

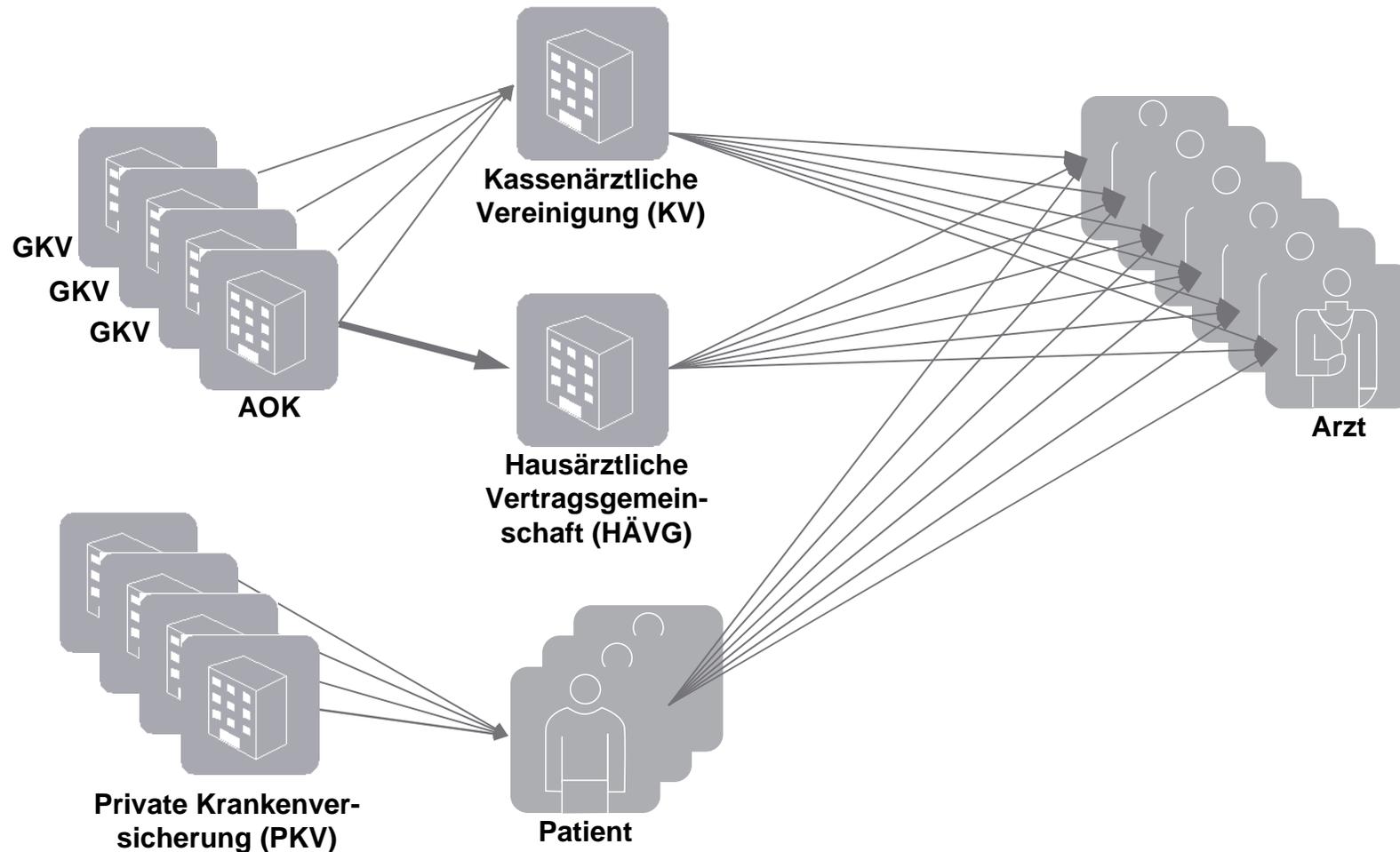
Abrechnung von ambulanten und medizinischen Leistungen vor dem 01.07.2008



§ 73b SGB V – Hausarztzentrierte Versorgung (HZV)

- Die Krankenkassen haben ihren Versicherten eine besondere hausärztliche Versorgung (hausarztzentrierte Versorgung) anzubieten.
- Für den teilnehmenden Arzt bedeutet dies:
 - Eine Sicherstellung von Qualitätskriterien
 - Eine höhere Vergütung als von der KV
- Für den Patienten bedeutet dies:
 - Eine Verpflichtung gegenüber seiner Krankenkasse für mind. 1 Jahr, nur einen selbst ausgewählten teilnehmenden Hausarzt in Anspruch zu nehmen.
 - Fachärzte dürfen nur mit Überweisung vom Hausarzt in Anspruch zu nehmen.
 - Ausgenommen hiervon sind Augenärzte, Frauenärzte, Zahnärzte und Kinderärzte.
 - Eine effektive und effiziente Betreuung durch die zentrale Koordinierungs- und Steuerungsfunktion des Hausarztes.

Abrechnung von ambulanten und medizinischen Leistungen nach dem 01.07.2008 in Baden-Württemberg



Auswirkungen des § 73 b für BW und Bayern

- Das Honorar, welches über die KVen deutschlandweit an die abrechnenden Vertragsärzte in 2007 ausgeschüttet wurde, betrug 25,9 Milliarden €
 - Für Baden-Württemberg beläuft sich der Betrag auf ca. 1,9 Milliarden €
 - Für Bayern beläuft sich der Betrag auf ca. 2,8 Milliarden €
- Durch die Einführung der hausarztzentrierten Versorgung nach § 73b werden in Zukunft ca. 30% – 40% dieser Honorare über Vertragsgemeinschaften an die Ärzte ausgeschüttet.
 - Baden-Württemberg ca.: 700 Mio €
 - Bayern ca.: 1 Milliarde €

Agenda

1. Grundlagen - Vergütungssystem der niedergelassenen Ärzte
2. Hausarztzentrierte Versorgung (HZV) - Motivation und Ziele
3. Ausbau der Infrastruktur - Weitere Anwendungen
4. Sicherheitsfunktionen der HZV-Infrastruktur
5. ICW Healthcare Connector
6. HZV-Infrastruktur - Telematik-Infrastruktur der gematik
7. Lessons Learned

Hausarztzentrierte Versorgung (HZV) - Motivation - Ziele

Ziele der AOK BW

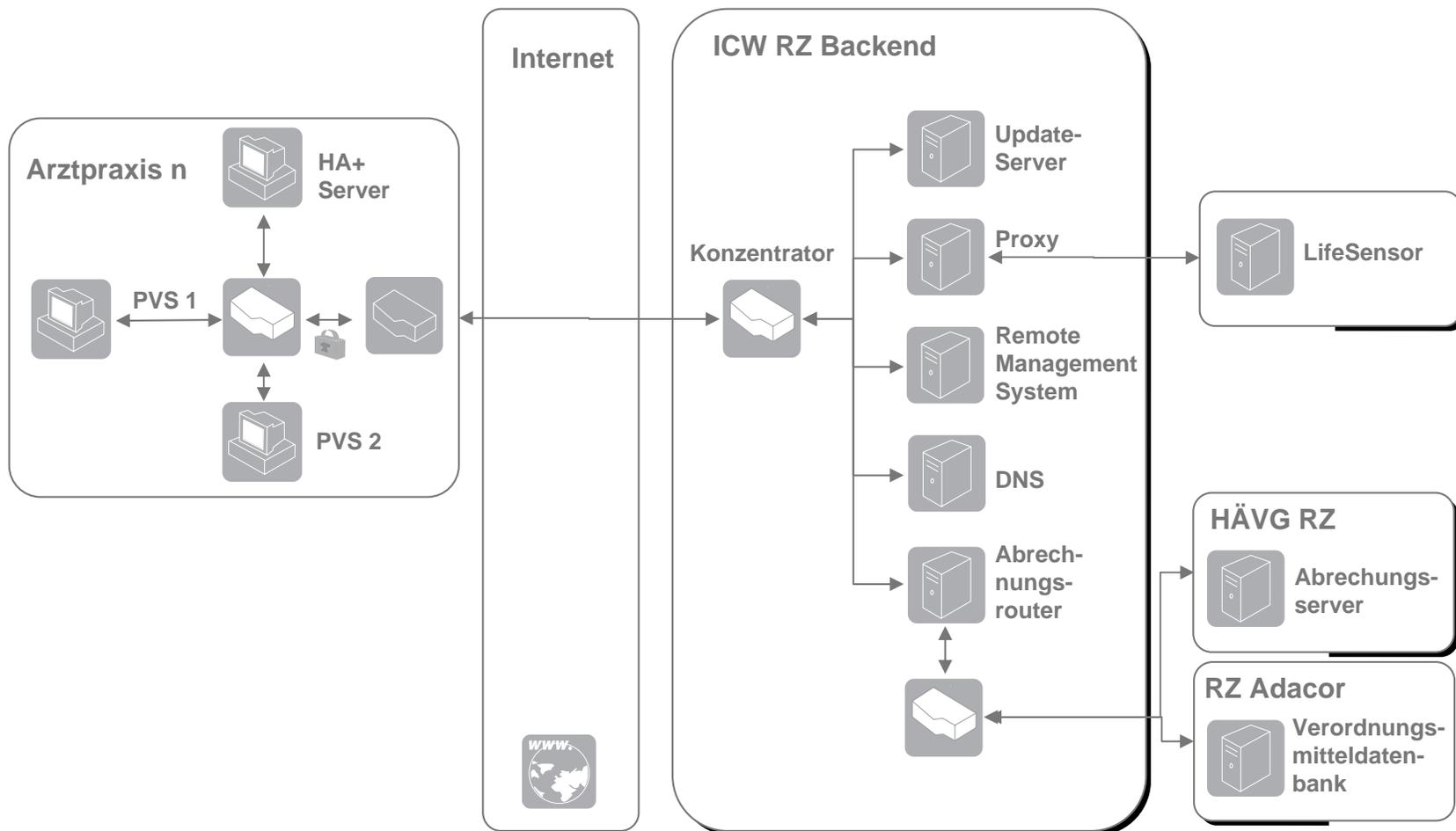
- Eine effektive und effiziente Betreuung des Patienten durch die zentrale Koordinierungs- und Steuerungsfunktion des Hausarztes.
- Die Erfüllung des § 73b

Vertragspartner der HZV

- HZV-Vertragspartner:
 - AOK Baden-Württemberg
 - Hausärztliche Vertragsgemeinschaft eG
 - MEDIVERBUND Dienstleistungs-GmbH

- 951 Arztpraxen sind mittels Healthcare Connector angebunden
- 1.250 Hausärzte arbeiten mit der HZV-Infrastruktur
- 3.000 Hausärzte haben sich angemeldet
- 405.000 Versicherte der AOK sind eingeschrieben

Schematische Darstellung der HZV-Infrastruktur in Baden-Württemberg



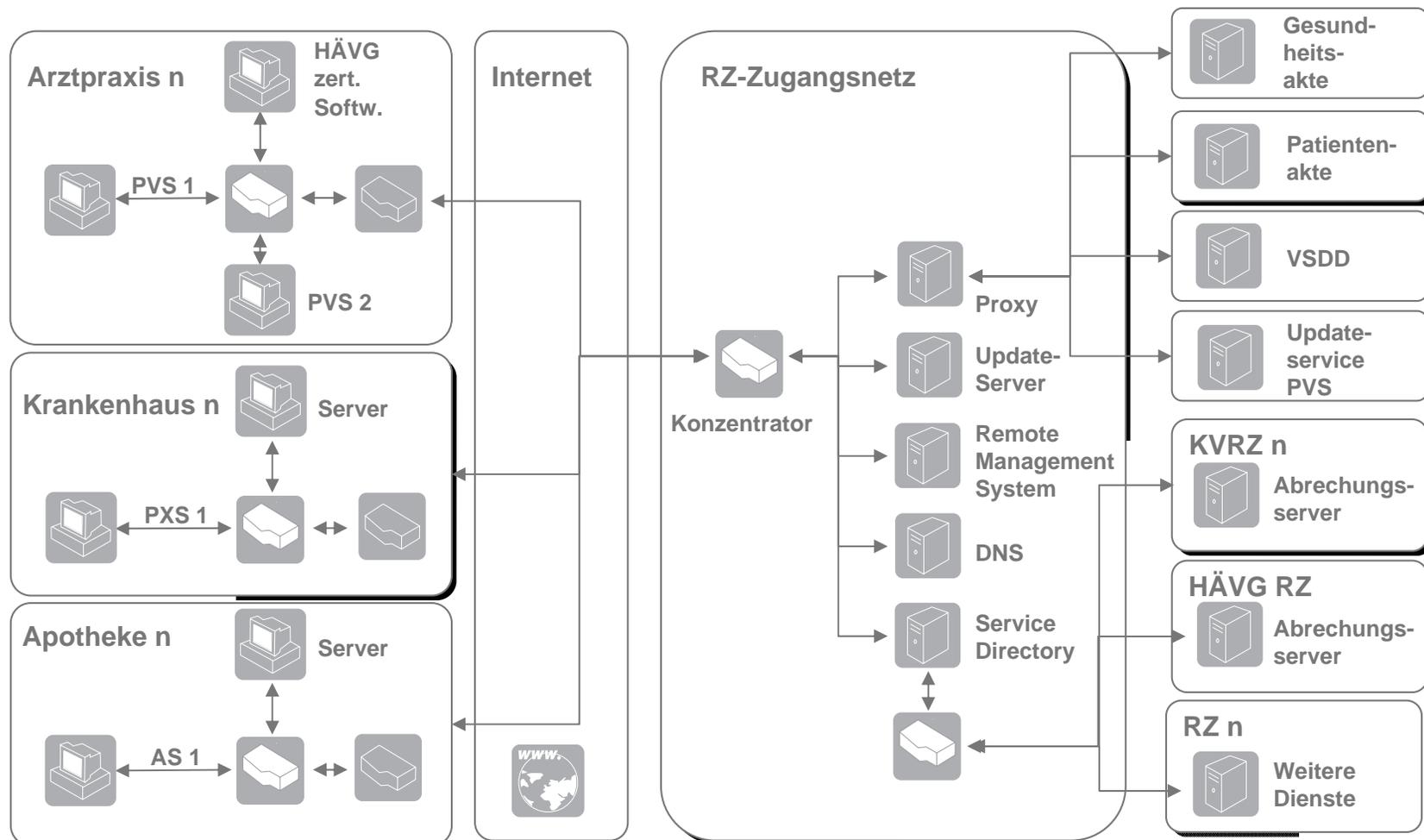
Agenda

1. Grundlagen - Vergütungssystem der niedergelassenen Ärzte
2. Hausarztzentrierte Versorgung (HZV) - Motivation und Ziele
3. Ausbau der Infrastruktur - Weitere Anwendungen
4. Sicherheitsfunktionen der HZV-Infrastruktur
5. ICW Healthcare Connector
6. HZV-Infrastruktur - Telematik-Infrastruktur der gematik
7. Lessons Learned

Next Steps – eHealth-Infrastruktur

- Ausbau der eHealth-Infrastruktur
- Einführung des LifeSensor AOK-Patientenpasses
 - Im Rahmen der freiwilligen Teilnahme an dem Forschungsvorhaben erhalten die Teilnehmer eine kostenfreie LifeSensor Gesundheitsakte: den AOK-Patientenpass.
 - Ziel ist die Erforschung der Auswirkungen einer elektronischen Patientenakte auf
 - das Gesundheitsverhalten der Versicherten
 - die Eigenverantwortlichkeit der Versicherten
 - das Arzt-Patienten-Verhältnis der Versicherten
 - Es können nur Versicherte der AOK teilnehmen, die in das Hausarzt-Programm eingeschrieben sind.
 - Den rechtlichen Rahmen bildet ein Forschungsvorhaben der AOK Baden-Württemberg über einen Zeitraum von fünf Jahren.
- Etablierung weiterer Mehrwertapplikationen, wie die sichere Übertragung von
 - Laborwerten
 - medizinischen Informationen
 -

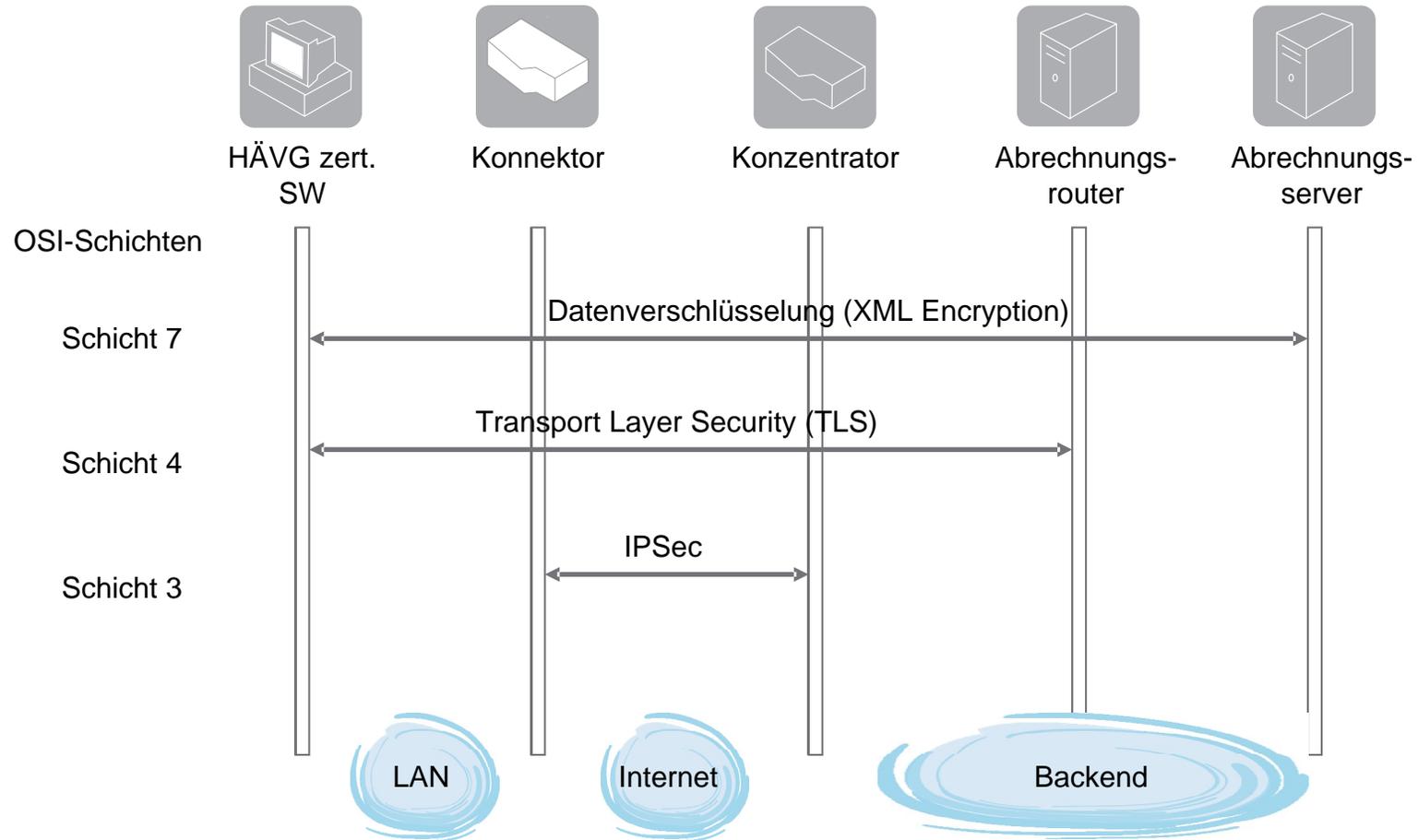
Schematische Darstellung einer neutralen eHealth Infrastruktur



Agenda

1. Grundlagen - Vergütungssystem der niedergelassenen Ärzte
2. Hausarztzentrierte Versorgung (HZV) - Motivation und Ziele
3. Ausbau der Infrastruktur - Weitere Anwendungen
4. Sicherheitsfunktionen der HZV-Infrastruktur
5. ICW Healthcare Connector
6. HZV-Infrastruktur - Telematik-Infrastruktur der gematik
7. Lessons Learned

Übermittlung der Abrechnungsdaten



Sicherheitsfunktionen des Konnektors

- Konform zu gematik Spezifikationen
- IKE v1
- Authentisierung: Digitale Signaturen mit RSA 2048 Bit
- Key Agreement: Diffie Hellman (DH) Gruppe 5
- Verschlüsselung: AES 256 Bit im CBC Mode
- Perfect Forward Secrecy (PFS)
- Layer 2 Tunneling Protokoll (L2TP)

Firewall

- Paketfilter (LAN & WAN)
- Stateful Inspection

- Betreiber: D-Trust
- X.509v3 Zertifikate für Konnektoren & Konzentratoren (IPSec), Konnektoren & Remote Management System (TLS)
- Sperrlisten (CRLs) zum Widerrufen von Zertifikaten

Remote Management System (RMS) für Konnektoren

- Sicherer Kanal zwischen RMS und ICW Healthcare Connector
 - TLS-Kanal mit Client & Server Authentisierung
- Software Updates
 - Update der Konnektor-Software (feingranular)
 - Updates werden signiert & verschlüsselt verteilt
- Konfiguration
- Sichern von Log-Dateien
- Monitoring
 - Prozesse
 - Verbindungen
- ...
- Remote Management reduziert Total Cost of Ownership (TCO)!

Agenda

1. Grundlagen - Vergütungssystem der niedergelassenen Ärzte
2. Hausarztzentrierte Versorgung (HZV) - Motivation und Ziele
3. Ausbau der Infrastruktur - Weitere Anwendungen
4. Sicherheitsfunktionen der HZV-Infrastruktur
5. ICW Healthcare Connector
6. HZV-Infrastruktur - Telematik-Infrastruktur der gematik
7. Lessons Learned

Komponenten des ICW Healthcare Connector

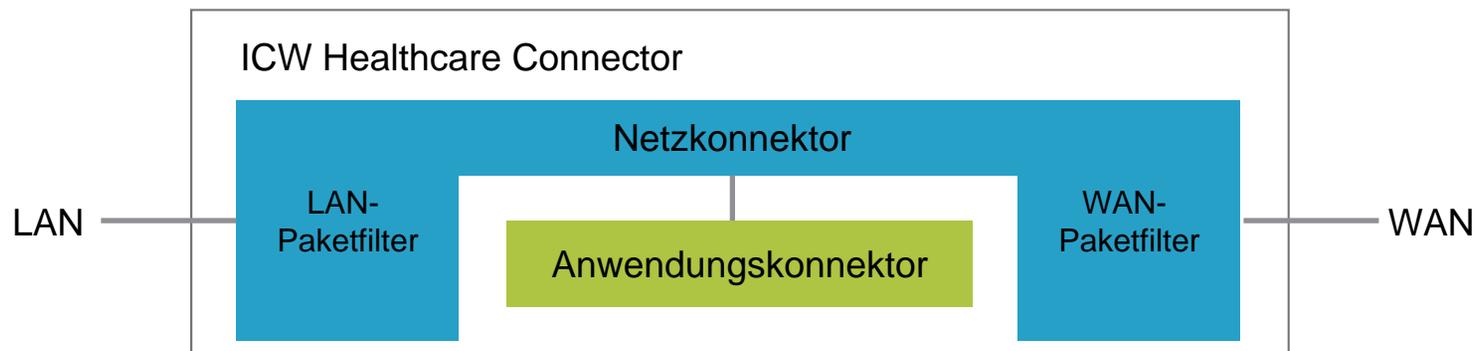
Netzkonnektor

- VPN Client
- Firewall: Paketfilter (LAN und WAN) mit Stateful Inspection
- Partnerprodukt

- Separationsmechanismen

ICW Anwendungs-konnektor

- Anwendungslogik
 - Gematik: Karten-, Kartenterminaldienste, Signaturanwendungskomponente...
- Administrationsschnittstelle (lokal & remote)



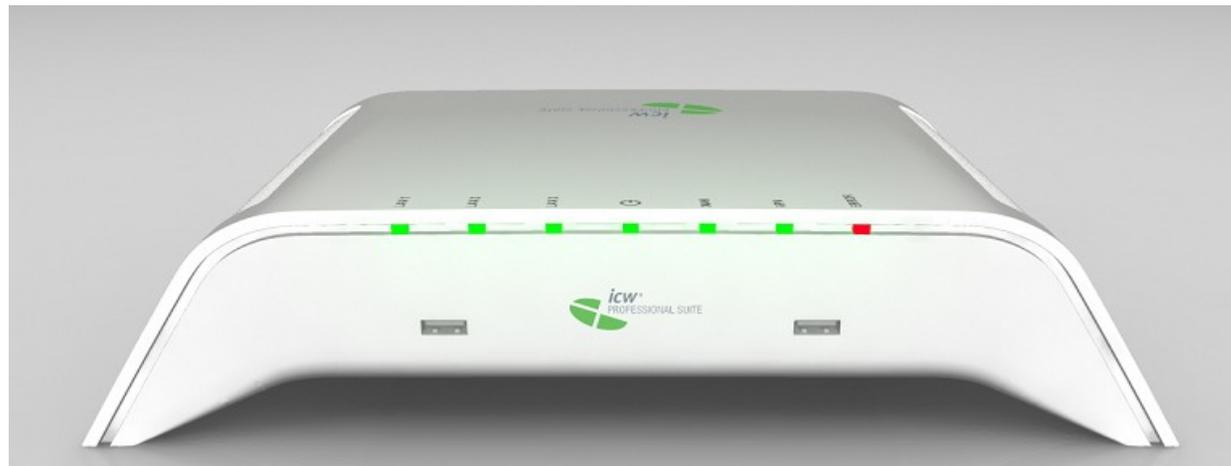
ICW Healthcare Connector based on Cisco AXP

- Hardware: Cisco ISR 1841
- Netzkonnektor: Cisco IOS
- Sicherheit des Cisco IOS untersucht gemäß
 - Common Criteria (CC)
 - FIPS 140-2



ICW Healthcare Connector based on SINA

- ICW Hardware
- SINA Netzkonnektor (NK) der Firma Secunet
- SINA Produkte bis Sicherheitsstufe STRENG GEHEIM zugelassen
- SINA NK in Common Criteria (CC) Evaluierung
 - konform zum BSI Protection Profile (EAL3+)
 - Widerstandsfähigkeit gegen hohes Angriffspotential (AVA_VAN.5)



Agenda

1. Grundlagen - Vergütungssystem der niedergelassenen Ärzte
2. Hausarztzentrierte Versorgung (HZV) - Motivation und Ziele
3. Ausbau der Infrastruktur - Weitere Anwendungen
4. Sicherheitsfunktionen der HZV-Infrastruktur
5. ICW Healthcare Connector
6. HZV-Infrastruktur - Telematik-Infrastruktur der gematik
7. Lessons Learned

Anwendungen in der Telematik-Infrastruktur der gematik

Freiwillige Anwendungen SGB V §291a

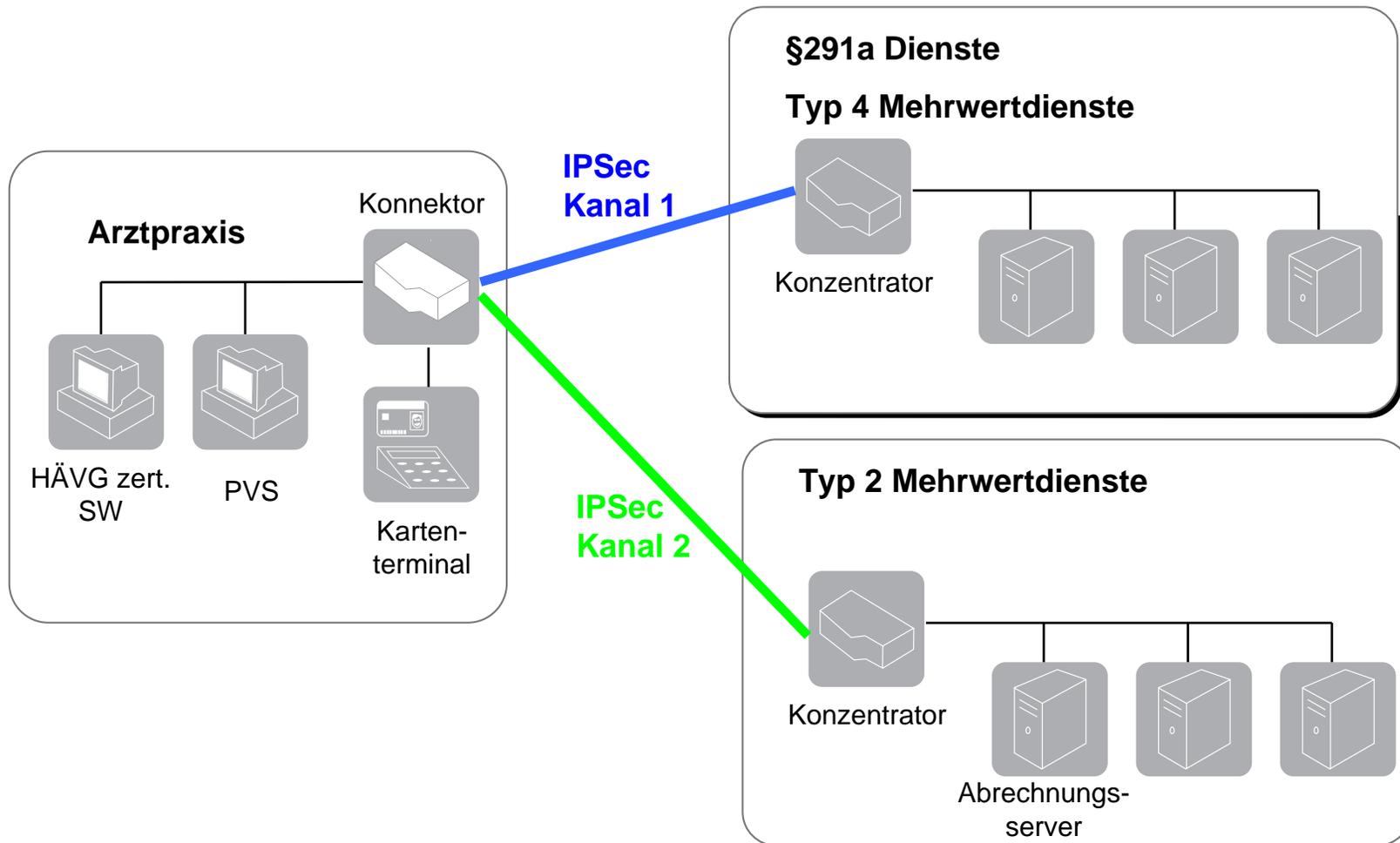
- elektronische Verordnung
- Versichertenstammdaten

- Notfalldaten
- elektronischer Arztbrief
- Arzneimitteltherapiesicherheit
- elektronische Patientenakte
- ...

Mehrwert- anwendungen

- Typ 1: lokale Mehrwertanwendungen
- **Typ 2: Informationstechnisch von der TI getrennte Mehrwertanwendungen**
- Typ 3: Nachnutzung von Infrastrukturdiensten
- Typ 4: Mehrwertanwendungen als Fachanwendungen in der TI

HZV-Infrastruktur als Typ 2 Mehrwertanwendung



Agenda

1. Grundlagen - Vergütungssystem der niedergelassenen Ärzte
2. Hausarztzentrierte Versorgung (HZV) - Motivation und Ziele
3. Ausbau der Infrastruktur - Weitere Anwendungen
4. Sicherheitsfunktionen der HZV-Infrastruktur
5. ICW Healthcare Connector
6. HZV-Infrastruktur - Telematik-Infrastruktur der gematik
7. Lessons Learned

Erfahrungen aus dem Rollout Baden-Württemberg



Total Cost of Ownership (TCO) ist

- durch eine optimale Fernwartbarkeit der Komponenten reduziert
- nicht höher als bei weniger sicheren Soft-VPN-Lösungen



Mögliche Stolpersteine eines Massen-Rollouts wurden identifiziert!

- Terminvereinbarung mit den Leistungserbringern
- Qualifizierung der Servicetechniker bezüglich DSL, ...



Kontakt

InterComponentWare AG

Hauptsitz

Industriestraße 41

69190 Walldorf, Deutschland

Tel.: +49 (0) 6227 385 100

Fax: +49 (0) 6227 385 199

E-Mail: info@icw-global.com

www.icw-global.com