KV TELEMATIK

Ein Tochterunternehmen der
Kassenärztlichen Bundesvereinigung

KV-Connect – sicherer Datenaustausch im SNK

Dr. Mark Schäfer

Workshop
Laborkommunikation
Berlin, 25. Juni 2015

Inhalt

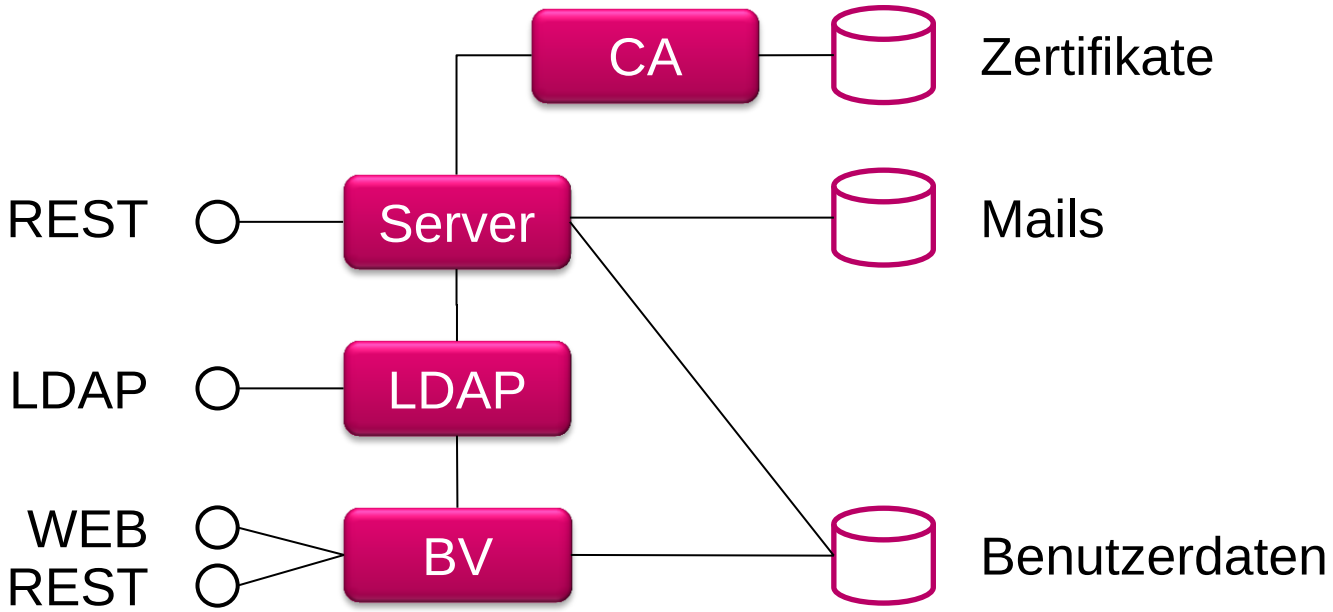
- Überblick über das Gesamtsystem
- Kryptographische Standards
- Benutzerverwaltung
- KV-Connect Client

KV-CONNECT GESAMTSYSTEM

Gesamtsystem

- Das KV-Connect-System ist ausschließlich im SNK verfügbar
  - Keine technischen sondern politische/organisatorische Gründe
- Zwei Referenzsysteme im Internet
  - Ref-1 spiegelt den aktuellen Stand der Produktion
  - Ref-2 spiegelt den zukünftigen Stand
- Alle Verbindungen TLS-Verschlüsselt

KV-Connect Serverseite



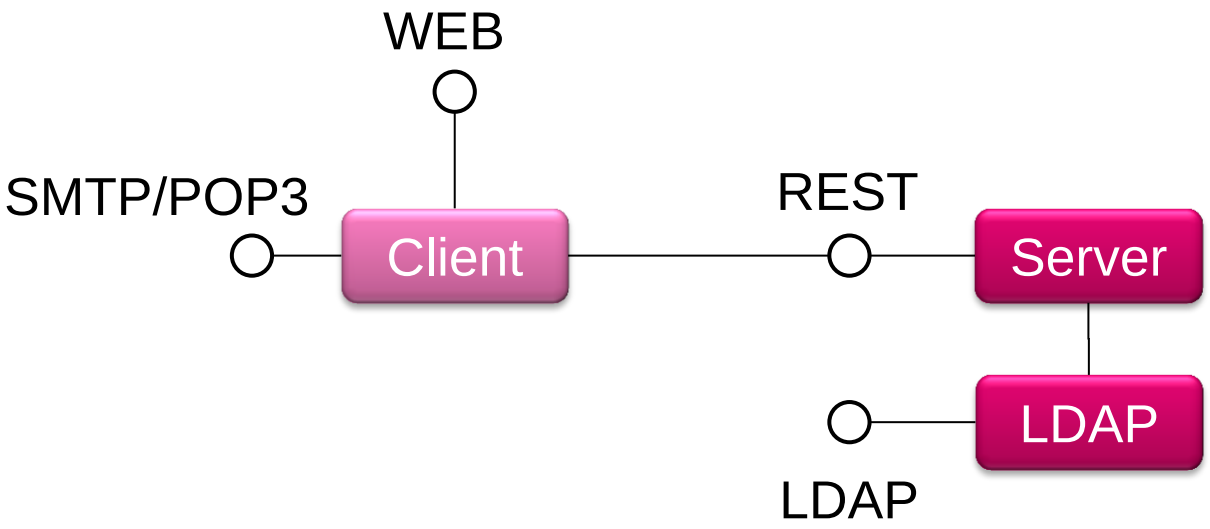
KV-Connect Server

- Fassade für das Gesamtsystem
- Empfänger suchen
- Zertifikate holen
- Konto verwalten
- Zertifikate verwalten
- Mailversand (Senden, Holen, Löschen)

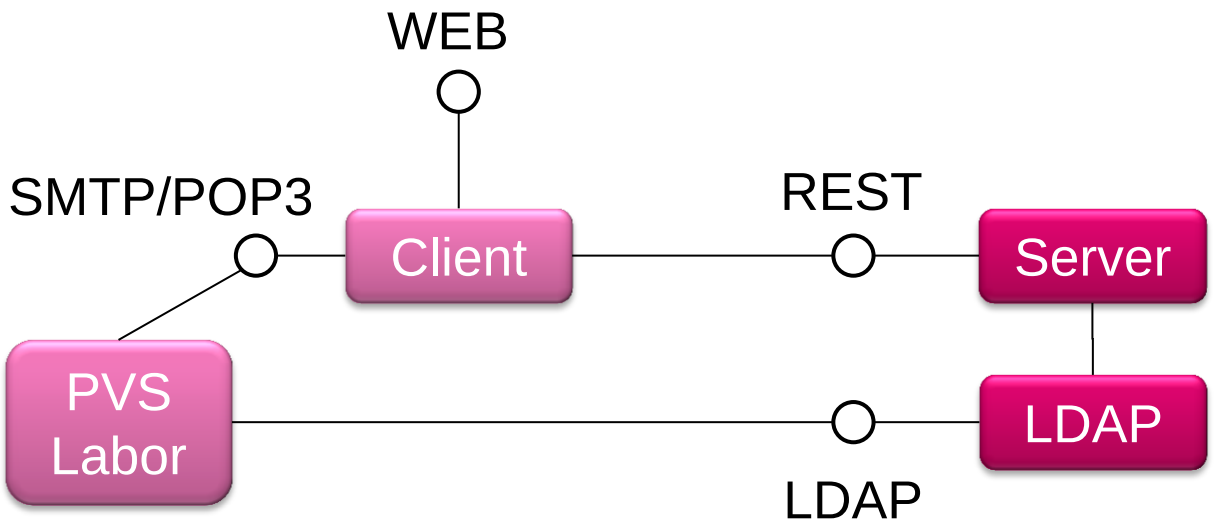
REST-Schnittstelle des Servers

- HTTP wie es mal gedacht war
- REST vs SOAP
  - SOAP: einfach zu implementieren - schwierig zu benutzen
  - REST: schwierig zu implementieren - einfach zu benutzen
- Zustandslose Verbindung, gut parallelisierbar

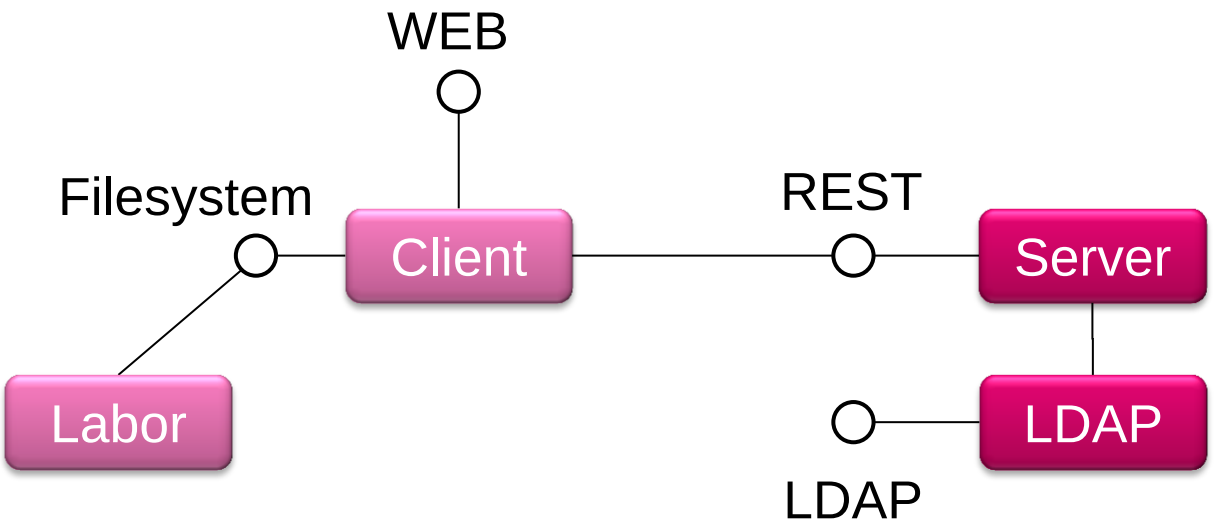
KV-Connect Client



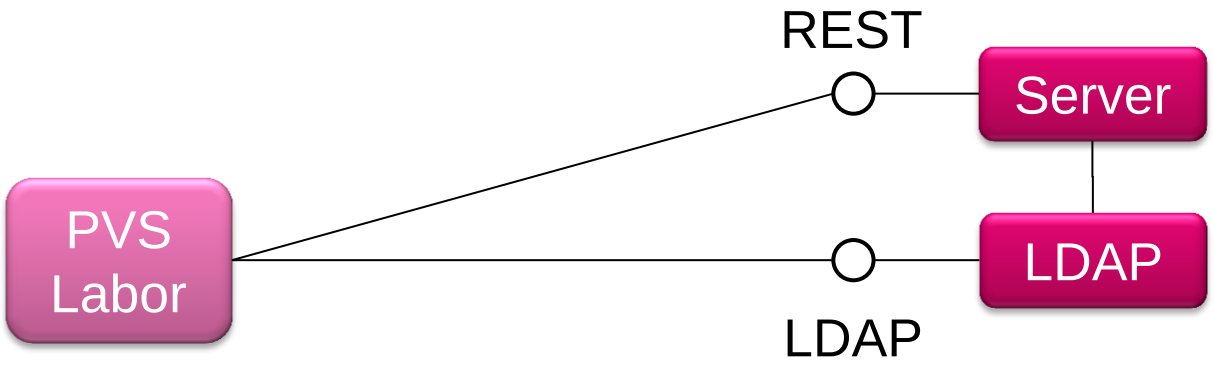
KV-Connect Client mit PVS/Laborsystem



KV-Connect Massenclient im Labor



KV-Connect mit PVS/Laborsystem ohne Client

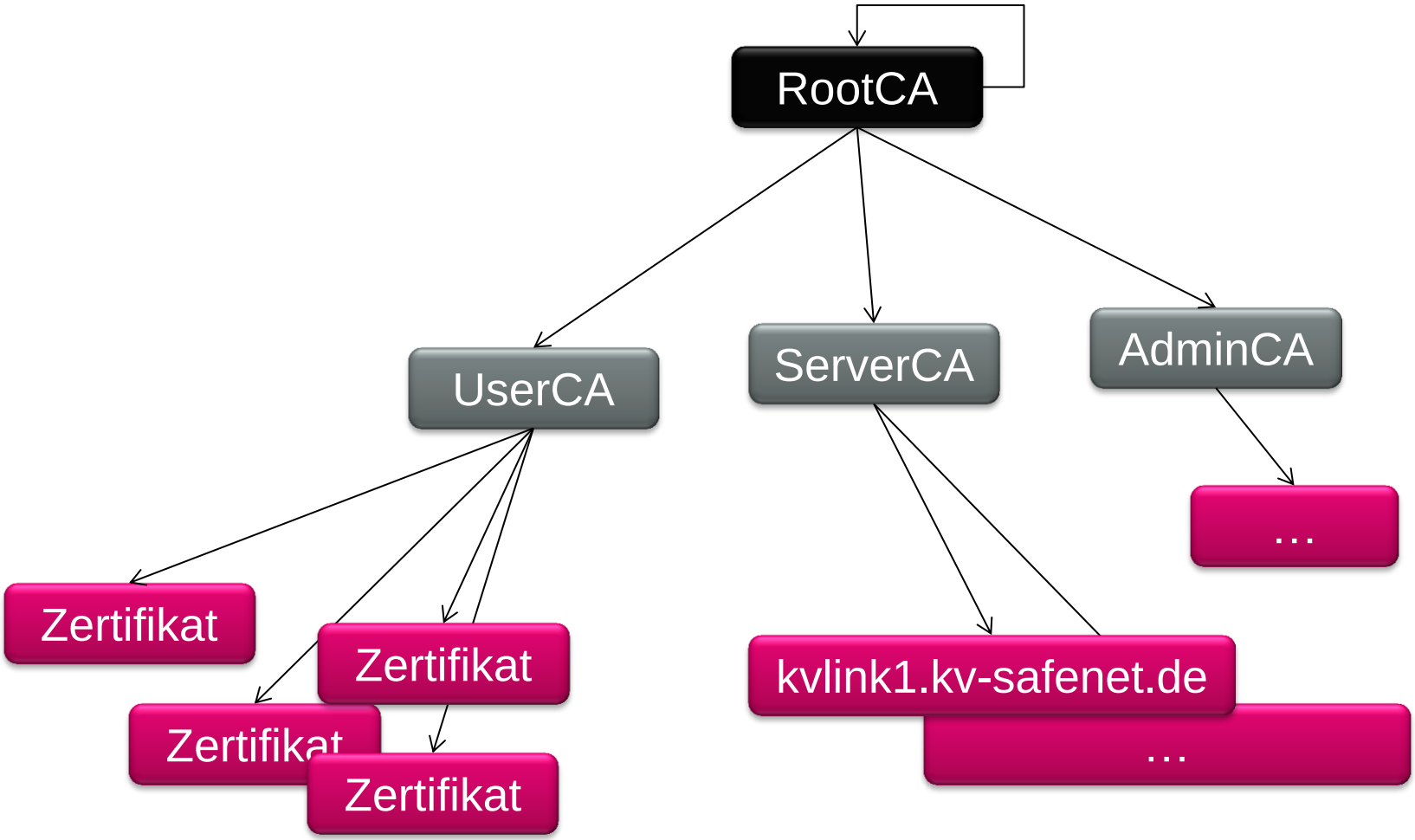


KRYPTOGRAPHISCHE STANDARDS

Zertifikate mit x509

- Standard für das Ausstellen von Zertifikaten
- Enthält den öffentlichen Schlüssel des Eigentümers
- Signiert vom Aussteller
- KV-Connect betreibt eigene Zertifikatshierarchie

Zertifikatshierarchie



S/MIME

- Standard für signierten und verschlüsselten Nachrichtenversand
- Spezielle Form von MIME
- Bei KV-Connnect leicht eingeschränkt (Untermenge von Algorithmen und Formaten)
- Betreff (und andere Header) werden nicht verschlüsselt und signiert

S/MIME

- Schlüsselpaar des Users für Signatur und Verschlüsselung
- Signaturformat: multipart/signed
- Signatur: SHA-256 mit RSA-Encryption
- Verschlüsselungsformat: application/pkcs7-mime
- Verschlüsselung: AES-128-CBC

Ab 2016

- Laufende Kommentierung für Softwarehäuser
- CRLs werden angeboten und müssen benutzt werden
- Expliziter Rückruf von Zertifikaten möglich
- Verschlüsselung mit AES256
- Strikte Cipher-Suites für Server-Anbindung

KV-CONNECT BENUTZERVERWALTUNG

Benutzerverwaltung

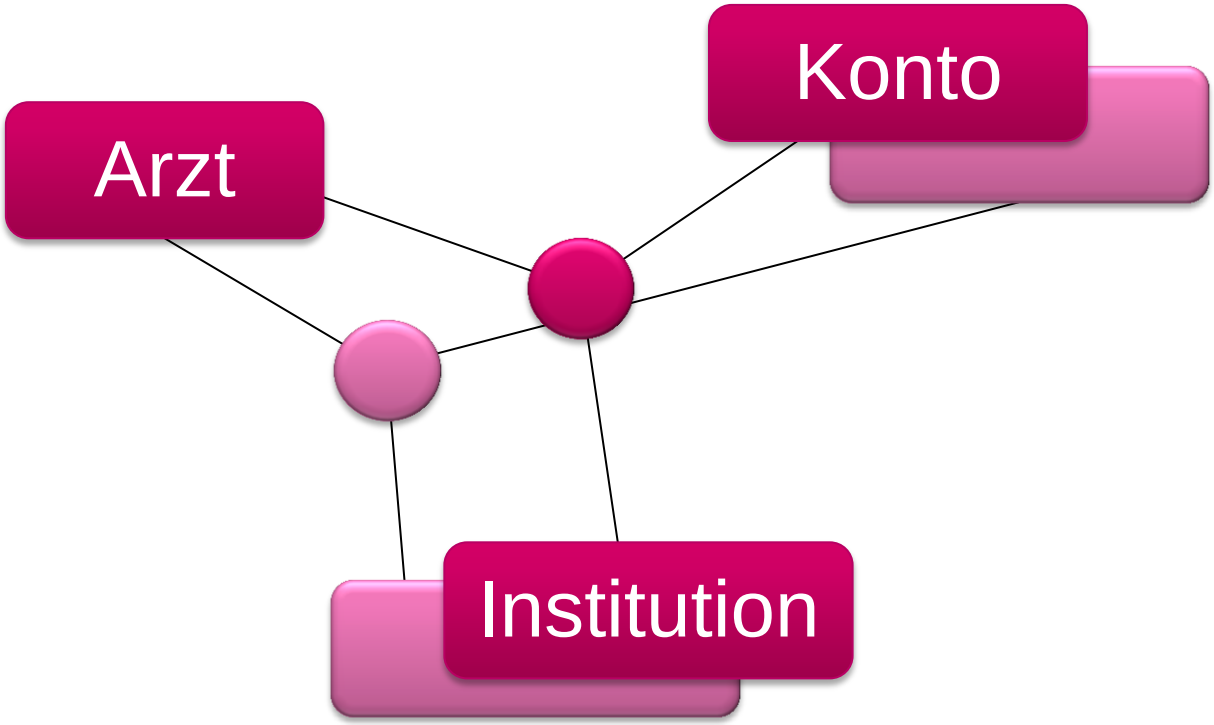
- Eigenentwicklung, mandantenfähig
- Mandanten sind üblicherweise KVen
- KV Telematik hat eigenen Mandanten für spezielle Anwender, z.B. Berufsgenossenschaften

- Verwalter sind Personen, die KV-Connect-Anwender in der Benutzerverwaltung pflegen
- Üblicherweise hat ein Verwalter Rechte für genau einen Mandanten

Objekte der Benutzerverwaltung

- Anwender
  - 99% Ärzte
  - Andere Anwender, z.B. KV-Mitarbeiter
- Organisationseinheiten
  - Praxis
  - MVZ
  - Krankenhaus
  - …
- Konten
  - Ein Konto pro Anwender und Organisationseinheit

Benutzerverwaltung



Verzeichnisdienst - LDAP

- Lightweight Directory Access Protocol
- Standard für die Ablage von „Adressbüchern“
- Name, Adresse etc.
- Zertifikate

- Alternativ: Suche und Zugriff über REST-Schnittstelle des KV-Connect Servers

LDAP

objectClass	***kbvmailPerson (strukturell)***
objectClass	***posixAccount (zusätzlich)***
cn	**mammasoft.bel.kvb**
gidNumber	**1000**
homeDirectory	**/tmp**
mandant	**Ref_eins**
sn	**Pletzer**
uid	**mammasoft.bel.kvb**
uidNumber	**37727**
Arztnummer	5293509
Fachgruppe	170 - FA Pathologie
givenName	Martin
IsLockedOut	FALSE
istArzt	TRUE
l	München
LANR	5293509
mail	mammasoft.bel.kvb@kv-safenet.de
ou	Kassenärztliche Vereinigung Bayerns – MammaSoft
postalCode	80687
street	Elsenheimerstr. 39
unique	594416ae-7b53-43a8-ab4f-dba0a7a29d91@99
userSMIMECertificate	Binäre Daten (1806 Bytes)

DER KV-CONNECT CLIENT

KV-Connect Client

- Hauptzweck
  - Implementierung der Kryptographie-Komponenten
  - Angebot einer Standardschnittstelle
  - Referenzimplementierung
- Zur Installation beim Kunden
  - Einzelplatzbetrieb
  - Lokaler Server
- Modulbasiert (OSGi)
  - Standardclient
  - Massenclient

KV-Connect Client Schnittstellen

- SMTP
  - Simple Mail Transfer Protocol
  - Mailversand
- POP3
  - Post Office Protocol
  - Mail abholen
- Webconfig
  - Passwortänderung
  - Anfordern von Zertifikaten

KV-Connect Client Technik

- KV-Connect Client läuft auf Java 7/8 mit OSGi
- Modulplattform auf Java-Basis
- Anwendung als Sammlung von Bundles
- Kommunikation über definierte Schnittstellen
- Basis für Variabilität des Clients

KV TELEMATIK

Ein Tochterunternehmen der
Kassenärztlichen Bundesvereinigung

Fragen, Anregungen, Hinweise