

# Advanced Aspects of IT-Infrastructures in Healthcare



## ELGA

Vorlesung  
WiSe 2018

Mag. Alexander Stromberger



**INSO - Industrial Software**

Institut für Rechnergestützte Automation | Fakultät für Informatik | Technische Universität Wien

# Vorstellungsrunde

**Mag. Alexander Stromberger**

Mathematik mit Schwerpunkt Informatik (Klagenfurt)

as@pamedo.at

2013 – jetzt: Bundesrechenzentrum

Vorsitzender CISO AG

Architekt/Sicherheitsverantwortlicher eHealth/ELGA

Projektmanager ELGA Berechtigungssystem



2011 – 2013: NextiraOne  
(Contract-M., Escalation-M., Service-Desk, PM Gesundh.)

2007 – 2011: Devoteam Consulting (PM Gesundheitswesen)

2007 – 2013: Freiberuflich (IT, Gesundheitswesen)

2005 – 2007: HBLA Wassermannngasse (Kustos & Lehre)

2002 – 2007: Haus der Barmherzigkeit (IT, Gesundheitswesen)

2001 – 2002: Quant-X (Stratus HA-Server)

2000 – 2001: Elmont IT (IT Manager)

1997 – 2000: Funder Industrie (IT)

1996 – 1997: Universität Klagenfurt (Lektor)

1991 – 1997: Freiberuflich (IT)

Die meisten Inhalte dieser Folien sind öffentlich verfügbar.

Um Ihnen im Zuge der Lehrveranstaltung jedoch tiefergehende Informationen des Aufbaus von ELGA als „Blaupause“ für eine private Cloud geben zu können, wurden diese Folien mit nicht öffentlichen Inhalten ergänzt.

Vielen Dank an das Bundesministerium für Gesundheit und Frauen, die BRZ GmbH und die ELGA GmbH für die Freigabe der ursprünglich als „intern“ eingestufteten Inhalte in vorliegender, modifizierter Form für Lehrveranstaltungen.

# DICOM, HL7, IHE

Kurzeinführung

- **Wie können unterschiedliche Anwendungen Daten austauschen?**
  - Vielzahl von Codierungen möglich
  - Wie kann ich unterschiedliche Datenstrukturen darstellen?
  - Wie repräsentiere ich Datenstrukturen?
  - Wie garantiere ich, dass beide Anwendungen die gleiche Sprache sprechen?
  - Was passiert, wenn ein System z.B. ein neues Datenfeld zur Schnittstelle hinzufügt?
- **Es gibt nicht eine Lösung, sondern viele**
- **In den IT Systemen im Gesundheitsbereich haben sich HL7 und DICOM als Standards etabliert**

## Wikipedia:

*Digital Imaging and Communications in Medicine (DICOM; deutsch Digitale Bildgebung und -kommunikation in der Medizin) ist ein offener Standard zur Speicherung und zum Austausch von Informationen im medizinischen Bilddatenmanagement. Diese Informationen können beispielsweise digitale Bilder, Zusatzinformationen wie Segmentierungen, Oberflächendefinitionen oder Bildregistrierungen sein. DICOM standardisiert sowohl das Format zur Speicherung der Daten, als auch das Kommunikationsprotokoll zu deren Austausch.*

- **Beschränkt sich auf bildgebende Diagnostik und die dafür benötigten Abläufe**

Quelle: [https://de.wikipedia.org/wiki/Digital\\_Imaging\\_and\\_Communications\\_in\\_Medicine](https://de.wikipedia.org/wiki/Digital_Imaging_and_Communications_in_Medicine)

# HL7 v2 – Beispiel

**MSH|^~\&|GHH LAB|ELAB-3|GHH**

**OE|BLDG4|200202150930||ORU^R01|CNTRL-3456|P|2.4<cr>**

**PID|||555-44-**

**4444||EVERYWOMAN^EVE^E^^^L|JONES|19620320|F|||153 FERNWOOD**

**DR.^ ^STATESVILLE^OH^35292|| (206) 3345232| (206) 752-**

**121|||AC55544444||67-A4335^OH^20030520<cr>**

**OBR|1|845439^GHH OE|1045813^GHH**

**LAB|15545^GLUCOSE|||200202150730||||| 555-55-**

**5555^PRIMARY^PATRICIA P^^^^MD^^|F|||||444-44-**

**4444^HIPPOCRATES^HOWARD H^^^^MD<cr>**

**OBX|1|SN|1554-5^GLUCOSE^POST 12H**

**CFST:MCNC:PT:SER/PLAS:QN|^182|mg/dl|70\_105|H|||F<cr>**

- Von “GHH LAB” an “ELAB-3” Nachrichtentyp “ORU^R01”
- PID (Patient Identification) enthält demografische Daten:  
Pat-ID 555-44-4444. Eve E. Everywoman wurde am 20.03.1962 geboren und lebt in Statesville OH.
- OBR (Observation Request) enthält Auftragsinformationen: 15545^GLUCOSE.  
Auftrag erteilt von Patricia Primary MD und durchgeführt von Howard Hippocrates MD.
- OBX (Observation) beschreibt das Ergebnis: 182 mg/dl.

Quelle: [http://www.ringholm.com/docs/04300\\_en.htm](http://www.ringholm.com/docs/04300_en.htm)

- **Wikipedia:**  
*Health Level 7 (HL7) ist eine Gruppe internationaler Standards für den Austausch von Daten zwischen Organisationen im Gesundheitswesen und deren Computersystemen.*
- **Erste Zeile gibt Nachrichtentyp an**
- **Danach werden entsprechend des Nachrichtentyps die Datensegmente übertragen**
- **Sehr kompakte Form der Darstellung**
  - Eigentlich beinhaltet die Struktur fast nur Daten und Trennzeichen
- **Sehr eingeschränkte Kompatibilität**
- **Beinahe unlesbar wenn keine vollständige Beschreibung des Nachrichtentyps vorliegt**
- **Seit der Etablierung von XML verliert HL7 v2 stetig an Bedeutung.**

Quelle: <https://de.wikipedia.org/wiki/HL7>



# HL7 v3 – Beispiel 1/6

```
<POLB_IN224200 ITSVersion="XML_1.0" xmlns="urn:hl7-org:v3"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <id root="2.16.840.1.113883.19.1122.7" extension="CNTRL-3456"/>
  <creationTime value="200202150930-0400"/>
  <!-- The version of the datatypes/RIM/vocabulary used is that of May 2006 -->
  <versionCode code="2006-05"/>
  <!-- interaction id= Observation Event Complete, w/o Receiver Responsibilities -
->
  <interactionId root="2.16.840.1.113883.1.6" extension="POLB_IN224200"/>
  <processingCode code="P"/>
  <processingModeCode nullFlavor="OTH"/>
  <acceptAckCode code="ER"/>
  <receiver typeCode="RCV">
    <device classCode="DEV" determinerCode="INSTANCE">
      <id extension="GHH LAB" root="2.16.840.1.113883.19.1122.1"/>
      <asLocatedEntity classCode="LOCE">
        <location classCode="PLC" determinerCode="INSTANCE">
          <id root="2.16.840.1.113883.19.1122.2" extension="ELAB-3"/>
        </location>
      </asLocatedEntity>
    </device>
  </receiver>
</POLB_IN224200>
```

Quelle: [http://www.ringholm.com/docs/04300\\_en.htm](http://www.ringholm.com/docs/04300_en.htm)

# HL7 v3 – Beispiel 2/6

```
<sender typeCode="SND">
  <device classCode="DEV" determinerCode="INSTANCE">
    <id root="2.16.840.1.113883.19.1122.1" extension="GHH OE"/>
    <asLocatedEntity classCode="LOCE">
      <location classCode="PLC" determinerCode="INSTANCE">
        <id root="2.16.840.1.113883.19.1122.2" extension="BLDG24"/>
      </location>
    </asLocatedEntity>
  </device>
</sender>
<!-- Trigger Event Control Act & Domain Content -->
</POLB_IN224200>
```

```
<controlActProcess classCode="CACT" moodCode="EVN">
  <code code="POLB_TE224200" codeSystem="2.16.840.1.113883.1.18"/>
  <subject typeCode="SUBJ" contextConductionInd="false">
    <!-- domain content has been removed
```

see next section of this whitepaper-->

Quelle: [http://www.ringholm.com/docs/04300\\_en.htm](http://www.ringholm.com/docs/04300_en.htm)

# HL7 v3 – Beispiel 3/6

```
<observationEvent>
  <id root="2.16.840.1.113883.19.1122.4" extension="1045813"
    assigningAuthorityName="GHH LAB Filler Orders"/>
  <code code="1554-5" codeSystemName="LN"
    codeSystem="2.16.840.1.113883.6.1"
    displayName="GLUCOSE^POST 12H CFST:MCNC:PT:SER/PLAS:QN"/>
  <statusCode code="completed"/>
  <effectiveTime value="200202150730"/>
  <priorityCode code="R"/>
  <confidentialityCode code="N"
    codeSystem="2.16.840.1.113883.5.25"/>
  <value xsi:type="PQ" value="182" unit="mg/dL"/>
  <interpretationCode code="H"/>
  <referenceRange>
    <interpretationRange>
      <value xsi:type="IVL_PQ">
        <low value="70" unit="mg/dL"/>
        <high value="105" unit="mg/dL"/>
      </value>
    </interpretationRange>
  </referenceRange>
</observationEvent>
```

Quelle: [http://www.ringholm.com/docs/04300\\_en.htm](http://www.ringholm.com/docs/04300_en.htm)

# HL7 v3 – Beispiel 4/6

```
<author>
<time value="200202150730"/>
<modeCode code="WRITTEN"/>
<signatureCode code="S"/>
  <assignedEntity>
    <id root="2.16.840.1.113883.19.1122.3" extension="444-444-4444"/>
    <assignedPerson>
      <name>
        <given>Harold</given>
        <given>H</given>
        <family>Hippocrates</family>
        <suffix qualifier="AC">MD</suffix>
      </name>
    </assignedPerson>
  </assignedEntity>
</author>
```

Quelle: [http://www.ringholm.com/docs/04300\\_en.htm](http://www.ringholm.com/docs/04300_en.htm)

# HL7 v3 – Beispiel 5/6

```
<recordTarget>
  <patientClinical>
    <id root="2.16.840.1.113883.19.1122.5" extension="444-22-2222"
      assigningAuthorityName="GHH Lab Patient IDs"/>
    <statusCode code="active"/>
    <patientPerson>
      <name use="L">
        <given>Eve</given>
        <given>E</given>
        <family>Everywoman</family>
      </name>
      <asOtherIDs>
        <id extension="AC555444444" assigningAuthorityName="SSN"
          root="2.16.840.1.113883.4.1"/>
      </asOtherIDs>
    </patientPerson>
  </patientClinical>
</recordTarget>
```

Quelle: [http://www.ringholm.com/docs/04300\\_en.htm](http://www.ringholm.com/docs/04300_en.htm)

```
<inFulfillmentOf>
  <placerOrder>
    <id root="2.16.840.1.113883.19.1122.14" extension="845439"
      assigningAuthorityName="GHH OE Placer orders"/>
  </placerOrder>
</inFulfillmentOf>
</observationEvent>
```

Quelle: [http://www.ringholm.com/docs/04300\\_en.htm](http://www.ringholm.com/docs/04300_en.htm)

- **HL7 v3 basiert auf XML und bietet daher eine Möglichkeit, Daten selbstbeschreibend darzustellen.**
- **„Meta-Daten“ und Daten werden gemeinsam dargestellt**
- **Eindeutige IDs notwendig -> OID**
- **Sehr hoher Overhead an „Meta-Daten“**
- **Kompatibilität bei Erweiterungen möglich**
- **Nutzung von XML Schemas (XSD)**
- **Ausgelegt auf die Verwendung von Webservices (WSDL)**
- **Verwendung von Standard-Parsern**

## Wikipedia:

*Integrating the Healthcare Enterprise (IHE) ist eine Initiative von Anwendern und Herstellern mit dem Ziel, den Datenaustausch zwischen IT-Systemen im Gesundheitswesen zu standardisieren und zu harmonisieren. Die Umsetzung der medizinischen Prozessabläufe zwischen den Systemen und die Schaffung von Interoperabilität stehen hierbei im Vordergrund. IHE formuliert dazu Anforderungen aus der Praxis in so genannten Use Cases, identifiziert relevante Standards und entwickelt technische Leitfäden, so genannte Profile, mit denen ein Hersteller sein Produkt umsetzen und testen kann. Beim internationalen "Connectathon" testen die Hersteller ihre Systeme untereinander und bereiten sie auf den Praxiseinsatz vor.*

<http://www.ihe.net>

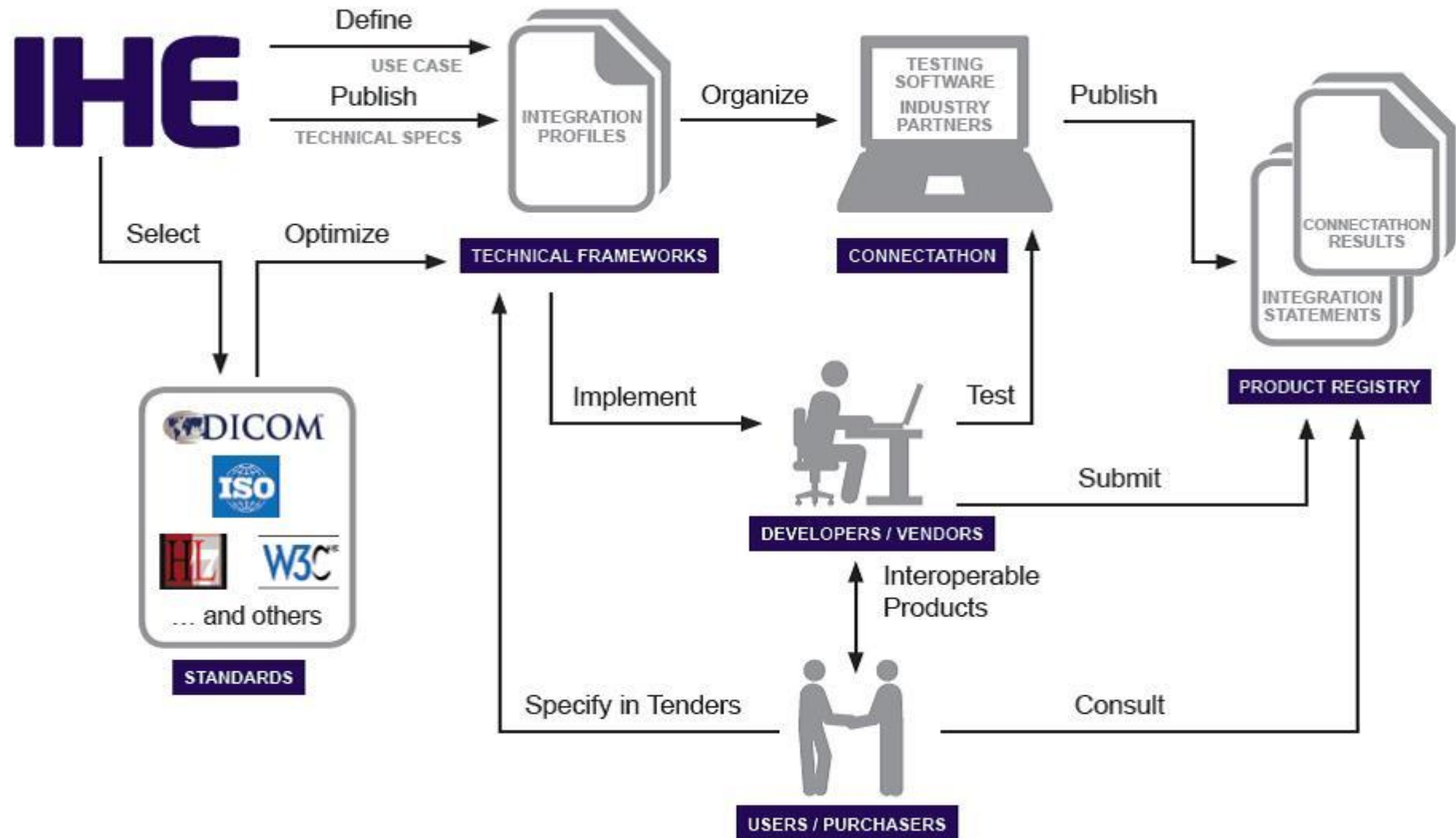
Quelle: [https://de.wikipedia.org/wiki/Integrating\\_the\\_Healthcare\\_Enterprise](https://de.wikipedia.org/wiki/Integrating_the_Healthcare_Enterprise)



- ***IHE brings together users and developers of healthcare information technology (HIT) in an annually recurring four-step process:***
  - 1. Clinical and technical experts define critical use cases for information sharing.***
  - 2. Technical experts create detailed specifications for communication among systems to address these use cases, selecting and optimizing established standards.***
  - 3. Industry implements these specifications called IHE Profiles in HIT systems.***
  - 4. IHE tests vendors' systems at carefully planned and supervised events called Connectathons.***

Quelle: [http://www.ihe.net/IHE\\_Process/](http://www.ihe.net/IHE_Process/)

# IHE – Ablauf



Quelle: [http://www.ihe.net/IHE\\_Process/](http://www.ihe.net/IHE_Process/)

- **IHE committees follow the four-step annual process to address interoperability in a variety of clinical domains:**
  - Anatomic Pathology
  - Cardiology
  - Dental
  - Endoscopy
  - Eye Care
  - IT Infrastructure
  - Laboratory
  - Patient Care Coordination
  - Patient Care Devices
  - Pharmacy
  - Quality, Research and Public Health
  - Radiation Oncology
  - Radiology

Quelle: <http://www.ihe.net>

*IHE Profiles provide a standards-based framework for sharing information within care sites and across networks. They address critical interoperability issues related to information access for care providers and patients, clinical workflow, security, administration and information infrastructure. Each profile defines the actors, transactions and information content required to address the clinical use case by referencing appropriate standards.*

- **Die IHE Profile sind in den IHE Technical Frameworks zu finden und nach IHE Domain aufgeteilt:**
  - [http://www.ihe.net/Technical\\_Frameworks](http://www.ihe.net/Technical_Frameworks)

Quelle: <http://www.ihe.net>

*IHE has been testing the interoperability of healthcare information technology (HIT) systems for more than a decade. At IHE Connectathons held regularly in several locations internationally, trained technical experts supervise testing of vendor systems, making use of advanced testing software developed by IHE and several partner organizations. More than 250 vendors worldwide have implemented and tested products with IHE capabilities.*

- **Die Ergebnisse sind öffentlich zugänglich:**
  - <http://connectathon-results.ihe.net>

Quelle: <http://www.ihe.net>

*The IHE Product Registry provides essential information for IT administrators and executives responsible for purchasing and integrating systems at healthcare sites and health information exchanges. Detailed results of testing at IHE Connectathons over the past several years in Europe, North America and Asia are made available in this easy-to-use online database. These results are cross-linked to IHE Integration Statements- conformance commitments of the IHE capabilities of commercial products-from dozens of vendors worldwide.*

- **Auch diese Datenbank kann online angefragt werden:**
  - <http://product-registry.ihe.net/>

Quelle: <http://www.ihe.net>

# eGov, OLD-Verwaltung, Terminologieserver

Übersicht Hilfssysteme

- **Problemstellung: Wie kann man „Menschen“ eindeutig identifizieren?**
  - in Österreich: Lösung in eGov
    - in Stammzahlenregister (SZR) Daten aus:
      - Zentrales Melderegister (ZMR)
      - Ergänzungsregister für natürliche Personen (ERnP)
- **Problemstellung: Verknüpfung von Daten**
  - Durch eindeutige Identifier lassen sich Daten über verschiedene Domänen verknüpfen...  
Finanzdaten, Gesundheit, Strafregister, ZMR, ....
  - Lösung: Man erstellt für verschiedene Domänen kryptografische Ableitungen der Stammzahl. „bereichsspezifische Personen-Kennung“ (bPK)
  - Beispiele (~30):
    - bPK:SV Sozialversicherung
    - bPK:GH Gesundheit
    - bPK:SA Steuern und Abgaben
  - Diese einzelnen bPKs können nicht zugeordnet werden.
  - Die Weitergabe von fremden bPKs erfolgt verschlüsselt.



## Wikipedia:

*In der Informatik ist ein Object Identifier (OID) ein weltweit eindeutiger Bezeichner, der benutzt wird um ein Informationsobjekt zu benennen (vgl. URN). Ein OID stellt einen Knoten in einem hierarchisch zugewiesenen Namensraum dar, der durch den ASN.1-Standard definiert ist. Jeder Knoten ist durch eine Folge von Nummern eindeutig gekennzeichnet, die seine Position beginnend an der Wurzel des Baumes angibt. Neue Knoten zur eigenen Verwendung können bei den entsprechenden Autoritäten des übergeordneten Knotens beantragt werden. Die Regeln für die Vergabe und Registrierung von OIDs sind festgelegt in den Normen ISO/IEC 9834 und DIN 66334. Die Verwaltung des OID-Baumes und die Sicherstellung der Eindeutigkeit von OIDs beruhen auf der Übertragung der Zuständigkeit für die untergeordneten Knoten an den Besitzer einer OID.*

Quelle: [https://de.wikipedia.org/wiki/Object\\_Identifier](https://de.wikipedia.org/wiki/Object_Identifier)

- **Unicode Label  
(mit der OID verbundener Term)**
- **Beschreibung (zumindest englisch)**
- **Kategorie**
- **Status**
- **Erstell- und Änderungsdatum**
- **Links**
- **Kommentar**
- **Ggf. Attachments**

- **Der OID Baum stellt keine Hierarchie/Klassifikation dar**
  - Aus einem Teil einer OID kann keine Bedeutung abgeleitet werden.
  - Eine OID ist lediglich die Referenz zu einer Beschreibung, welche recherchierbar sein soll.
  - Autorisierte Organisationen (Besitzer einer OID), können unterhalb ihres OID-Knotens weitere OID eigenverantwortlich vergeben
  - Die OID Registration Authority ist für die Eindeutigkeit, Disjunktheit und Richtigkeit verantwortlich.
- **OID Registry**
  - OID Vergabe und Verwaltung (Eindeutigkeit!)
- **OID Repository**
  - Sammelt OID Einträge mit Metadaten zur Suche
  - Leider gibt es kein globales Repository

- **Einträge**

- weltweit eindeutig
- permanent
  - nicht löschar
  - deaktivierbar (obsolet)
  - änderbar

- **Verschiedene Notationen (Bsp. Internet)**

- ASN.1-Notation:
  - mit sek. Text: {1 3 6 1}
  - OID-IRI: {iso(1) org(3) dod(6) internet(1)}
- Punkt-Notation /iso/org/dod/internet
- URN-Notation 1.3.6.1  
urn:oid:1.3.6.1

- **Links**

- <http://www.oid-info.com/faq.htm>

- **6 Knoten**

- 1 (iso)

- 1.2 (member-body)

- 1.2.40 (at)

- 1.2.40.0 (on)

- 1.2.40.0.10 (Verwaltung)

- 1.2.40.0.11 (mag-14-wien)

- 1.2.40.0.23 (akh-linz)

- 1.2.40.0.29 (fhtw)

- 1.2.40.0.34 (eHealth-Austria)

- 1.2.40.0.35 (wienkav-root)

- **Links**

- <http://oid.gesundheit.gv.at> ( 1.2.40.0.34 )

# Verwendung von OIDs

- **eHealth**
  - DICOM
  - HL7
  - ELGA
- **X.509 Zertifikate**
- **X.500 Verzeichnisdienste**
- **LDAP-Schemata**
- **SNMP Management Information Base (MIB)**

- **Technische Interoperabilität**
  - Können Systeme miteinander Informationen austauschen?
- **Semantische Interoperabilität**
  - Können empfangene Daten durch Systeme semantisch interpretiert und weiter verarbeitet werden?
  - Wie hoch ist der Grad der semantischen Interoperabilität?
- **Prozess-Interoperabilität**
  - Reiner Datenaustausch ist zu wenig. Erst die optimale Integration der Computersysteme in die Arbeitsprozesse erhöht den Nutzen/die Qualität.

Quelle: Gibbons et al., 2007

# Begriffsdefinition

- **Vokabular (Wortschatz)**
  - alle zugelassenen Begriffe
- **kontrolliertes Vokabular**
  - keine Homonyme (Duplikate mit unterschiedlicher Bedeutung)
- **Codeliste**
  - kontrolliertes Vokabular mit eindeutigen Identifikatoren (Codes)
- **Value Set**
  - Codeliste für einen eng umrissenen Anwendungsbereich
- **Codesystem**
  - Codeliste mit allen zu ihrer Verwaltung notwendigen Regeln und Mitteln
- **Klassifikation (Systematik, Taxonomie)**
  - In Klassen geordnete und hierarchisch eingeteilte Vokabulare
- **Terminologie:**
  - Mengen von Termen, die das Konzeptsystem repräsentieren
- **Nomenklatur:**
  - Vokabular mit Definitionen, Beschreibungen, Synonymen
    - Thesaurus: vorhandene Verknüpfungen
- **Ontologie:**
  - Semantische Wissensdatenbanken
  - konsistente Thesauren mit formal definierter interner Vernetzung



- Definition der gemeinsam verwendeten Inhalte notwendig (Semantische Interoperabilität)
- Webseite  
<https://termpub.gesundheit.gv.at>
- Webservice

# Terminologieserver

The screenshot shows the 'Terminologie-Browser' web application. The browser address bar displays the URL <https://termpub.gesundheit.gv.at/TermBrowser/gui/main/main.zul>. The application header includes navigation links like 'Terminologie-Browser', 'Anmelden/Abmelden', 'Aktuelle Vorgänge', 'Hilfe', and 'Kontaktformular'. Below the header, there are logos for various institutions including 'Publikationsumgebung Terminologie-Browser', 'MINISTERIUM FRAUEN GESUNDHEIT', 'FH TECHNIKUM WIEN', 'BRZ', 'elga', 'Fachhochschule Dortmund', and 'ebusiness Plattform Gesundheitswesen'. The main content area is divided into two panels. The left panel, titled 'Code Systeme', shows a tree view of value sets, with 'APPC\_Modalitaet\_VS' selected and its version '1.0.9 (empfohlen)' highlighted. The right panel, titled 'Inhalte', displays a table of concepts for the selected value set. The table has three columns: 'Begriff', 'Code', and 'Quelle'. The concepts listed include 'Modalitaet unbestimmt', 'Röntgen', 'CT', 'MRT', 'US', 'NUK', 'PET', 'Endoskopie' (with sub-items like 'Kapselendoskopie' and 'Konfokale Laserendomikroskopie'), 'Mikroskopische Untersuchung', 'Optische Kohärenztomografie', 'Fotografische Dokumentation', and 'Video Dokumentation'. At the bottom of the interface, there is a red status bar indicating 'Publikationsplattform: Verbindung getrennt'.

Terminologie-Browser

Code Systeme Value Sets Suche

Name

- APPC\_Anatomie\_VS
- APPC\_Lateralitaet\_VS
- APPC\_Modalitaet\_VS
  - 1.0.7 (empfohlen)
  - 1.0.8 (empfohlen)
  - 1.0.9 (empfohlen)
- APPC\_Prozeduren\_VS
- DICOM\_SOPClasses\_VS
- ELGA\_ActCode\_AbgInfo\_VS
- ELGA\_ActCode\_PatInfo\_VS
- ELGA\_ActEncounterCode
- ELGA\_AddressUse
- ELGA\_AdministrativeGender
- ELGA\_Antibiotika
- ELGA\_AuditEventID\_VS
- ELGA\_AuditEventTvoe A-ARR VS

Globale Konzept Suche Details

Publikationsumgebung Terminologie-Browser

MINISTERIUM FRAUEN GESUNDHEIT

FH TECHNIKUM WIEN

BRZ

elga

Fachhochschule Dortmund

ebusiness Plattform Gesundheitswesen

Inhalte

Value Set: APPC\_Modalitaet\_VS | Version: 1.0.9

Begriff	Code	Quelle
Modalitaet unbestimmt	0	APPC_Modalitaet_1.0.9 (1.2.40.0.34.5.38.1)
Röntgen	1	APPC_Modalitaet_1.0.9 (1.2.40.0.34.5.38.1)
CT	2	APPC_Modalitaet_1.0.9 (1.2.40.0.34.5.38.1)
MRT	3	APPC_Modalitaet_1.0.9 (1.2.40.0.34.5.38.1)
US	4	APPC_Modalitaet_1.0.9 (1.2.40.0.34.5.38.1)
NUK	5	APPC_Modalitaet_1.0.9 (1.2.40.0.34.5.38.1)
PET	6	APPC_Modalitaet_1.0.9 (1.2.40.0.34.5.38.1)
Endoskopie	7	APPC_Modalitaet_1.0.9 (1.2.40.0.34.5.38.1)
Kapselendoskopie	7-1	APPC_Modalitaet_1.0.9 (1.2.40.0.34.5.38.1)
Konfokale Laserendomikroskopie	7-2	APPC_Modalitaet_1.0.9 (1.2.40.0.34.5.38.1)
Mikroskopische Untersuchung	8	APPC_Modalitaet_1.0.9 (1.2.40.0.34.5.38.1)
Optische Kohärenztomografie	9	APPC_Modalitaet_1.0.9 (1.2.40.0.34.5.38.1)
Fotografische Dokumentation	10	APPC_Modalitaet_1.0.9 (1.2.40.0.34.5.38.1)
Video Dokumentation	11	APPC_Modalitaet_1.0.9 (1.2.40.0.34.5.38.1)

Weitere Funktionen über Kontextmenüs verfügbar

Konzept Suche Details

Publikationsplattform: Verbindung getrennt

Quelle: <https://termpub.gesundheit.gv.at>

# Terminologieserver

The screenshot shows the 'Terminologie-Browser' web application. The browser window has a single tab titled 'Terminologie-Browser' with the URL <https://termpub.gesundheit.gv.at/TermBrowser/gui/main/main.zul>. The application header includes navigation links like 'Anmelden/Abmelden', 'Aktuelle Vorgänge', 'Hilfe', and 'Kontaktformular'. Below the header, there are logos for various institutions including 'MINISTERIUM FRAUEN GESUNDHEIT', 'FH TECHNIKUM WIEN', 'BRZ', 'elga', 'Fachhochschule Dortmund', and 'ebpg'. The main content area is divided into two panels. The left panel, titled 'Code Systeme', shows a tree view of code systems. The right panel, titled 'Inhalte', displays a table of concepts for the selected code system 'ELGA\_GDA\_Aggregatrollen | Version: ELGA\_GDA\_Aggregatrollen\_3.0'.

**Code Systeme** | Value Sets | Suche

**Inhalte**

Code System: ELGA\_GDA\_Aggregatrollen | Version: ELGA\_GDA\_Aggregatrollen\_3.0

Begriff	Code
Ärztin/Arzt	700
Zahnärztin/Zahnarzt	701
Krankenanstalt	702
Einrichtung der Pflege	703
Apotheke	704
ELGA-Beratung	705
ELGA-Ombudsstelle	706

Publikationsplattform: Verbindung getrennt

Quelle: <https://termpub.gesundheit.gv.at>

- **Kooperationsprojekt**
  - Fachhochschule Dortmund (Entwicklung und Programmierung)
  - Technikum Wien GmbH (Entwicklung und Programmierung)
  - Bundesrechenzentrum GmbH (Technik und Betrieb)
  - ELGA GmbH (Projektleitung und Testkoordination)
  - Österreichisches Bundesministerium für Gesundheit und Frauen
- **Teil der nationalen eHealth-Infrastruktur**
  - Das vorrangige Projektziel war, dem aus der Errichtung der ELGA resultierenden Bedarf an Terminologien Rechnung zu tragen. Darüber hinaus wurde ein Mehrwert dahingehend angestrebt, dass dieses Werkzeug auch für vergleichbare Anforderungen aus anderen eHealth-Anwendungen und einem erweiterten Benutzerkreis zur Verfügung steht. Nicht zuletzt auch durch die Verknüpfung mit der OID-Verwaltung wurde es somit von einem ursprünglichen ELGA-Teilprojekt zu einem – immer wichtiger werdenden – Bestandteil der nationalen eHealth-Infrastruktur weiterentwickelt.

Quelle: <https://www.gesundheit.gv.at/service/terminologieserver>

# ELGA Architektur

Einführung

## 15a-Vereinbarung für Gesundheit mit 200 Mio. für Primärversorgung

*Bund, Länder und Sozialversicherung haben sich im Zuge der Verhandlungen über den Finanzausgleich auf eine 15a-Vereinbarung für den Bereich Gesundheit weitgehend geeinigt. Der der APA vorliegende Entwurf dieses Vertrages sieht vor allem einen Ausbau der von der Ärztekammer bekämpften medizinischen Primärversorgung vor. Bis Ende 2020 sollen dafür 200 Millionen Euro investiert werden.*

*Die Bedeckung dieser Mehrkosten soll aus zweckgewidmeten Mitteln der Sozialversicherung und der Länder erfolgen. Außerdem sollen zur Finanzierung der Elektronischen Gesundheitsakte (ELGA) 41 Millionen Euro bis 2020 zur Verfügung gestellt werden.*

01.11.2016, <https://kurier.at/politik/inland/15a-vereinbarung-fuer-gesundheit-mit-200-mio-fuer-primarversorgung/228.387.116>

## Ärzte: Zugriff auf Elga zu schlecht gesichert

*Ein Passwort allein bietet keine ausreichende Sicherheit. Als Konsequenz fordert die Wiener Ärztekammer eine Zweifaktor-Authentifizierung.*

*Die Wiener Ärztekammer hat die Datensicherheit der elektronischen Gesundheitsakte (Elga) durch Cybersecurity-Experten untersuchen lassen und ortet Schwachstellen. So sei die Authentifizierung durch ein Passwort nicht ausreichend, wie Präsident Thomas Szekeres und sein Vize Johannes Steinhart am Dienstag erklärten. „Gesundheitsdaten sind die heikelsten Daten und werden im Darknet um mehr Geld gehandelt als Kreditkartennummern“, sagte Szekeres. Kommen die Daten in die falschen Hände, könne dies für Patienten beruflich und privat negative Folgen haben.*

*„Mit der Einführung von Elga haben sich die Angriffsfläche und die Auswirkungen von Angriffen erhöht“, sagte Thomas Stubbings, Cybersecurity-Experte und Geschäftsführer von TS Management Consulting. Er untersuchte gemeinsam mit einem Kollegen die Dokumentenarchitektur von Elga. Grundsätzlich konstatierte er dabei Positives: „Wir haben festgestellt, dass man sich sehr viele Gedanken macht zum Thema Sicherheit und wir haben keine offensichtlichen Schwachstellen entdeckt.“*

24.11.2017, [http://diepresse.com/home/innenpolitik/5159455/Aerzte\\_Zugriff-auf-Elga-zu-schlecht-gesichert](http://diepresse.com/home/innenpolitik/5159455/Aerzte_Zugriff-auf-Elga-zu-schlecht-gesichert)

## Wiener Ärztekammer äußerte erneut Sicherheitsbedenken gegen Elga

*IT-Experte: "Keine offensichtlichen Schwachstellen"*

*"Mit der Einführung von Elga haben sich die Angriffsfläche und die Auswirkungen von Angriffen erhöht", sagte Thomas Stubbings, Cybersecurity-Experte und Geschäftsführer von TS Management Consulting. Er untersuchte gemeinsam mit einem Kollegen die Dokumentenarchitektur von Elga, und ortete ein "sehr komplexes System". Grundsätzlich stellte er dabei Positives fest: "Wir haben festgestellt, dass man sich sehr viele Gedanken macht zum Thema Sicherheit und wir haben keine offensichtlichen Schwachstellen entdeckt", sagte er.*

*Ärztekammer will "Zweifaktor-Authentifizierung"*

*Als Konsequenz fordert die Wiener Ärztekammer Maßnahmen, die die aus ihrer Sicht bestehenden Schwachstellen abbauen würden. So soll statt der einfachen Anmeldung über Username und Passwort eine Zweifaktor-Authentifizierung eingeführt werden. Außerdem spricht sich die Ärztekammer für eine zentrale Benutzerverwaltung für alle Elga-berechtigten Anwender und die flächendeckende digitale Signatur von Gesundheitsdokumenten aus.*

24.11.2017, <http://derstandard.at/2000051413574/Wiener-Aerztekammer-aeusserte-erneut-Sicherheitsbedenken-gegen-Elga>



## Kritik an Geschäft mit Patientendaten

*Softwarefirmen bieten Geld um an geschützte Patientendaten zu kommen - Kritik von Datenschützern und Ärztekammer*

*Wien - Für 432 Euro im Jahr sollen Ärzte Softwarefirmen hochsensible und geschützte Daten von Patienten und ihrer eigenen Praxis zur Verfügung stellen. Sie werden mithilfe eines Programms vollautomatisch an das Marktforschungsinstitut IMS Health übermittelt. Das berichtet die Wiener Wochenzeitung Falter in ihrer am Mittwoch erscheinenden Ausgabe.*

*Ärztekammer und Datenschützer üben massive Kritik. Hans Zeger von der österreichischen Gesellschaft für Datenschutz (ARGE Daten) sagt, damit würden Ärzte ihre Vertraulichkeit verkaufen. Das Programm sei ein "enormes Sicherheitsproblem", ein Fremder könne ohne staatliche Kontrolle an höchst sensible Daten kommen. Es sei zu befürchten, dass die Daten an Dritte weiterverkauft werden.*

*Das Marktforschungsinstitut IMS Health gibt an, die Daten für eine Studie zu benötigen, um die Diagnose- und Therapiegewohnheiten niedergelassener Ärzte in Österreich zu zeigen. Das Institut verweist auf sein strenges Datenschutzprogramm, alle übermittelten Daten seien anonymisiert. "Die ärztliche Schweigepflicht wird in keiner Weise berührt", versichert IMS Health. Neben Datenschützern rät auch die Ärztekammer den Ärzten dringend davon ab, sich an Aktion zu beteiligen.*

24.04.2012, <http://derstandard.at/1334796111267/Datenschutz-gefaehrdet-Kritik-an-Geschaefit-mit-Patientendaten>

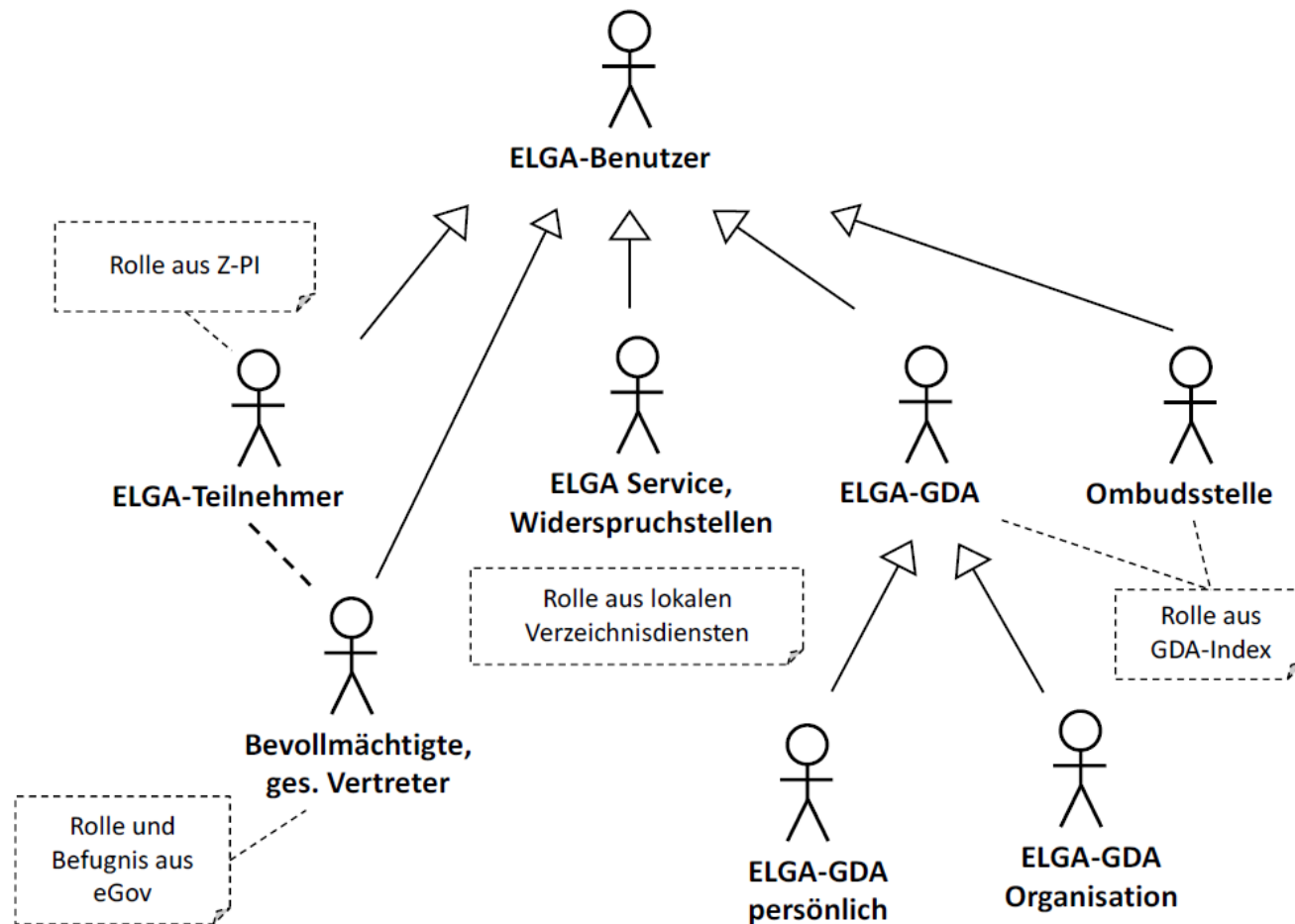
Vorranging sind Informationen öffentlich unter [www.elga.gv.at](http://www.elga.gv.at) zu finden.

- **Gesamtarchitektur v2.30a**
- **Infos für GDA und Softwarehersteller**
- **CDA Leitfäden**
- **Verwendete Normen**
- **Terminologien**

- **Informationen sind frei abrufbar**
  - <https://www.ris.bka.gv.at>
- **Im Kontext von eHealth sind insbesondere folgende Rechtsgrundlagen essentiell**
  - Gesundheitstelematikgesetz 2012 (GTelG 2012)
  - Gesundheitstelematikverordnung 2013 (GTelV 2013)
  - ELGA-Verordnung 2015 (ELGA-VO 2015)
  - Datenschutz-Grundverordnung (EU-DSGVO) (EU 2016/679)

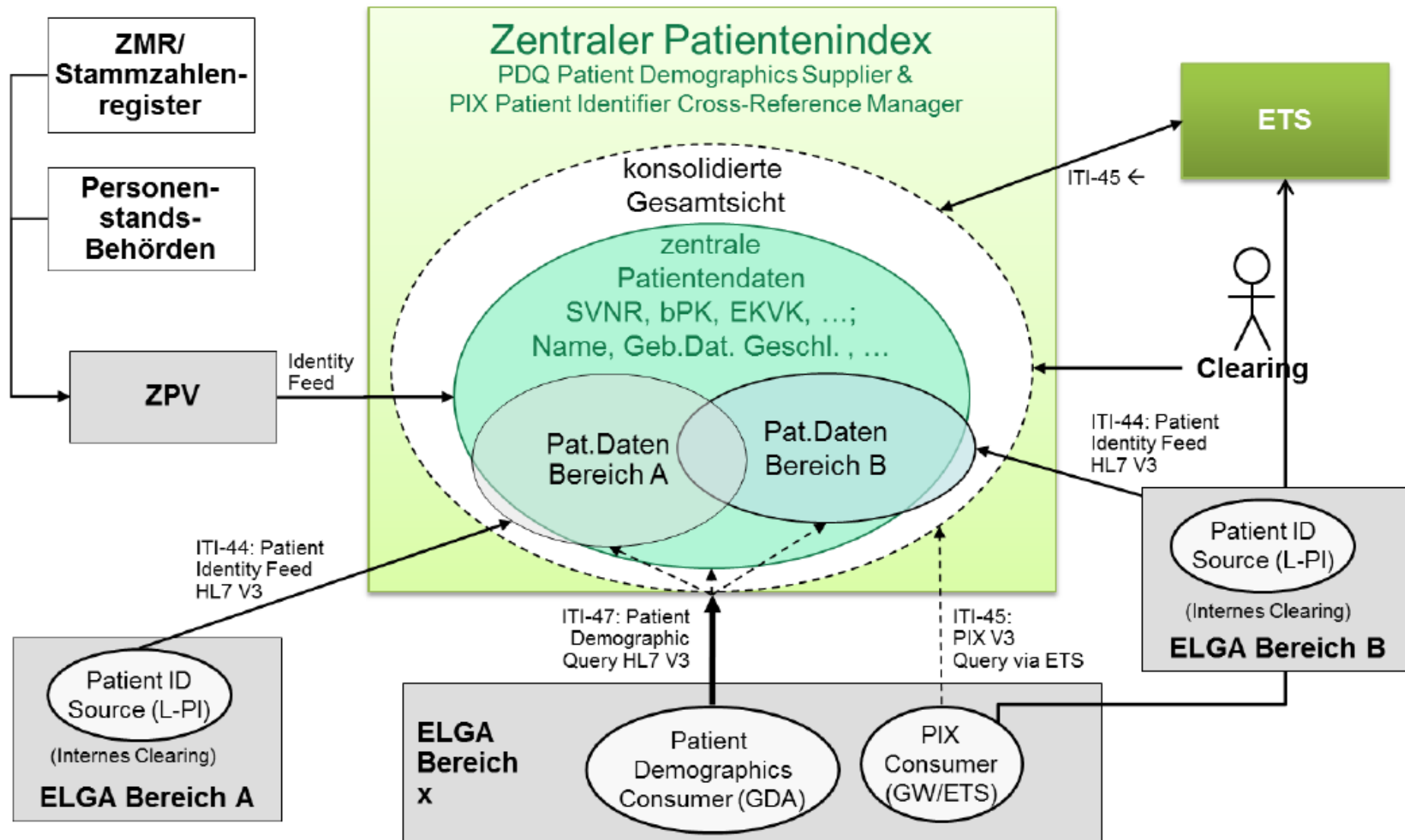
Quelle: <http://www.ris.bka.gv.at>, Stand 30.12.2016

- **direkt aus Gesetz/Verordnung ableitbar:**



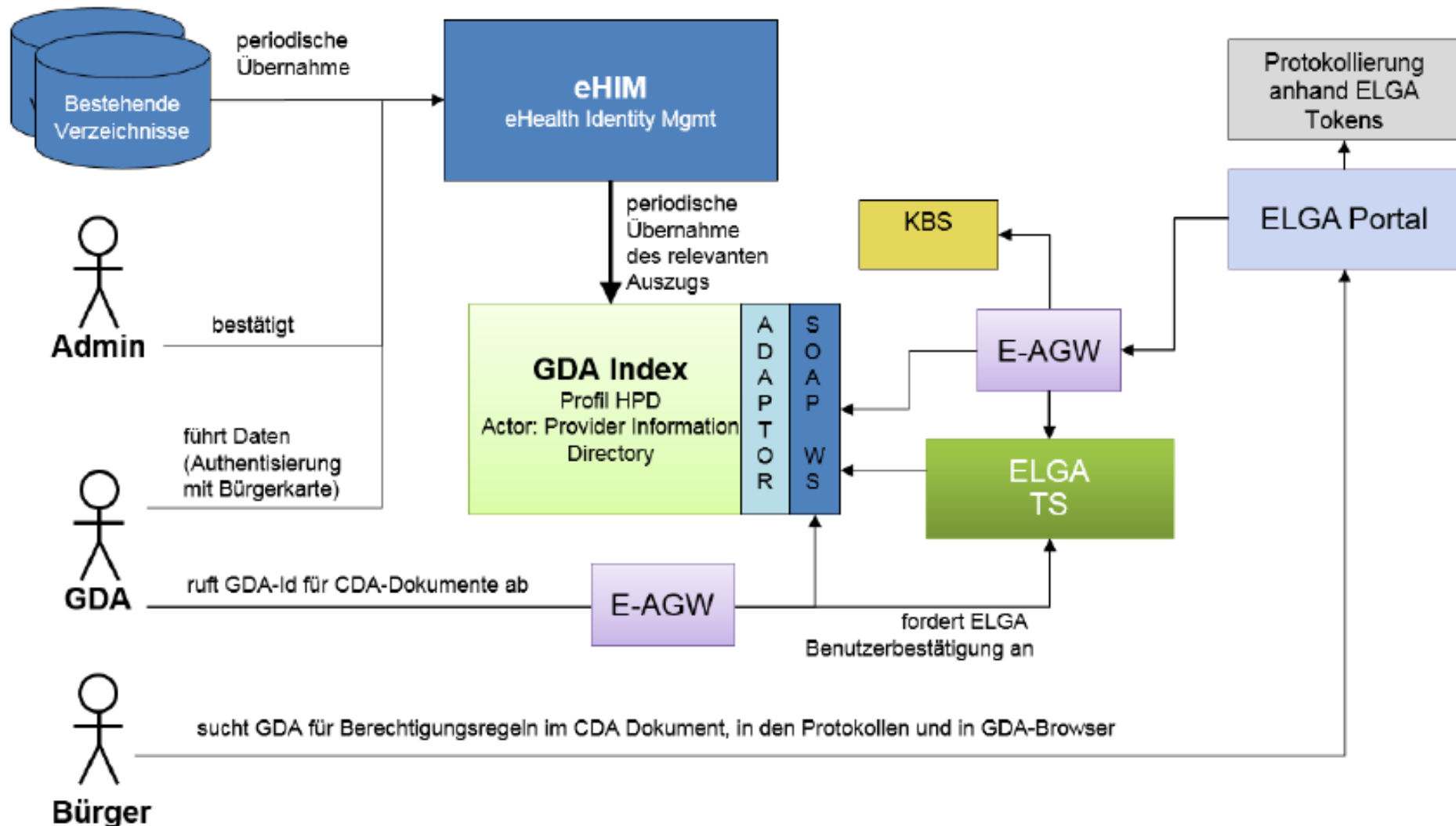
Quelle: ELGA Gesamtarchitektur v2.30a (Zeile 153)

# Der Zentrale Patienten-Index (Z-PI)



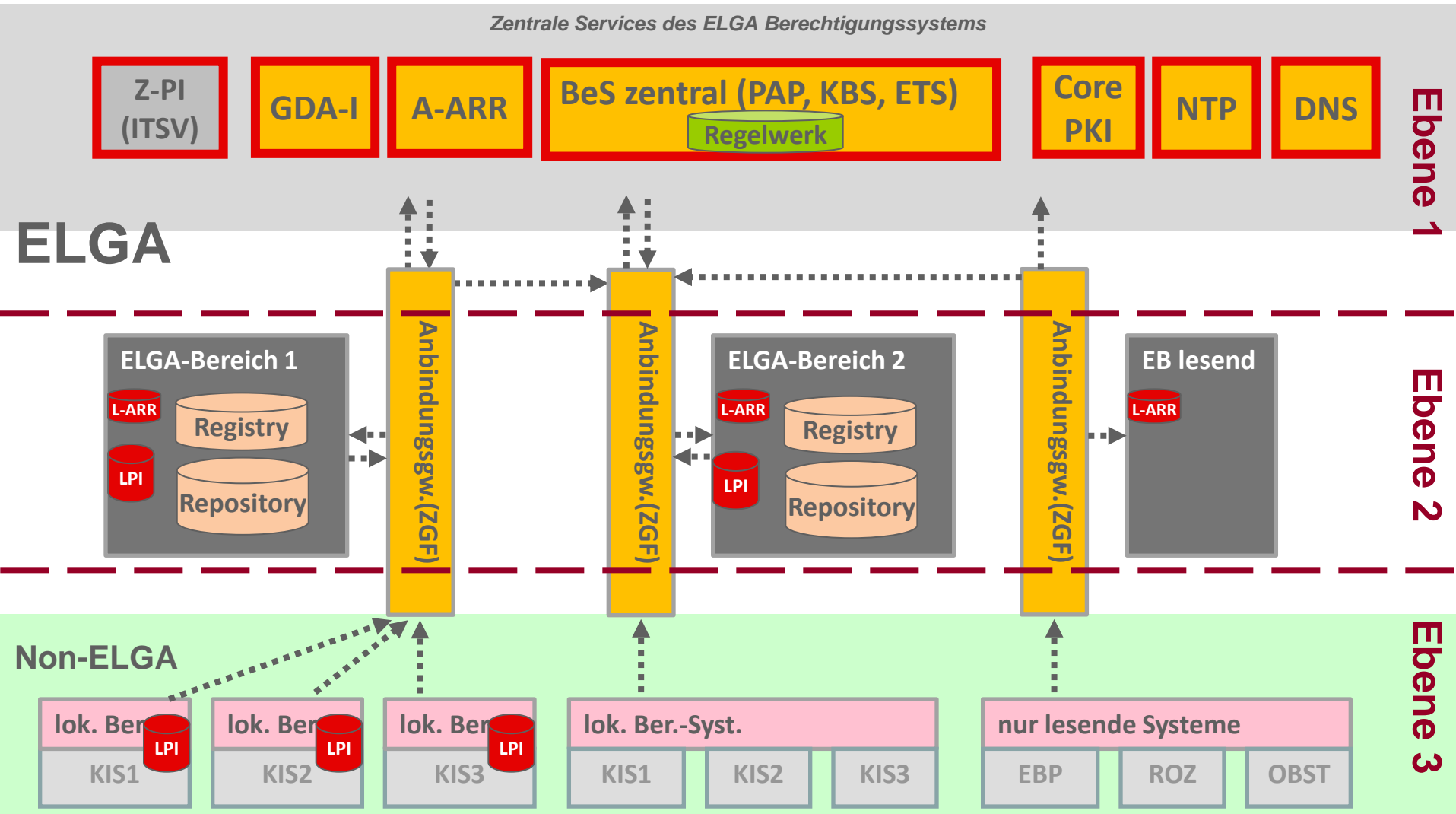
Quelle: ELGA Gesamtarchitektur v2.30a (Zeile 2515)

# Der Gesundheitsdienste Anbieter Index (GDA-I)



Quelle: ELGA Gesamtarchitektur v2.30a (Zeile 2705)

# Überblick Komponenten/Ebenen

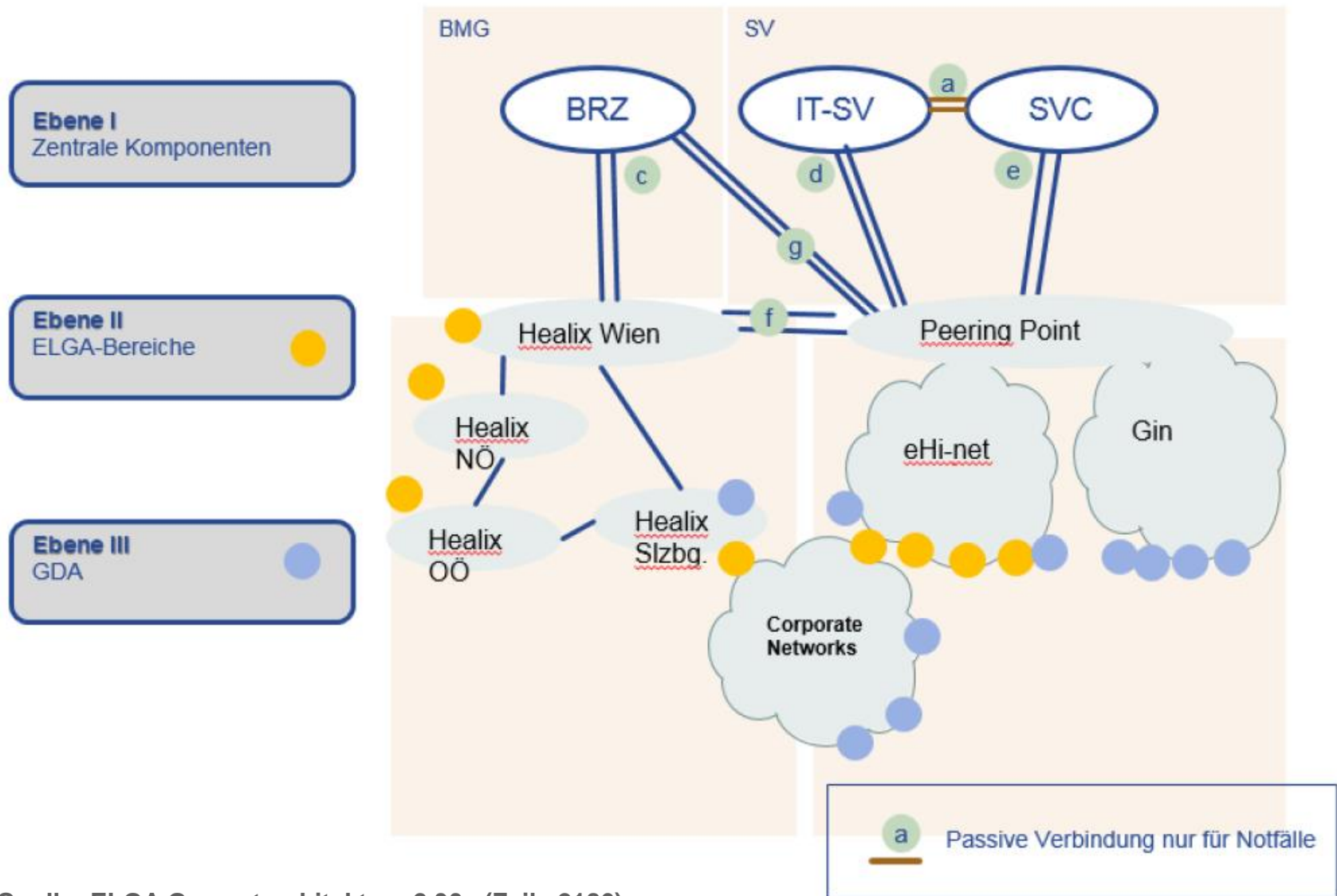


Quelle: ELGA Schulungsunterlagen, ©BRZ

- **je Umgebung (Produktion, ....)**
  - Datenspeicher (Affinity Domain, XDS)
    - Repository
    - Registry
    - L-PI
    - L-ARR (ATNA Protokollierung)
  - AGW (ELGA Anbindungsgateway)
  - GDAs (Gesundheits-Dienste-Anbieter)
    - Clients wie KIS, LIS, RIS, ...
- **Infrastruktur Dienste**
  - DNS, NTP,
  - PKI (Public-Key-Infrastructure)
  - Technische Hilfsdienste für Logfiles, Monitoring



# Genutzte Netzwerke



Quelle: ELGA Gesamtarchitektur v2.30a (Zeile 2186)

# Zugriffe in ELGA nach Rolle

ELGA Rolle	PAP		e-Bef. CDA	e-Med	A-ARR	L-ARR	Z-L-ARR	KBS				Z-PI
	Indiv. Policy	Gener Policy						Amb	Stat	Entl	Del.	
GDA Arzt	✗	✗	✓	✓	✗	✓	✗	✓	✗	✗	✓	✓
GDA Apotheke	✗	✗	✗	✓	✗	✓	✗	✓	✗	✗	✗	✓
GDA KH	✗	✗	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓
GDA PH	✗	✗	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓
Bürger Teilnehmer	✓	✗	✓	✓	✓	✗	✗	✓	✓	✓	✓	✗
Regelwerk-Administrator	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Sicherheits-Administrator	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗
WIST	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
OBST	✓	✗	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓



Schreiben aufgrund e-Card  
Kontaktbestätigung



Schreiben, beliebige (auch e-Card)  
Kontaktbestätigung



Nur lesen



Nur Opt-out  
bzw. Re-Opt-In



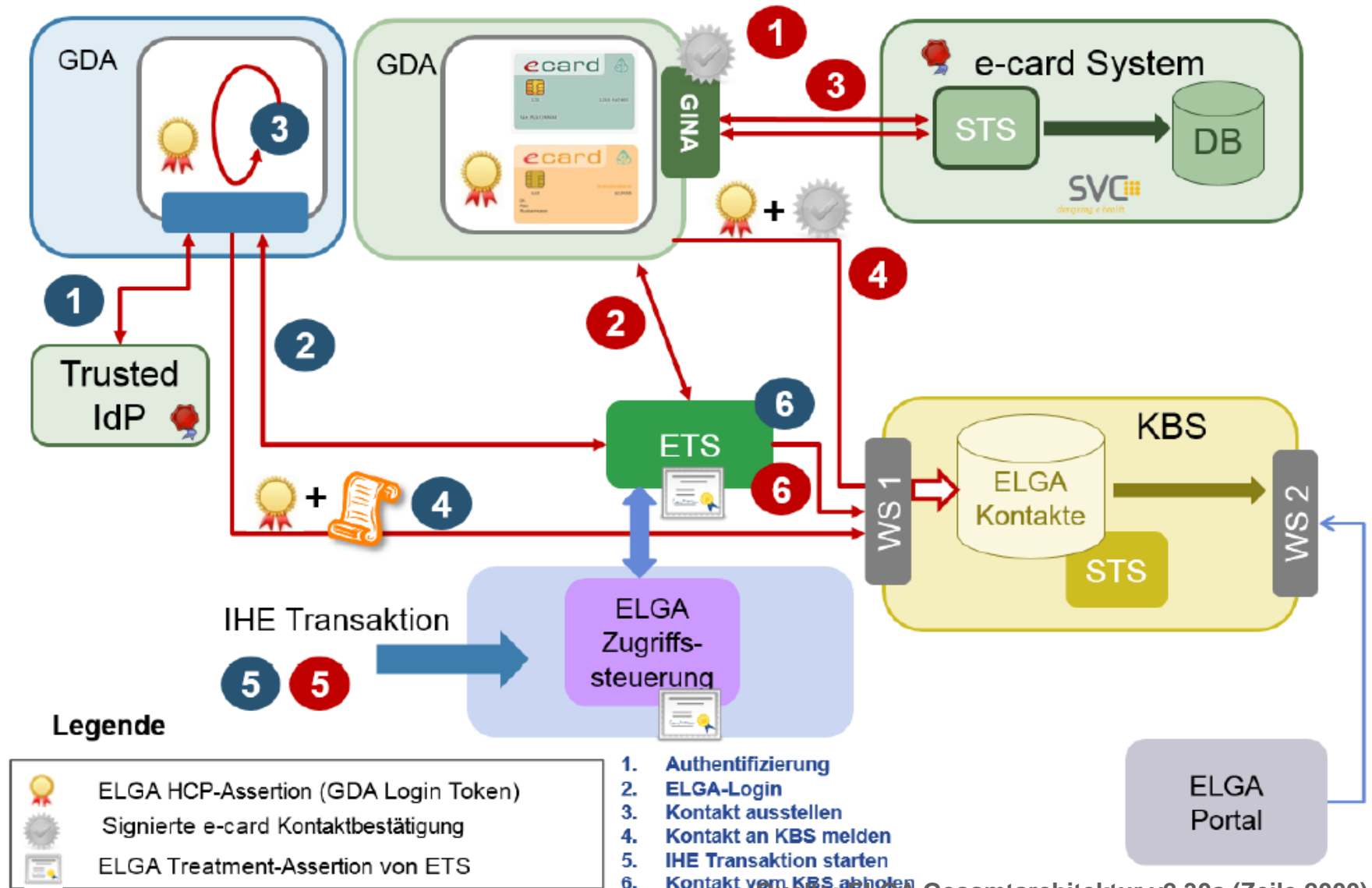
Lesen und  
schreiben



Kein Zugriff

Quelle: ELGA Gesamtarchitektur v2.30a (Zeile 3620)

# ELGA und eCard

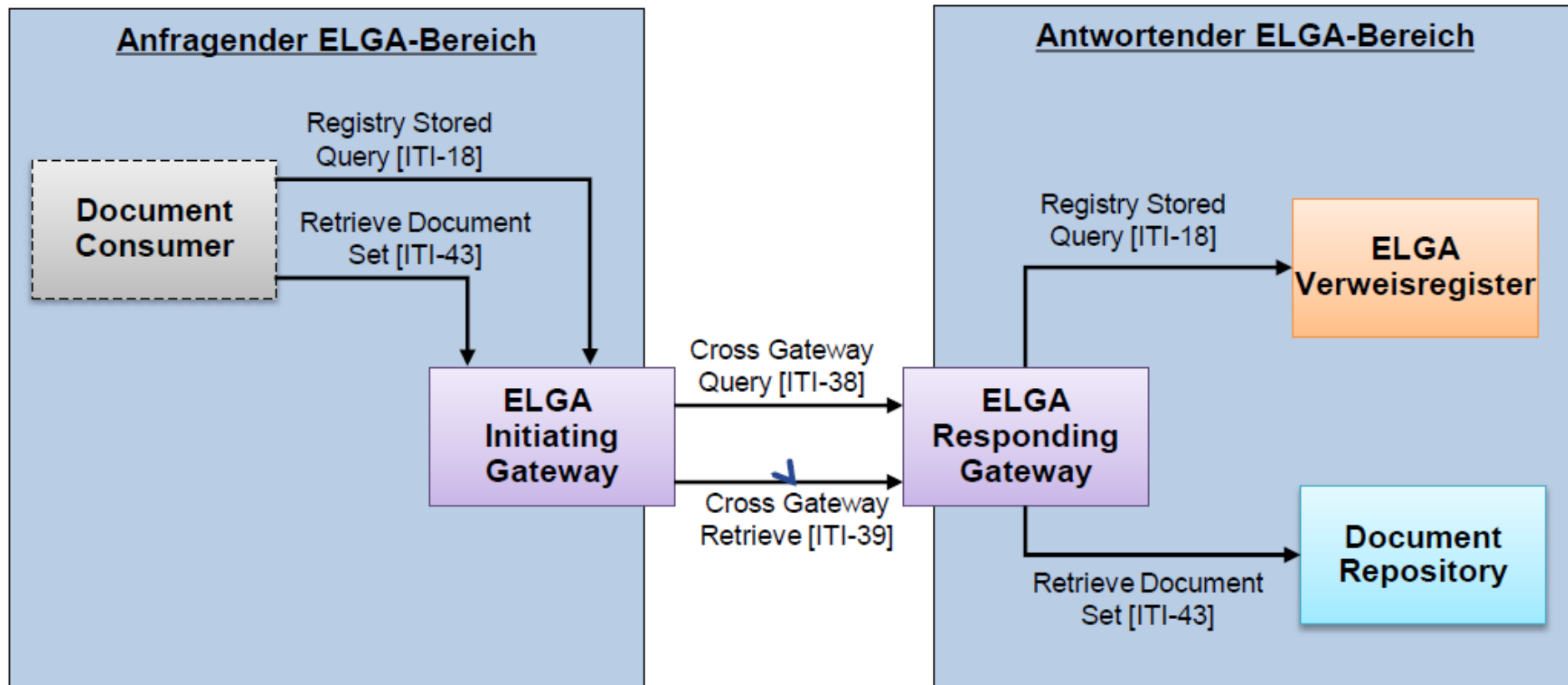


Quelle: ELGA Gesamtarchitektur v2.30a (Zeile 2000)

# Dokumentenzugriff 1

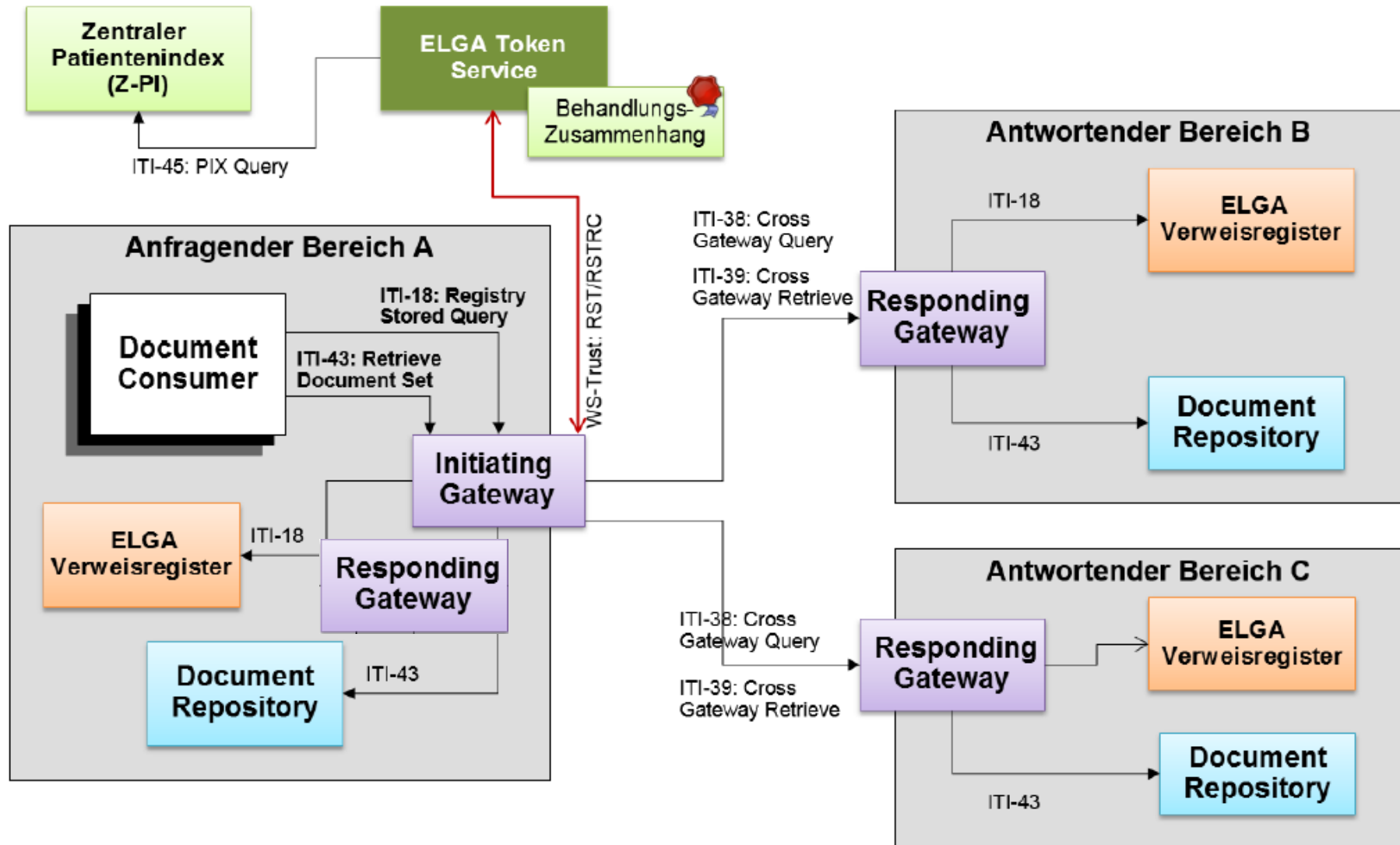
In ELGA erfolgt der Austausch der Dokumente direkt zwischen den ELGA Bereichen.

Es erfolgt keine zentrale Speicherung der Daten.



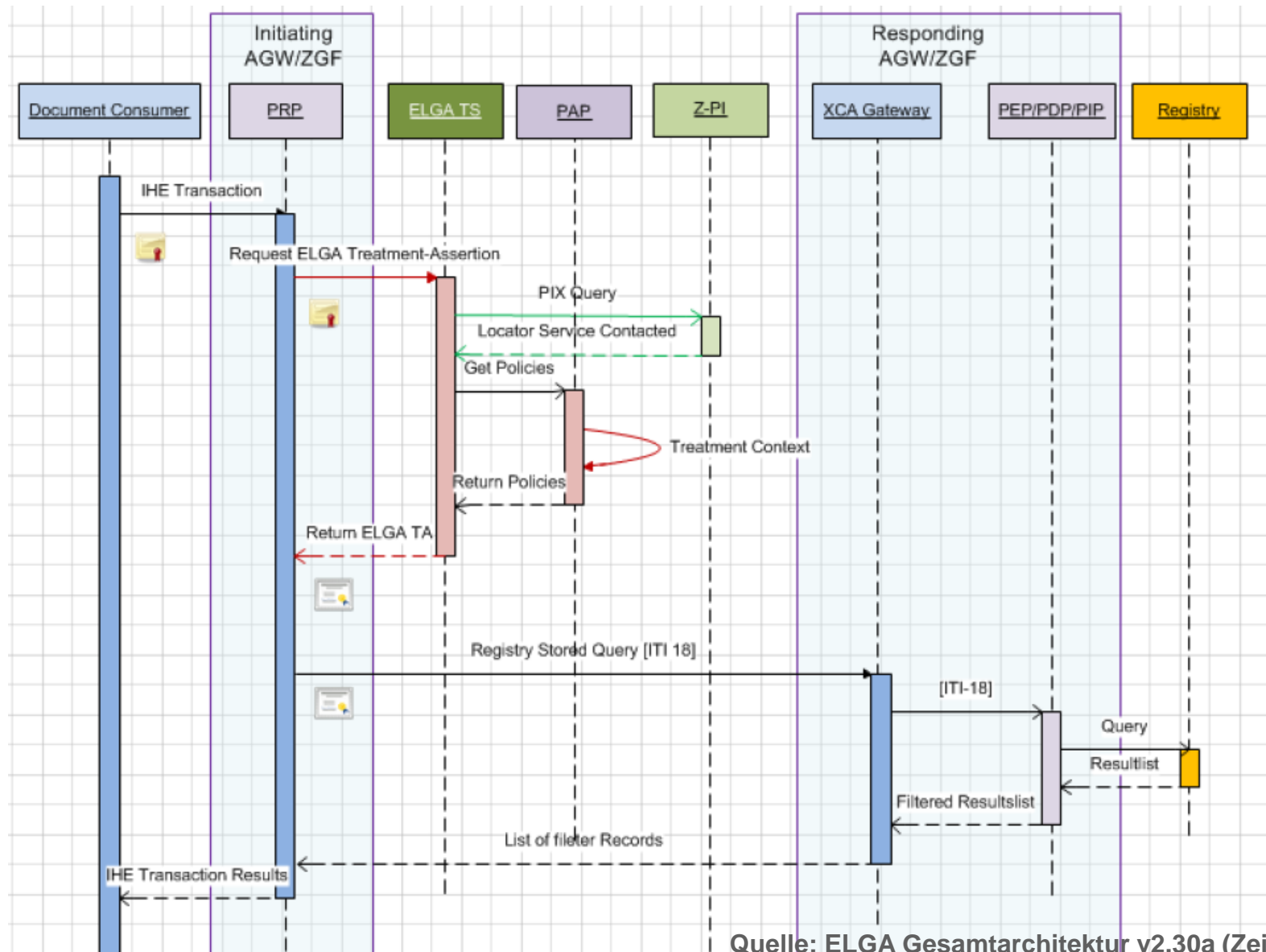
Quelle: ELGA Gesamtarchitektur v2.30a (Zeile 376)

# Dokumentenzugriff 2



Quelle: ELGA Gesamtarchitektur v2.30a (Zeile 812, korrigiert)

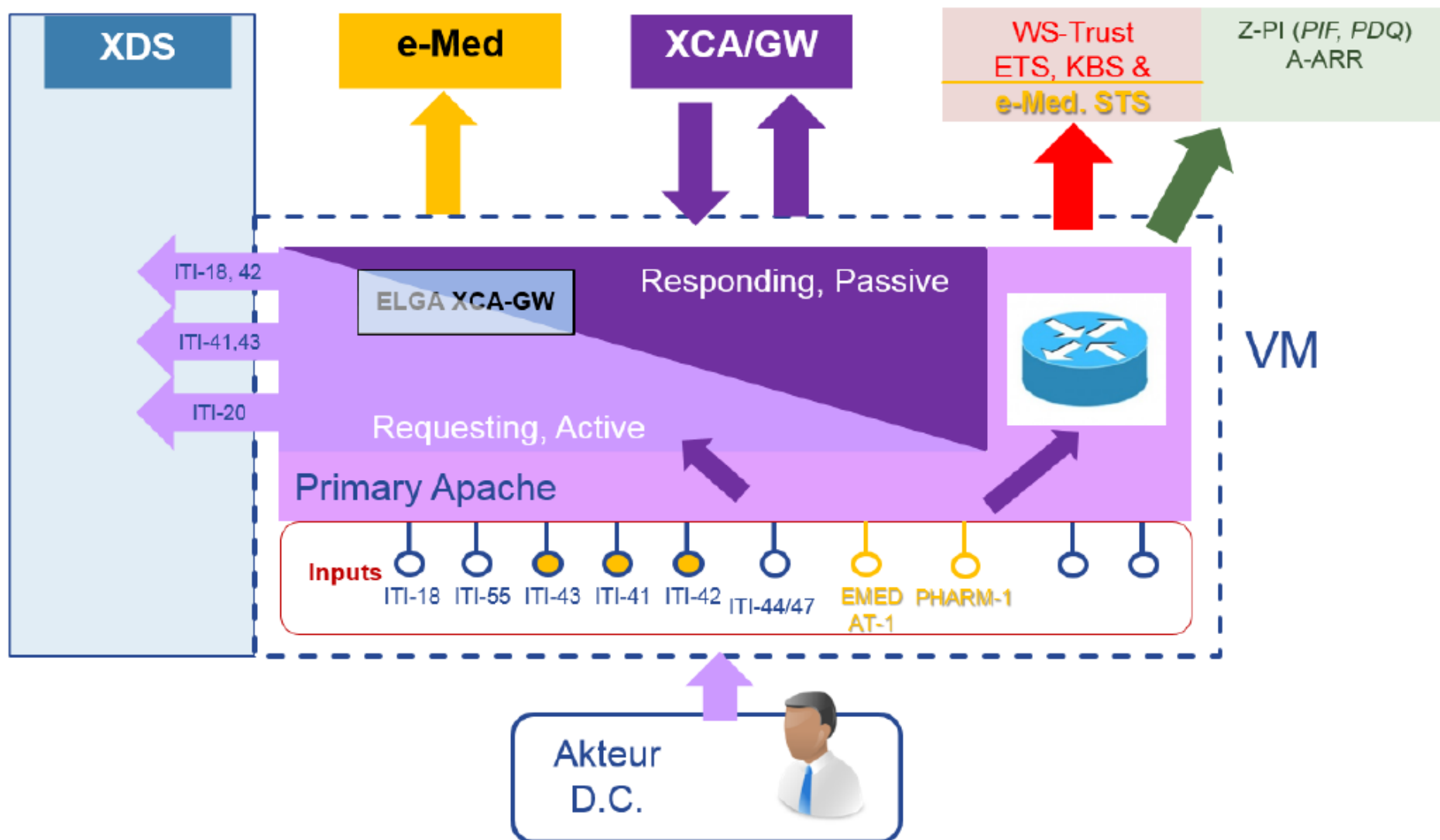
# Dokumentenzugriff 3 (Suchdetail)



Quelle: ELGA Gesamtarchitektur v2.30a (Zeile 6041)

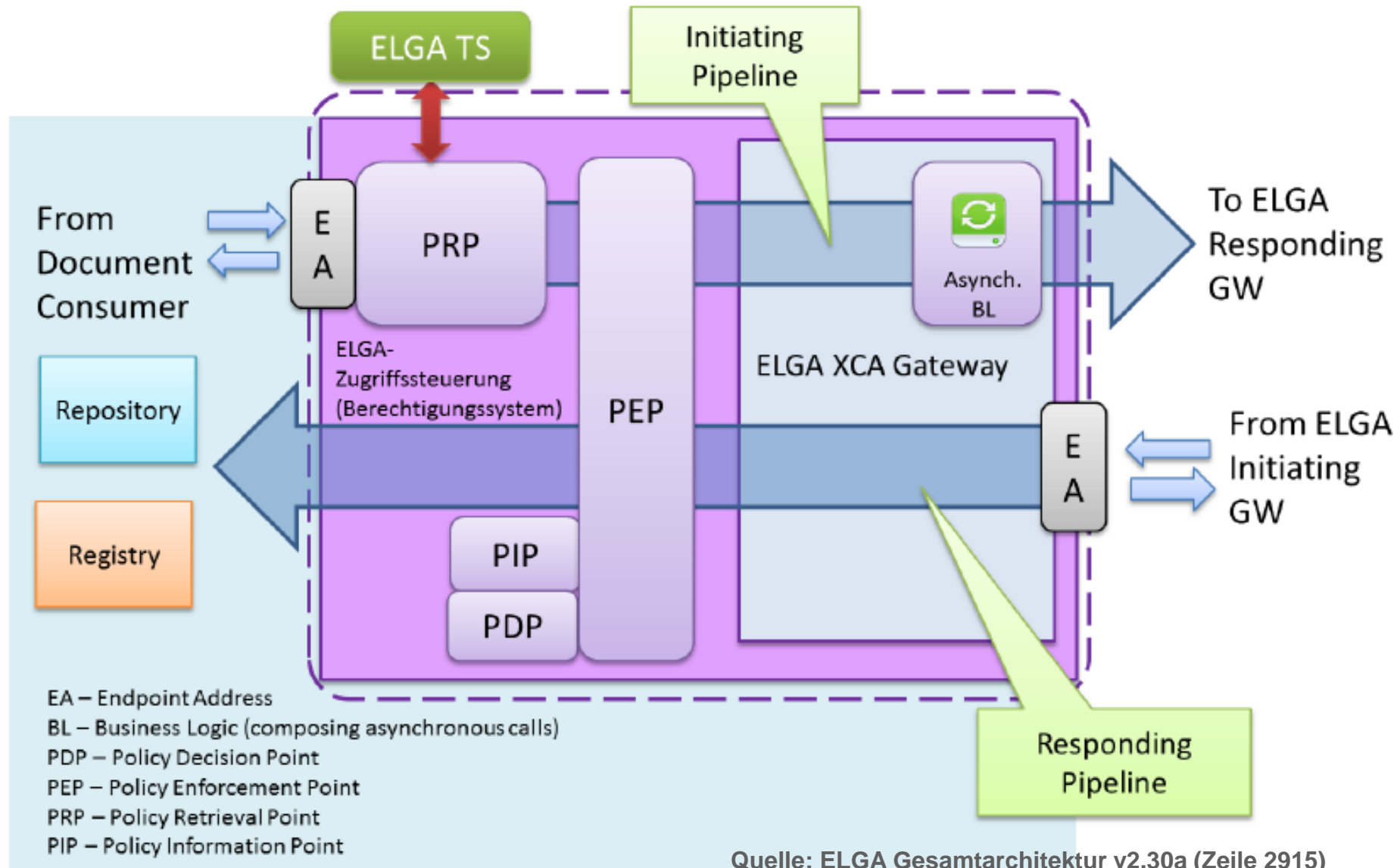


# ELGA Anbindungsgateway (AGW)



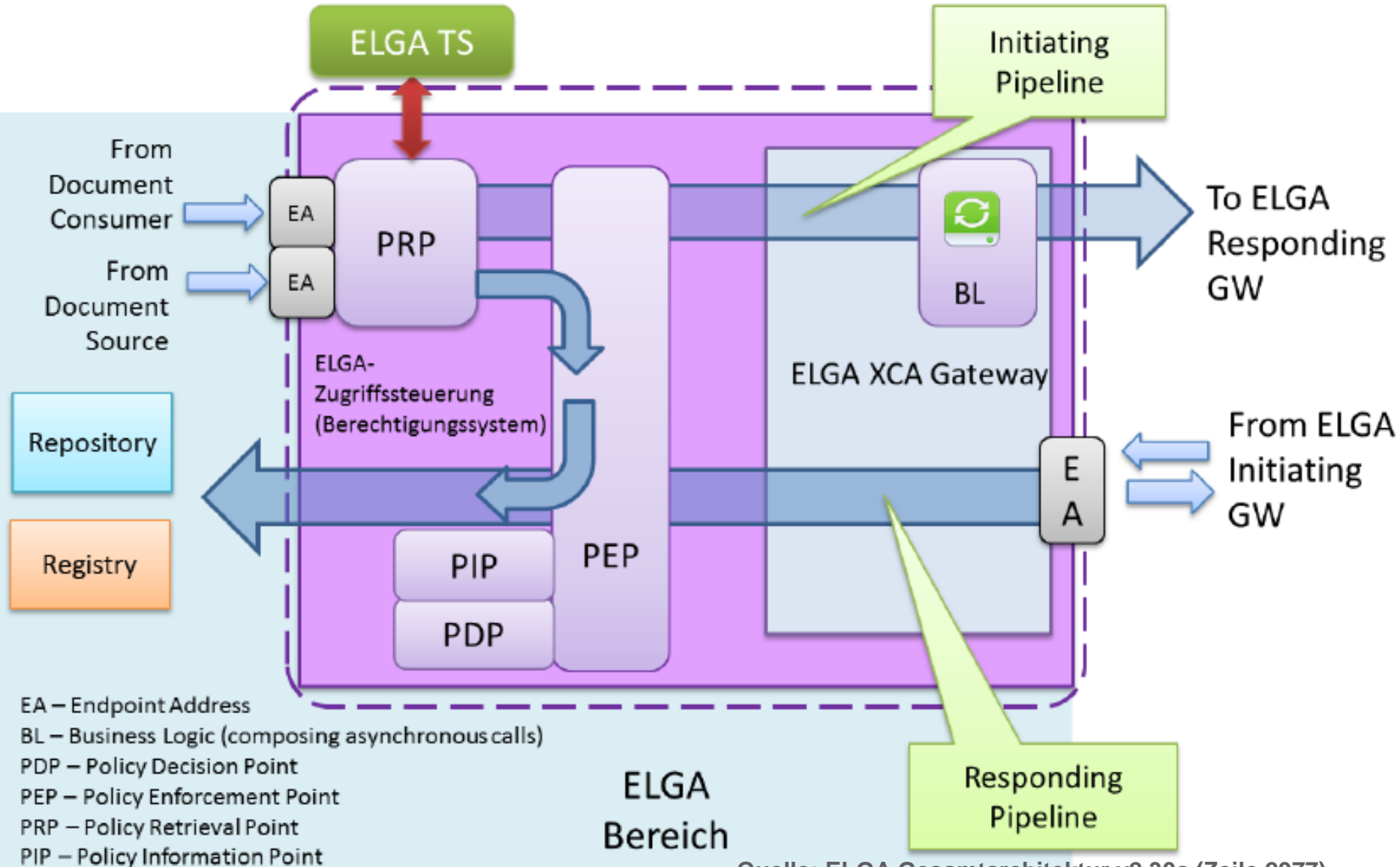
Quelle: ELGA Gesamtarchitektur v2.30a (Zeile 5648)

# AGW Policy Enforcement



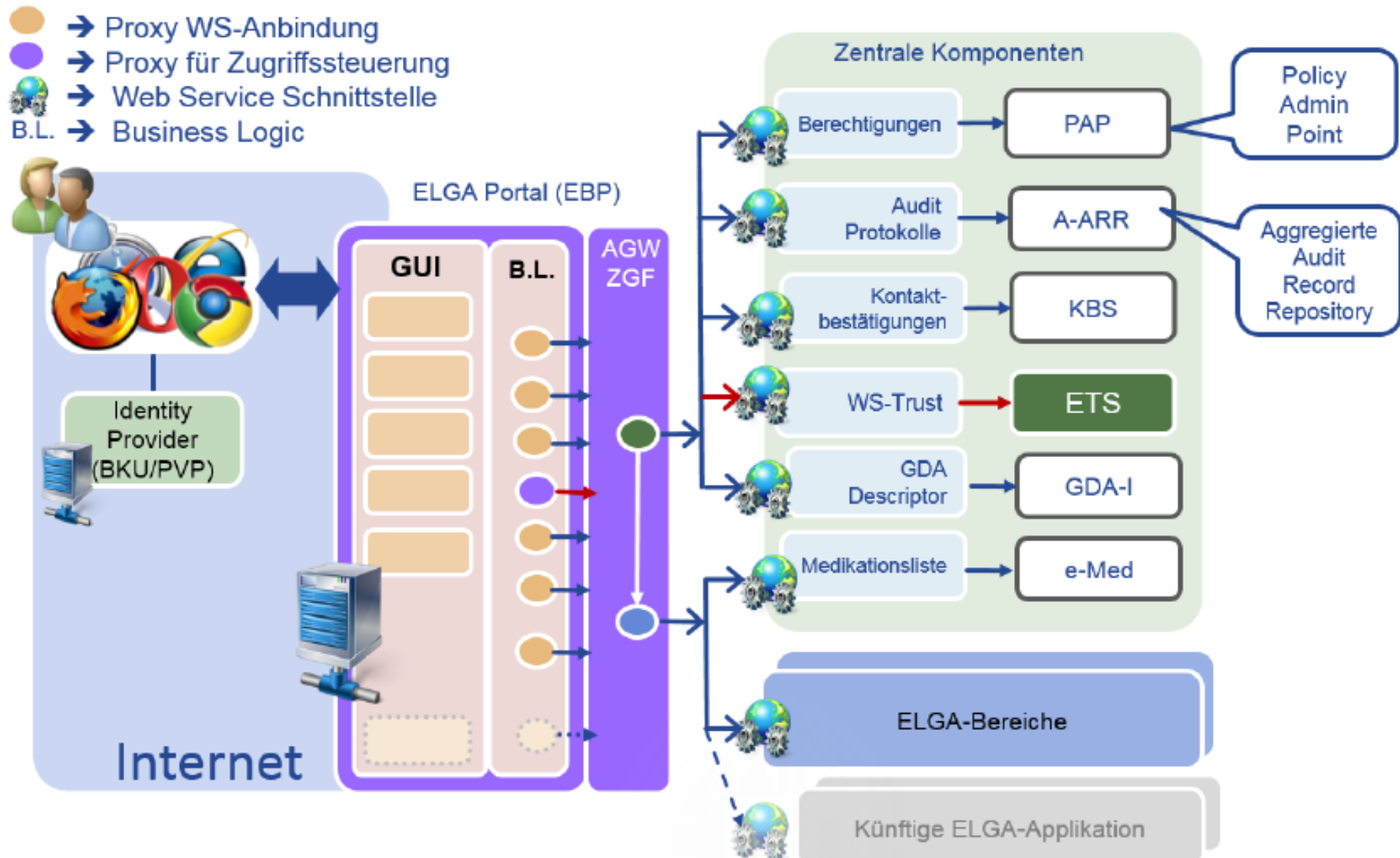


# AGW Schreibvorgänge



Quelle: ELGA Gesamtarchitektur v2.30a (Zeile 2977)

# ELGA Bürger-Portal (EBP)



Quelle: ELGA Gesamtarchitektur v2.30a (Zeile 5307)

## eMED-ID

§ 18 Abs 4 Z 4 GTELG 2012

eMED^12^ XST3KU892344^20131219^1234010170

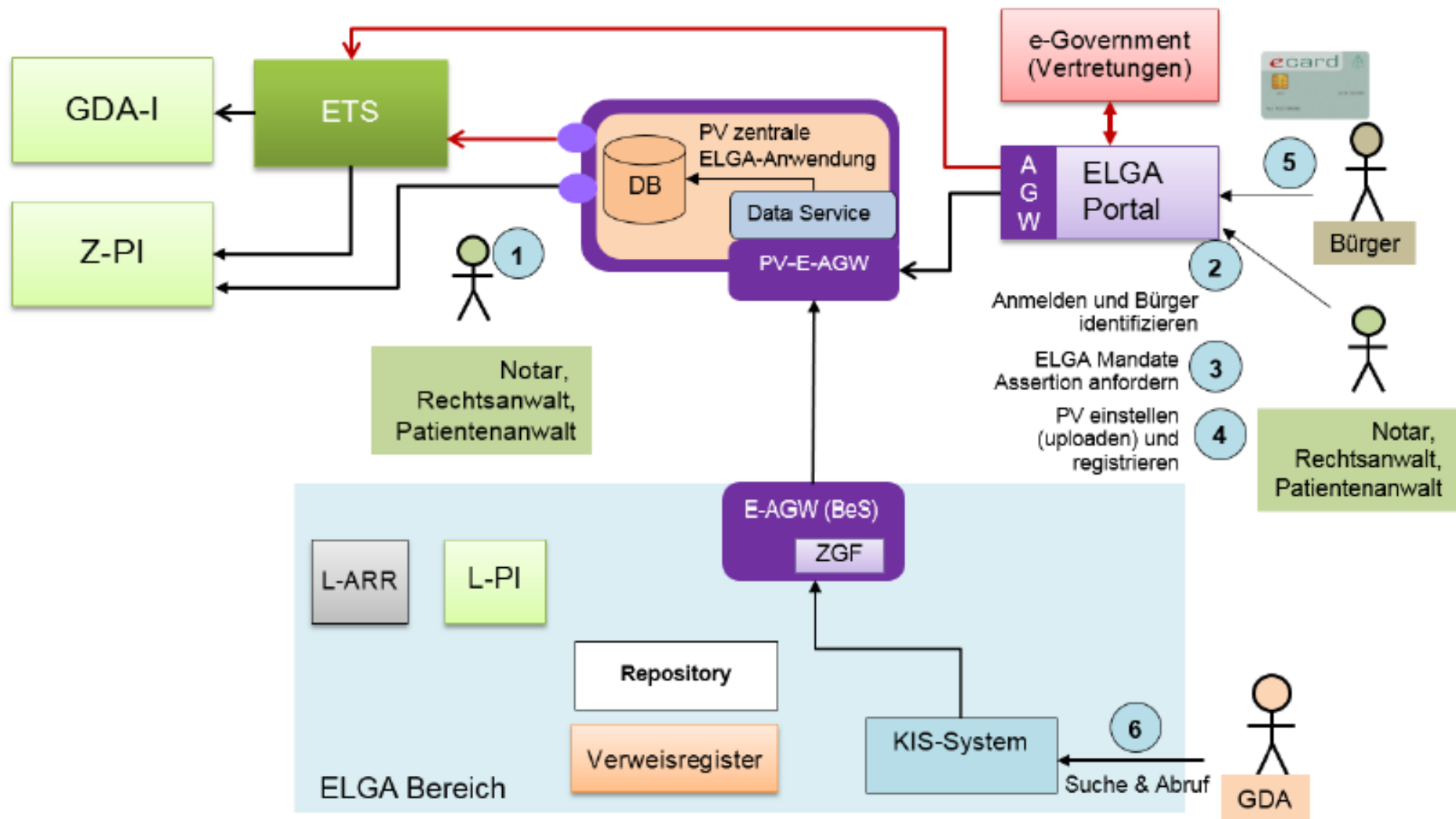


GKK WGKK BtrKK				Mitglieds-Nr.	
<input type="checkbox"/> A	<input type="checkbox"/> B	<input type="checkbox"/> VAES	<input type="checkbox"/> BVA (SR, Bed.)	<input type="checkbox"/> gew. Wirtschaft.	<input type="checkbox"/> Bauern
			<input type="checkbox"/> Einzelständig Arbeitslos Selbstversichert	<input checked="" type="checkbox"/> Pensionist(in)	<input type="checkbox"/> Kriegenste- labene(n)
Aussteller(in) - bitte zutreffendes Feld ankreuzen!					
Familienname(n)		Vorname(n)		Versicherungsnummer	
Patient/in				1212 01 12 60	
Wolfgang Amadeus					
Anschrift					
Heinestrasse 22, 1020 Wien					
Versichert/e/r					
(Nur ausfüllen, wenn Patient/in eine Angestellte/r ist)					
Beschäftigt bei (Dienstgeber/in, Dienstort)					
Taxe		Gültig: 14 Tage ab Verordnung Datum:			
		Rp.			
		Abilify 10mg - Tabletten, 28 Stk.			
		1-0-0-0			
		Cymbalta 60mg - Hartkapseln, 28 Stk.			
		1-0-0-0			
		Trittico Retard 150mg - Tabletten, 20 Stk.			
		1/3-1/3-1/3-1			
		XST3 KU89 2344			
		Rezeptack. Nr.			
		Anzahl			
		Stempel der Apotheke/Hausapotheke			
		Stempel und Unterschrift des Arztes			
		Arztbescheinigung bei Rezeptgebührenbefreiung			

Quelle: ELGA Gesamtarchitektur v2.30a (Zeile 5693)

- Rollout bei niedergelassenen Ärzten laufend
- openNCP (EU)
- Patient Summary
- Patienten Verfügung
- Dokumentarten
- Bildgebung
- Impfpass
- eHealth
- CDA Levels

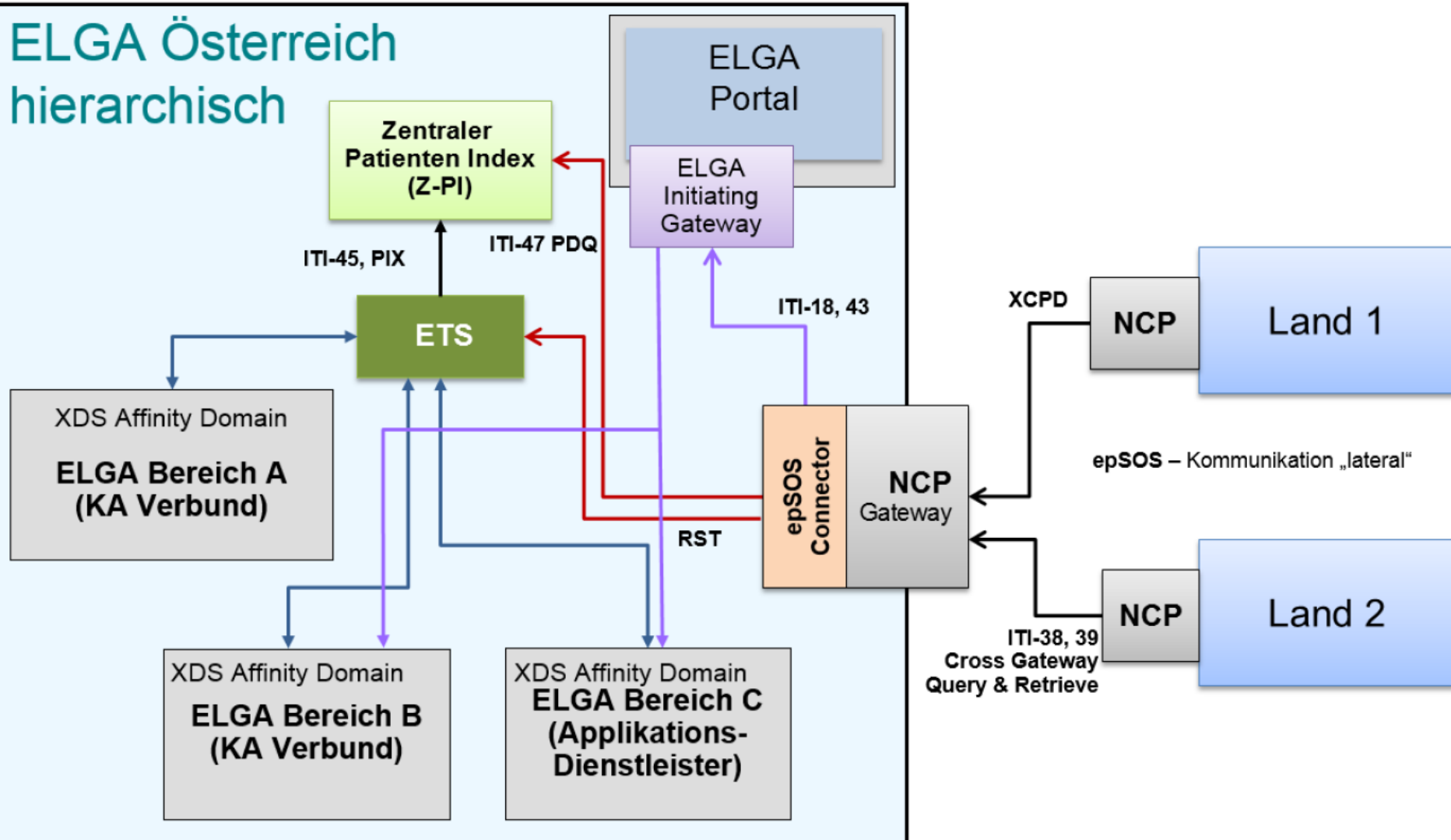
# Ausblick: Patientenverfügung



Quelle: ELGA Gesamtarchitektur v2.30a (Zeile 5840)

# ELGA und die EU

## ELGA Österreich hierarchisch



Quelle: ELGA Gesamtarchitektur v2.30a (Zeile 792)

# Bedeutung ELGA für Gesundheitswesen

- **Mit ELGA wurde eine Infrastruktur für den Gesundheitsbereich auf Basis von IHE Standards aufgebaut**
  - Health Care Providers (GDA-I)
  - Patient Identifier (Z-PI)
  - Policy Enforcement & Logging (BeS,A-ARR)
- **Möglichkeit durch minimale Anpassungen (Assertions, Policies) andere Applikationen auf Basis der vorhandenen Infrastruktur umzusetzen**

# ELGA Umsetzung/Betrieb

ELGA als Blaupause für eine „Private Cloud“



- **Stand 30.11.2016 (ca. 12 Monate nach Start)**

- 2 Bereiche seit 12 Monaten online
- 2 Bereiche seit 6 Monaten online
- 122 GDAs angebunden
- ~ 3.000.000 Dokumente
- ~ 1.300.000 Menschen haben Kontakte
- ~ 255.000 Menschen haben Opt-Out
- ~ 5.000 Menschen haben anderen Willen
- ~ 40.000.000 Transaktionen durchgeführt

- **Stand 30.04.2017 (ca. 17 Monate nach Start)**

- 13 Bereiche angebunden
- 200 GDAs angebunden
- ~ 6.870.000 Dokument einbracht (eBefunde)
- ~ 163.000 Verschreibungen (eMedikation)
- ~ 2.500.000 Menschen haben Kontakte (28,6%)
- ~ 262.000 Menschen haben Opt-Out (~3.0%)
- ~ 600.000 Transaktionen / Tag

- **Stand 31.03.2018 (ca. 28 Monate nach Start)**
  - 13 Bereiche online
  - 920 GDAs angebunden
  - niedergelassene Ärzte in Vorarlberg angebunden
  - ~ 16.500.000 Dokumente
  - ~ 1.500.000 e-Medikationen
  - ~ 4.700.000 Menschen haben Kontakte
  - ~ 7.100.000 Kontakte
  - ~ 268.000 Menschen haben Opt-Out
  - ~ 6.000 Menschen haben anderen Willen
  - ~ 620.000.000 Transaktionen durchgeführt
  - ~ 72.000.000 Transaktionen im Monat

- **Stand 31.10.2018 (ca. 35 Monate nach Start)**
  - 13 Bereiche online
  - 3.000 GDAs angebunden
  - niedergelassene Ärzte in Vorarlberg, Steiermark, Kärnten, Tirol angebunden
  - ~ 23.500.000 Dokumente
  - ~ 14.500.000 e-Medikationen
  - ~ 6.000.000 Menschen haben/hatten Kontakte
  - ~ 8.800.000 aktuelle Kontakte (1J)
  - ~ 44.000.000 Kontakte in Summe
  - ~ 285.000 Menschen haben Full Opt-Out
  - ~ 8.000 Menschen haben anderen Willen
  - ~ 260.000.000 Transaktionen durchgeführt
  - ~ 25.000.000 Transaktionen im Monat (aktuell)
  - ~ 165.000.000 im EBP einsehbare Protokolleinträge (3J)

- **Challenge Betriebsführung**
- **notwendige Hilfssysteme**
- **Verteilte Services**
- **Komponenten**
- **Netzwerke / DNS / Aufbau Global**
- **Tier 3 Modell (BRZ) / Loadbalancing**
- **Datenfluss / Sicherheit**

# ELGA Organisation



Meine elektronische  
Gesundheitsakte

## Eigentümer / Auftraggeber



BUNDESMINISTERIUM FÜR  
ARBEIT, SOZIALES, GESUNDHEIT  
UND KONSUMENTENSCHUTZ



Hauptverband der  
österreichischen  
Sozialversicherungsträger

## Continual Service Improvement

Service Strategy

Service Design



ELGA GmbH

Service Transition

Service Operations

**BRZ**

ELGA Betriebsführung



## Zentrale Dienste



**BRZ**

## ELGA Bereiche

### öffentlich rechtliche



NÖ Gesundheits- und Sozialfonds

**KABEG**

tirol kliniken



### private



health-net

SIEMENS  
Healthineers

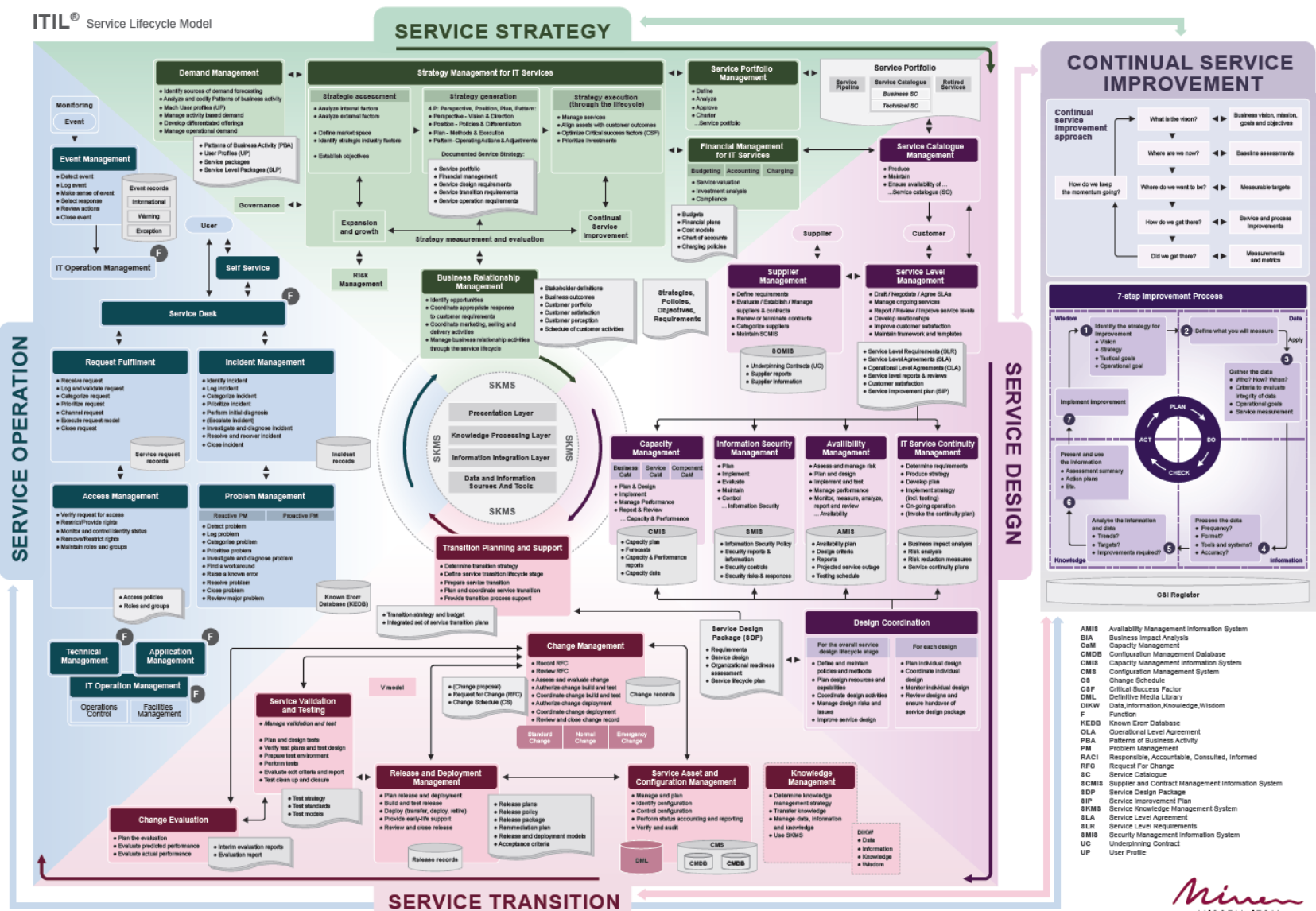
Quelle: interne Dokumentation, ©BRZ

# Challenge Betriebsführung

- **Betriebsverantwortung**
  - BMASGK (gesetzlicher Betreiber)
  - Übertragung von Betriebsaufgaben
- **ELGA Gesamtbetriebsführung (BRZ)**
  - Übergreifende Steuerung/Koordination Betrieb
- **zentrale Betreiber**
  - BRZ
  - SVC (Bürgerportal, eMed, Read-Only Zugang)
  - ITSV (Z-PI, Serviceline)
- **Bereichsbetreiber**
  - öffentlichrechtliche Betreiber
    - Länder: Wien, NÖ, ...
    - AUVA
  - private Betreiber
    - A1, HNET, AURA
    - eGor (Vinzenzgruppe, Barmherzige Brüder)

- **Problem: Hohe Gefahr von Inkompatibilitäten**
  - hohe Komplexität
  - sehr viele Partner
  - praktisch gesamtes Gesundheitssystem in Österreich betroffen
- **Lösung:**
  - Service Transition
    - Frühe Analyse von Änderungen  
Change Management
    - Stringente Release-Planung  
Release Management
    - essentiell für Erfolg:  
Transition-Planning und –Support
  - Staging
    - Umfangreiche Tests in mehreren Umgebungen

## ITIL® Service Lifecycle Model

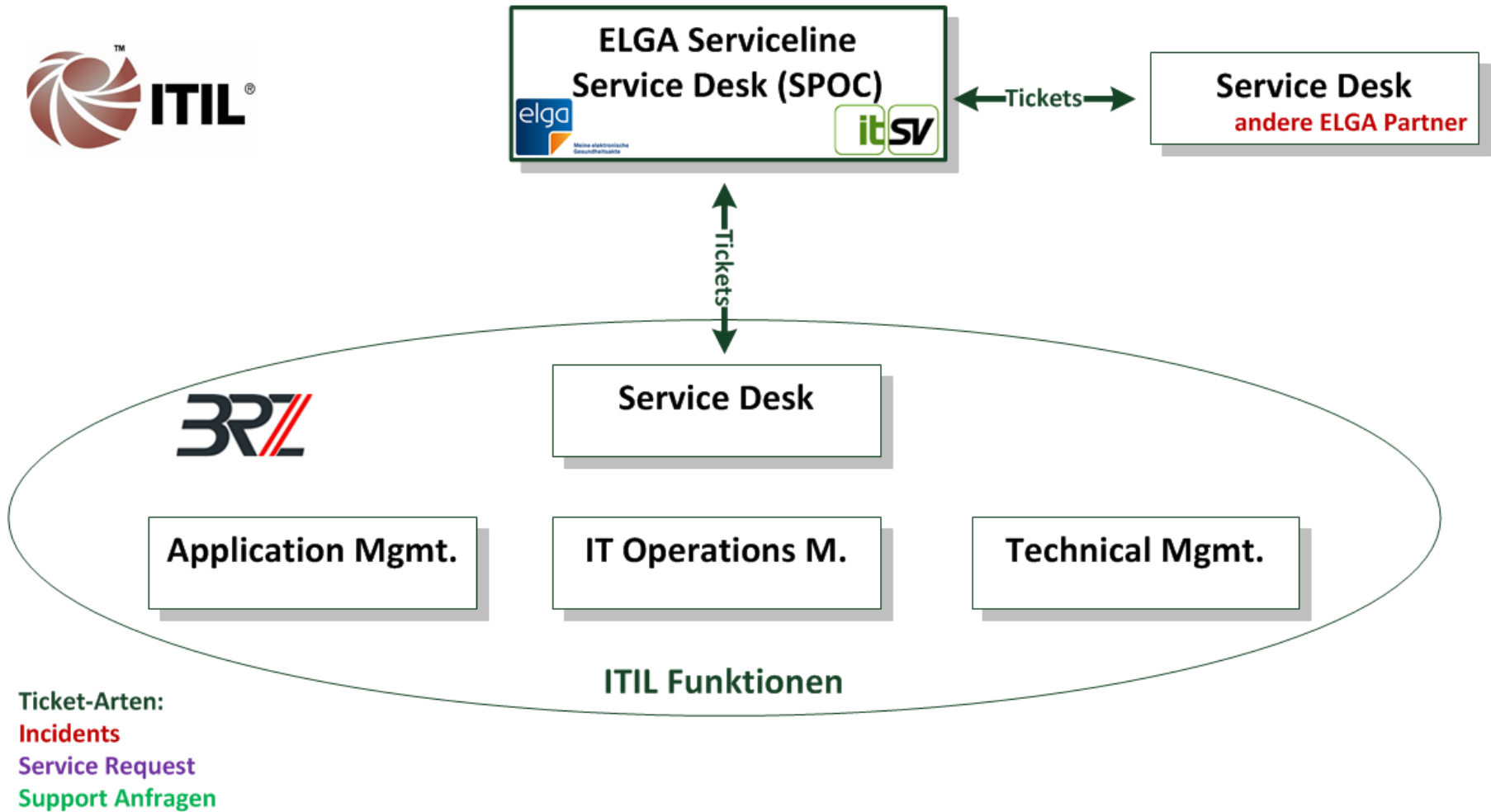


ITIL® is a Registered Trade Mark, and Registered Community Trade Mark of The Office of Government Commerce/Demand

Poster authors: Ivana Nissen, Maja Jagust | Copyright: ITS Partners: Croatia, www.bsn.hr, www.nissen.hr | Poster version 3.3, February 2014



# ITIL Funktionen

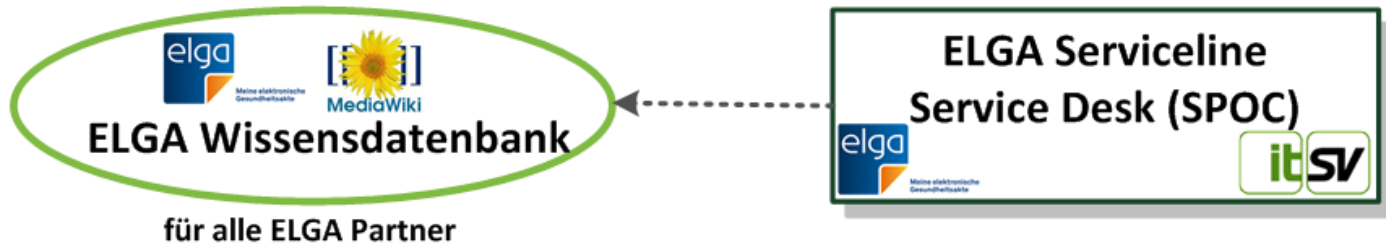


Quelle: interne Dokumentation, ©BRZ

- **ELGA Serviceline (ITSV)**
  - Single Point of Contact (SPOC)
  - für alle Organisationen
  - für Bürger
  - Helpdesk jeder Organisation  
intern als 1st Level vorgelagert
- **Service Requests**
  - normierte Abläufe (Prüfungen, Freigaben)
  - standardisierte Formulare
  - z.B. Firewallfreischaltung, Zertifikate, ....
- **Incidents**
  - Incidents mit einheitlicher Klassifizierung
  - Über alle Organisationen
  - 1 verantwortliche Rolle über alle Organisationen
- **Support Anfragen**
  - Unterstützung für Partner

- **Für ein Projekt bzw. einen Betrieb mit vielen Partnern sind einige Tools erforderlich**
  - Dokumenten Management (z.B. Sharepoint)
  - Sicherer Dokumentenaustausch  
(mit detaillierten Zugriffsrechten und zertifikatsbasierter Authentisierung)
  - Defekt-Management (JIRA)
  - Ticketsystem (für Incidents, Service Requests, Supportanfragen)
  - Umbrella Monitoring System
  - Wissensdatenbank (Wiki)
  - Wartungskalender (Betrieb)
  - Notfalltelefon (Bereitschaften der Partner)

# Dokumentation



Application Mgmt.

IT Operations M.

Technical Mgmt.

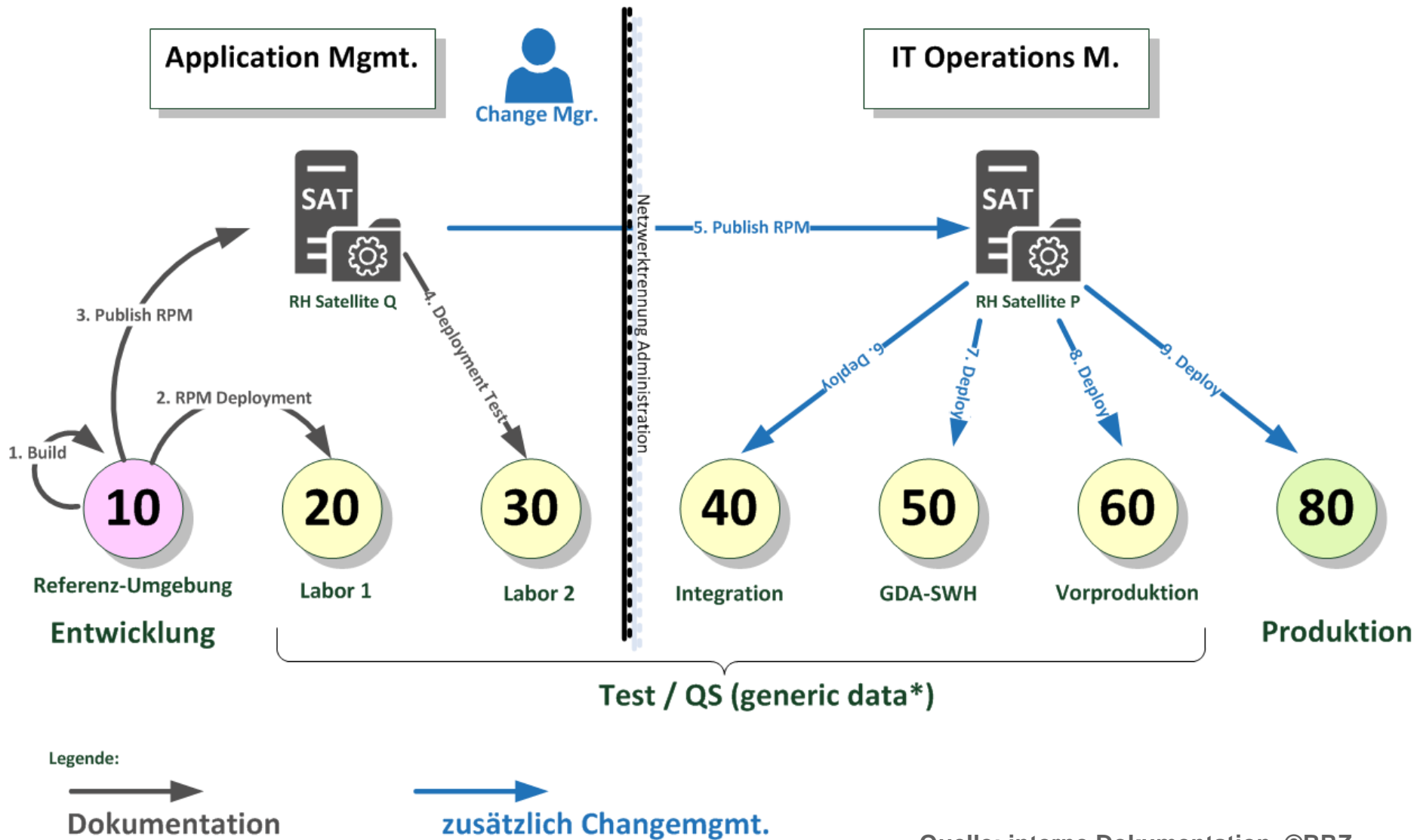


-----> inhaltliche Verantwortung/Befüllung



Quelle: interne Dokumentation, ©BRZ

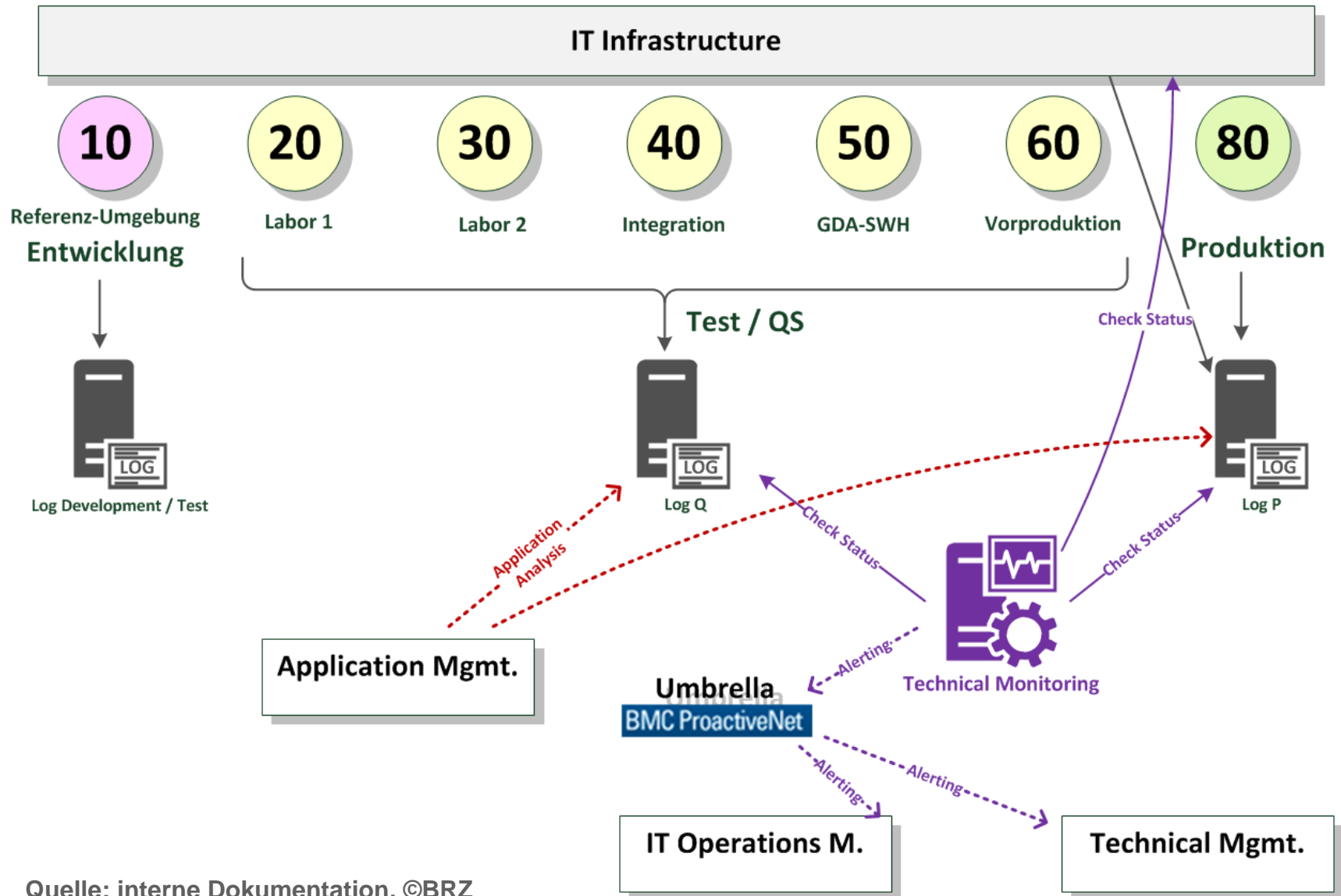
# Staging & Deployment



Quelle: interne Dokumentation, ©BRZ

- **Wie kann man das Verhalten des Gesamtsystems beeinflussen?**
  - SLAs für zentrale Komponenten und Services
  - SLAs für Bereiche
  - Antwortzeiten als Kriterium für Akzeptanz
  - Gemeinsame Service-Standards (inkl. Zeiten)?
  - Wie kann man Verfügbarkeit messen?
  - Pönalen im öffentlichen Bereich?
- **Was bedeutet das für ELGA-Partner?**
  - OLAs innerhalb der Organisation?
  - SLAs für Leitungen?
- **Wunsch SLAs und Budgets**

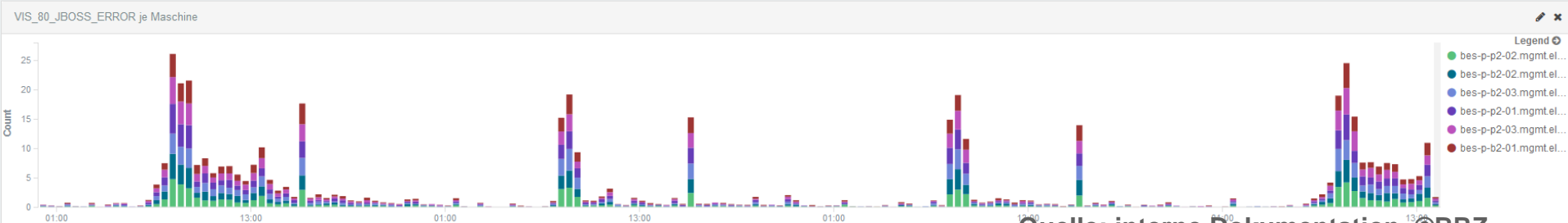
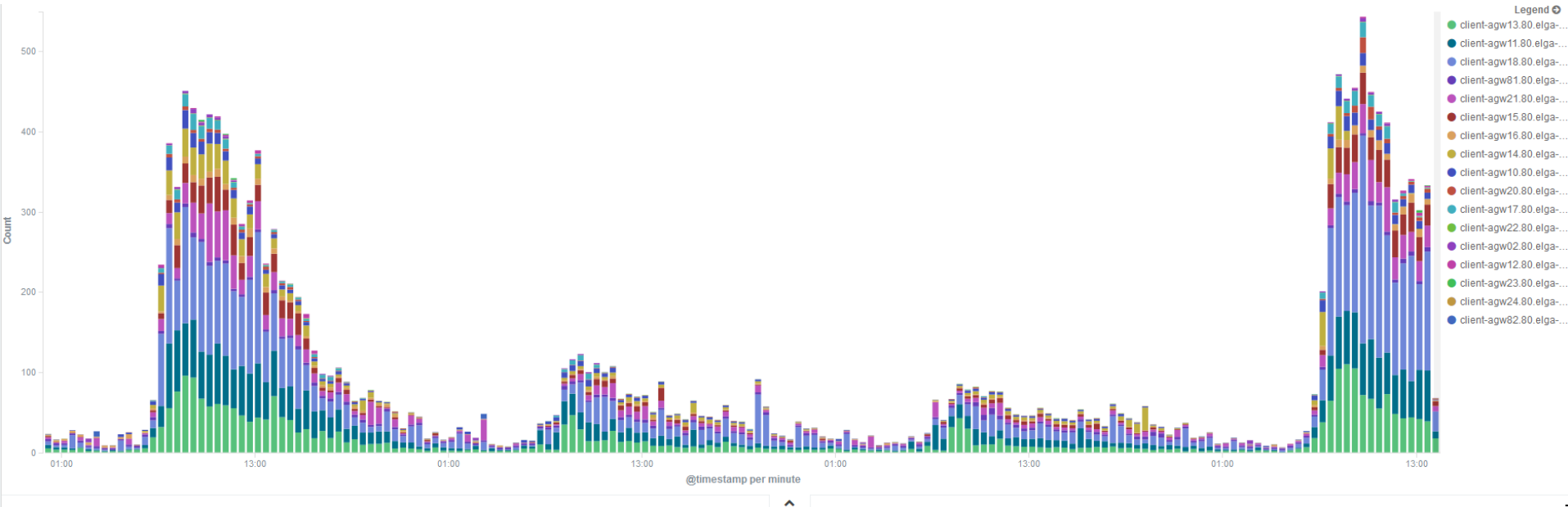
# Logfiles, Monitoring & Alerting



Quelle: interne Dokumentation, ©BRZ

# Logfile Aggregation

- Rückverfolgung einer Transaktion über die Systeme
- Gute Auswertbarkeit und Monitoring



Quelle: interne Dokumentation, ©BRZ



































# Umbrella Monitoring System



## Vorproduktion



Zentrale Komponenten ITSV	Zentrale Komponenten SVC - ELGA-Portal	Zentrale Komponenten SVC - SVC-RO	Zentrale Komponenten SVC - OBST
 Z-PI	 	 	 
Zentrale Komponenten BRZ - ELGA		Zentrale Komponenten SVC - eMedikation	
   BeS GDA-I OCSP - Q		 	
ELGA Vertretungsmodul (VEMO)			
 			
ELGA Bereiche			
             			
Status AGW ELGA Bereich			
Messtransaktionen ELGA Teilnehmer			
    			

Quelle: ELGA UMS

## Problem:

- Wie kann man bei der Kommunikation verteilte Services „normiert“ allen Betreibern zur Verfügung stellen?
- Wie kann man sicherstellen, dass jeder Betreiber bei seinen etablierten Namenskonventionen bleiben kann?

## Lösung:

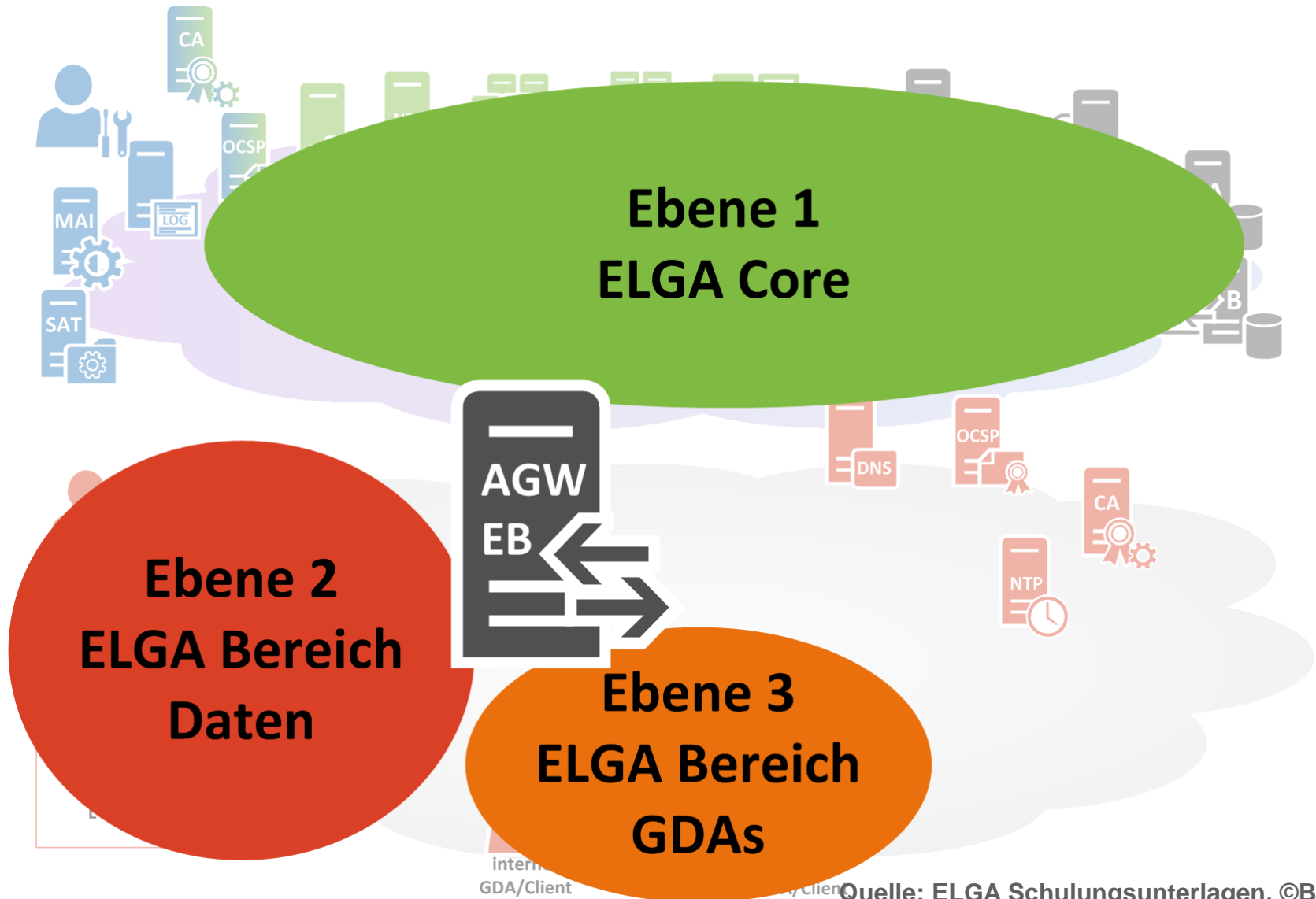
- Auftrennung in Ebenen (gemeinschaftlich / lokal)
- strikte Namenskonventionen für gemeinsame Kommunikation
- DNS als Schlüssel zum Erfolg
- Sicherheits-Proxy „AGW“ als konfigurierbarer Eintrittspunkt, welcher Reverse-Proxy Funktionalität bietet

Um die Kommunikation zu vereinfachen, wurde in ELGA folgendes Schema verwendet:

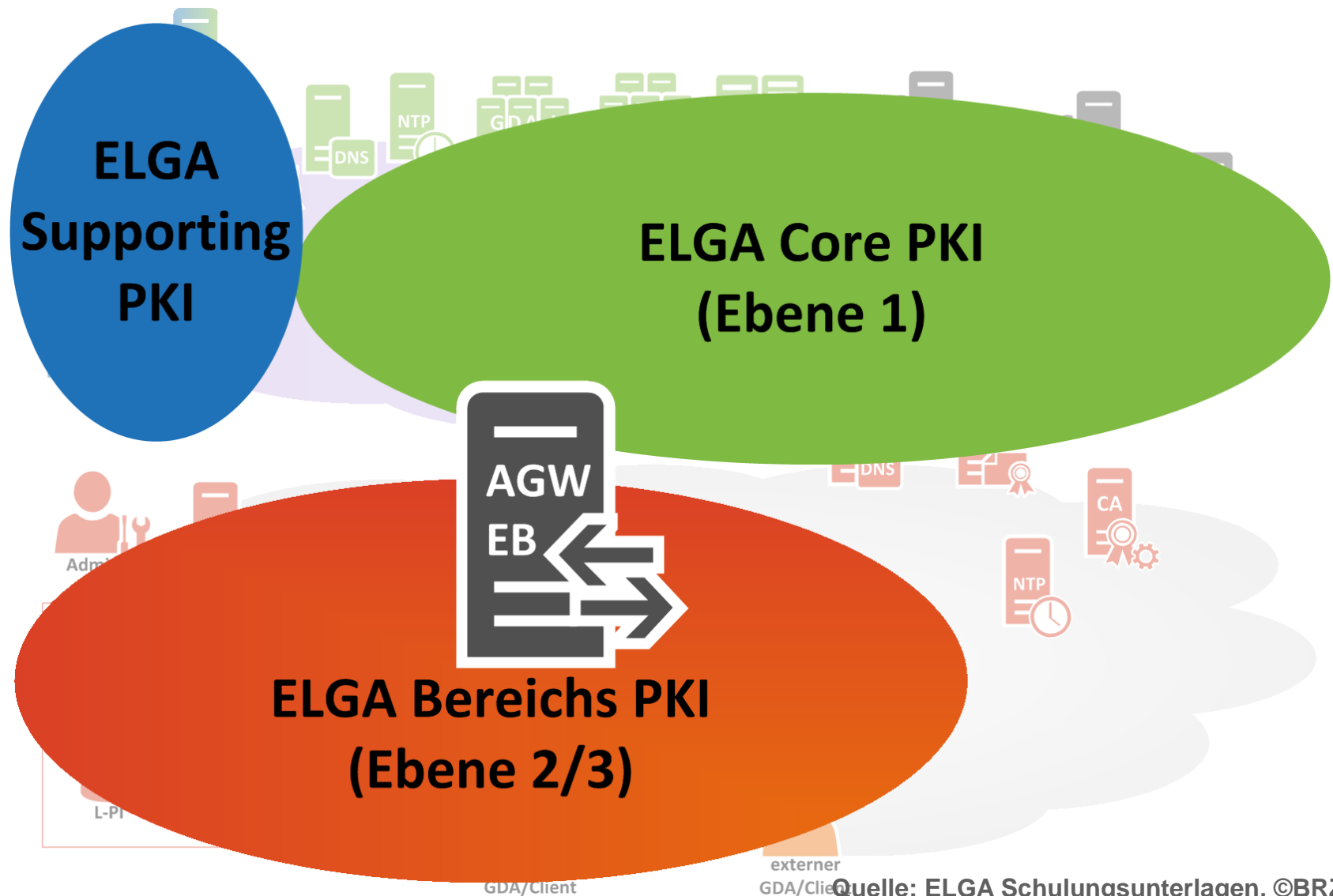
- Jedes Service wird folgendermaßen kodiert:  
`<service><betreiber>.<stage>.domain.at`
- Für Services gibt es ein Value Set  
(z.B. „dns“, „ntp“)
- Für Betreiber gibt es ein Value Set  
(z.B. „31“, „32“, ...)
- Für Stages gibt es ein Value Set  
(z.B. „32“, „99“, ...)

Dadurch kann sofort herausgelesen werden, um welches Service es sich handelt.

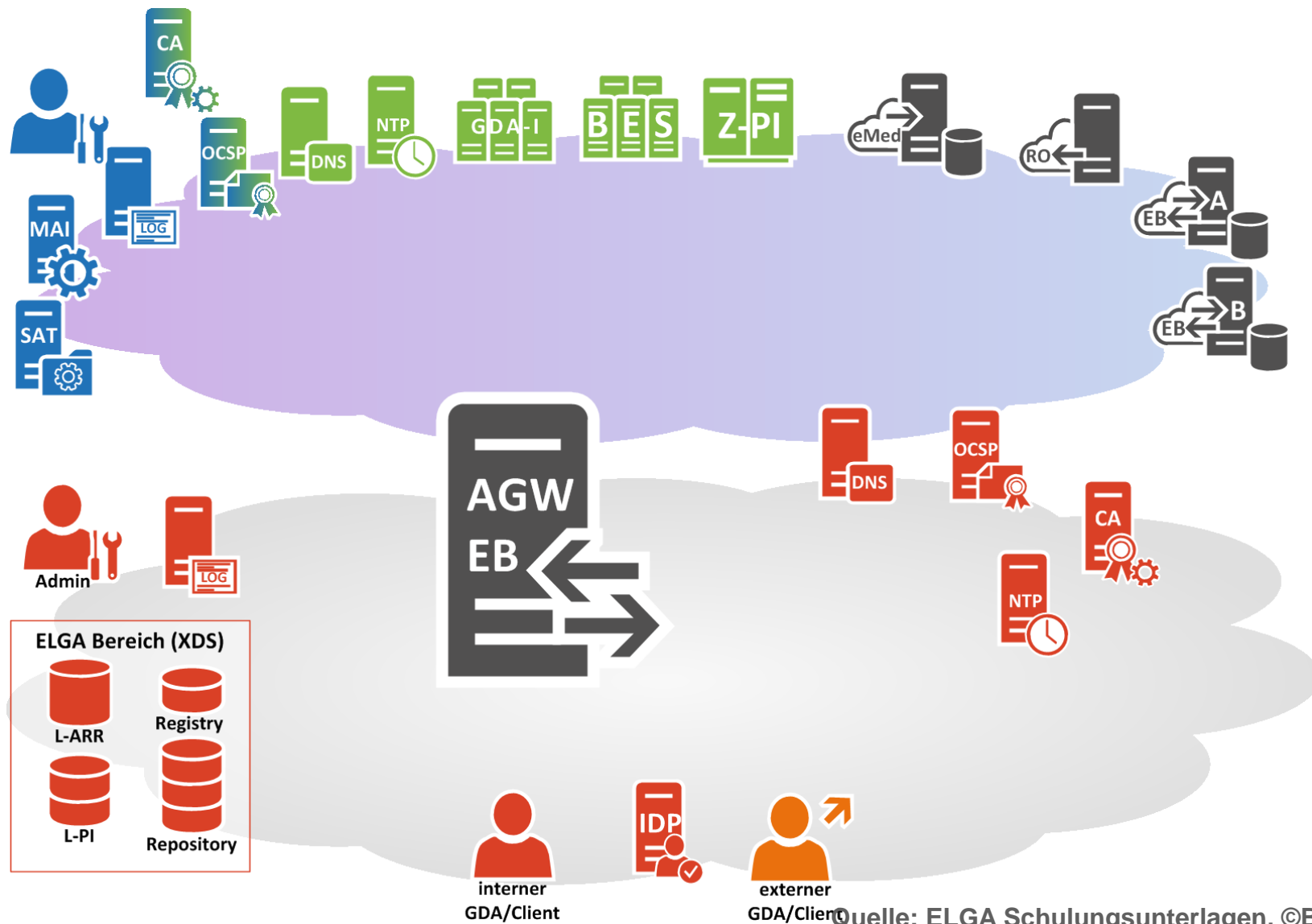
# Logische Ebenen



Quelle: ELGA Schulungsunterlagen, ©BRZ

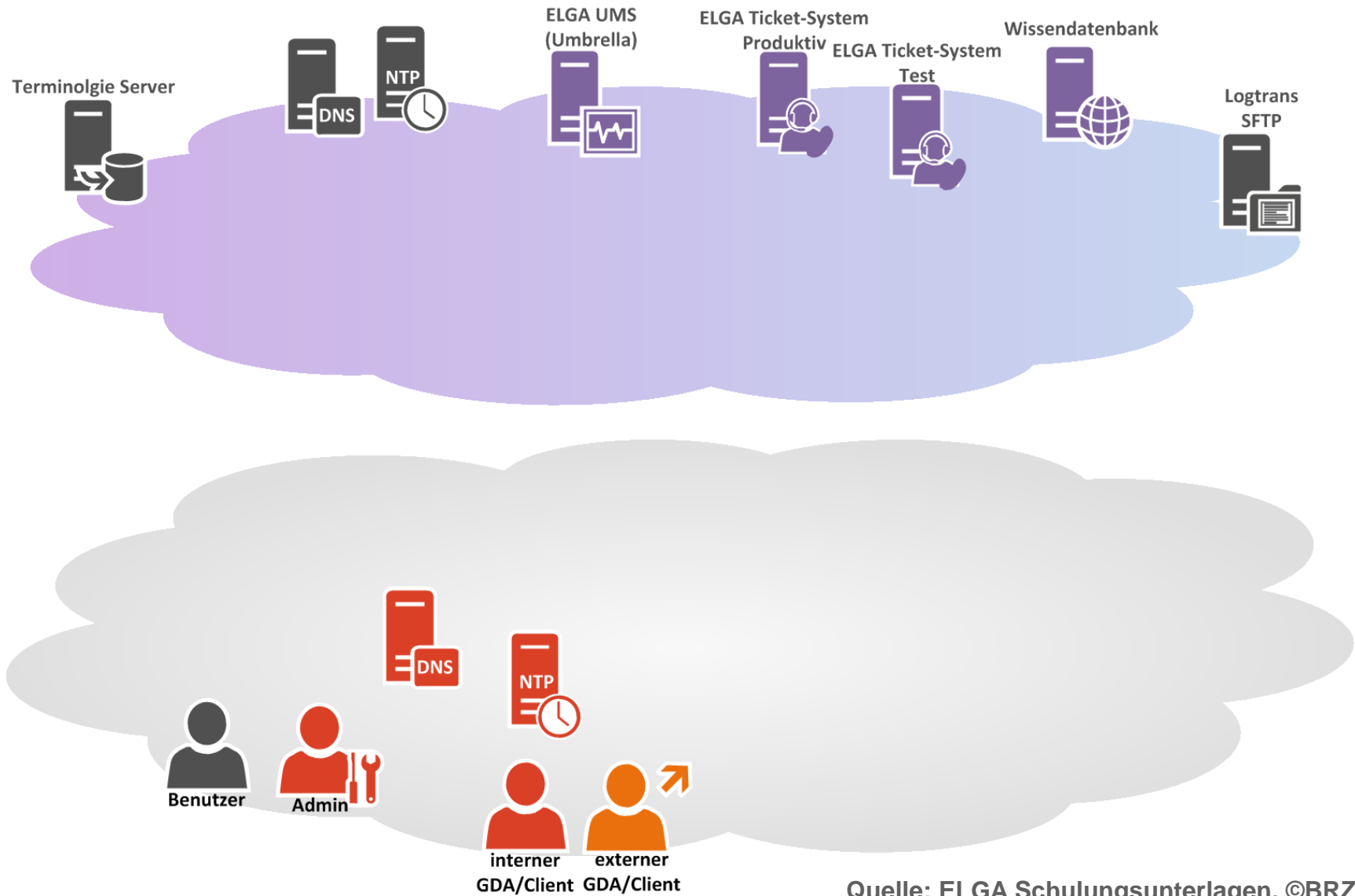


# Komponenten aus Sicht ELGA-Bereich



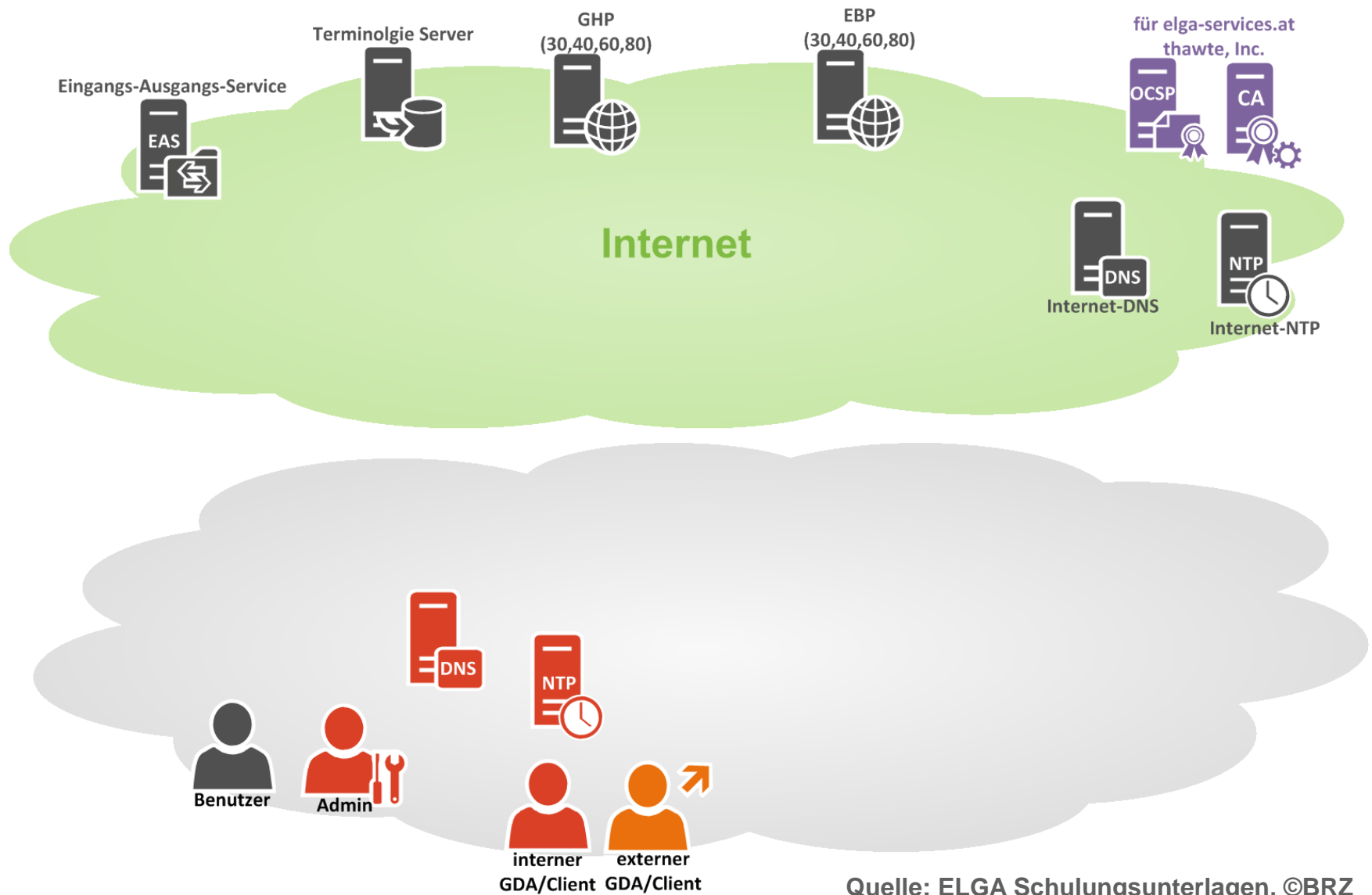
Quelle: ELGA Schulungsunterlagen, ©BRZ

# Hilfsservices Gesundheitsnetze



Quelle: ELGA Schulungsunterlagen, ©BRZ

# Hilfsservices Internet



Quelle: ELGA Schulungsunterlagen, ©BRZ



# 3-tier Modell

Alle Schichten sind voneinander getrennt.

Je nach eingesetztem System können beispielsweise Cluster oder lastverteilte Systeme eingesetzt werden.

Lastverteilte Systeme haben den Vorteil, dass man „in die Breite skalieren“ kann. Man fügt bei Bedarf einfach zusätzliche Server hinzu.

Beispielhafter Softwareeinsatz:

1. Apache mit SSL Terminierung
2. Applikation in JBOSS EAP
3. Daten in LDAP-Verzeichnisdienst

Firewall

Loadbalancer

**Tier 1  
(Sicherheit)**

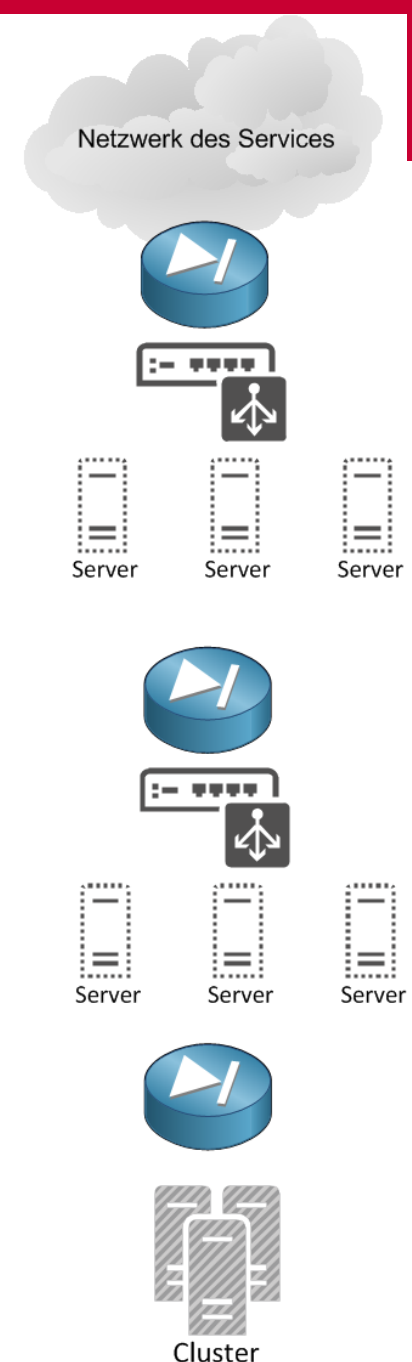
Firewall

Loadbalancer

**Tier 2  
(Anwendung)**

Firewall

**Tier 3  
(Persistenz)**



## ○ Vorteile

- Optimale Nutzung der Hardware
- Flexible Hardware Zuteilung im Betrieb
- Verschieben von Servern im Betrieb
- HA Option auch für nicht HA Systeme
- Monitoring
- Snapshots
- Unabhängig von „tatsächlicher Hardware“ (z.B. bei Treibern)

## ○ Nachteile

- Kosten für Virtualisierung
- Erhöhte Komplexität
- zusätzliche Fehlerquelle

- **Netzwerk**

- 50 VLANs
- 700 FW Objects
- 6500 FW Rules
  - ergibt ca. 1600.000 ACL Lines
- Redundante, hochverfügbare Anbindungen in Healix und eHiNet

- **Server**

- 52 physische Server im Workloadcluster
- 250 virtuelle Server
- 20 physische Server (DB, Backup, Supporting)

- **Storage**

- 360 HDDs
- 380 TB netto

## Wie lässt sich diese Infrastruktur verwalten?

### ○ **Technisch:**

- vmware
  - vSphere Suite
- Red Hat Satellite
  - gemanagtes Deployment von Software
- ELK (ElasticSearch)
  - zentrale Logfile-Verwaltung (auch von AGWs)
- Check\_MK
  - zentrales technisches Monitoring und Alarmierung

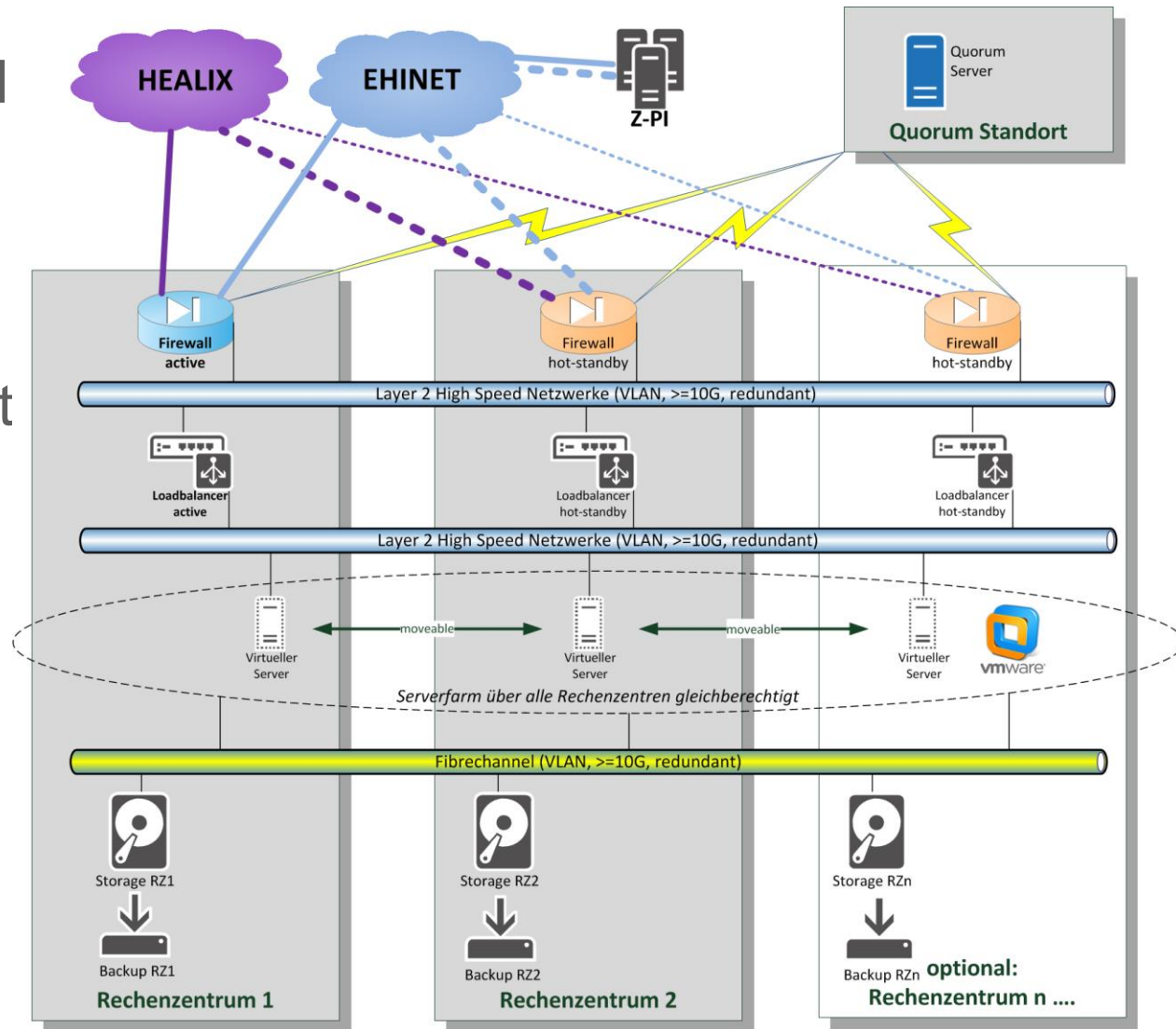
### ○ **Organisatorisch:**

- Klare Rolle / Verantwortungen
- Deployment Richtlinien
- Change Management
- Dokumentation, Dokumentation, Dokumentation

# Verteilte Standorte

Alle Standorte sind gleich-berechtigt.

Ein Quorum Standort verhindert das Split-Brain-Problem bei Clustern.



Quelle: Netzwerkkonzept BRZ

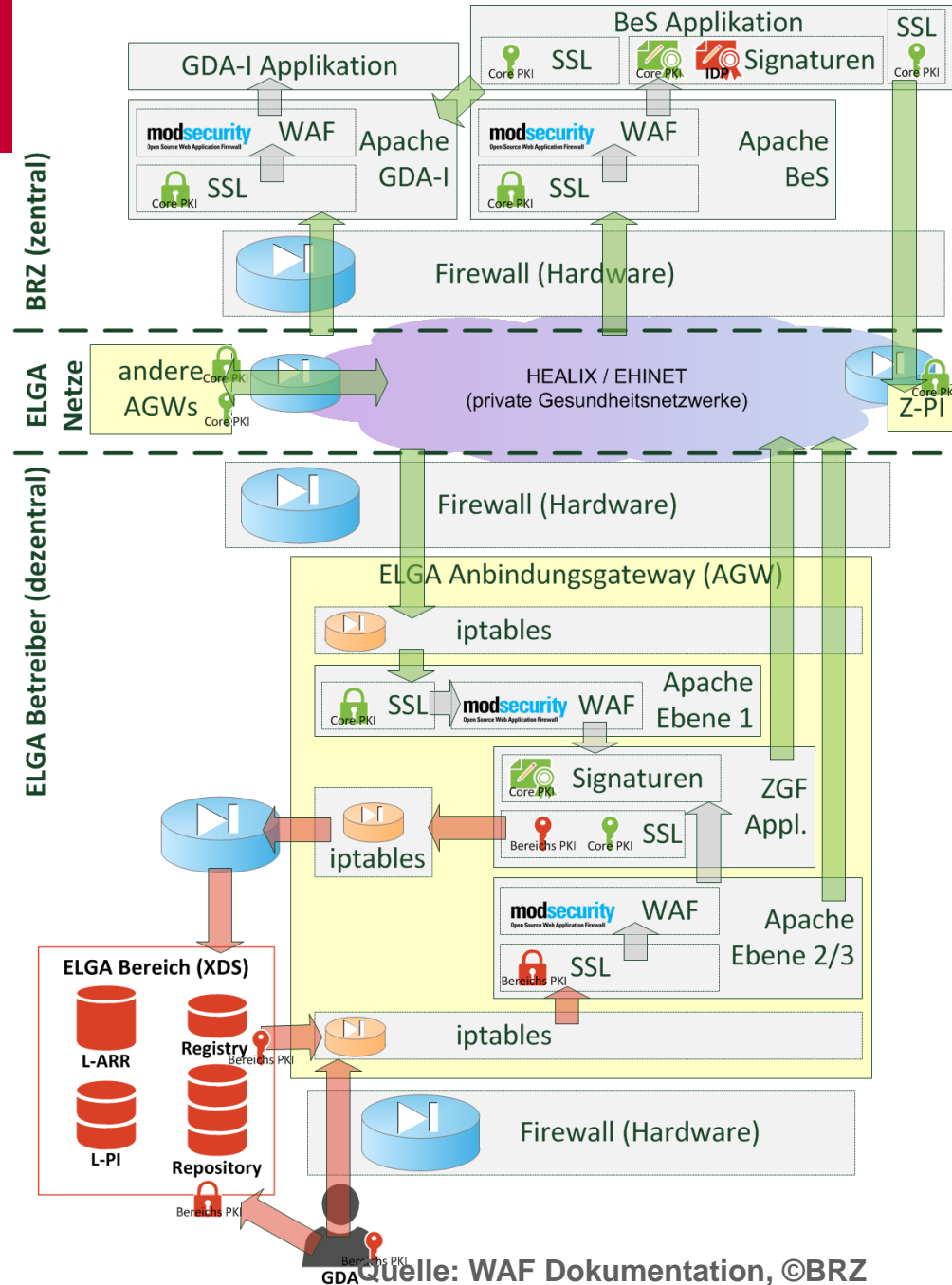
- **Was ist das AGW technisch?**
  - eine virtuelle Maschine (vmware) auf Basis RHEL mit 5 Netzwerkkarten
  - umgesetzt als Appliance (komplett menügeführt)
  - Sicherheits-Proxy, welcher die logische Ebene 1 (ELGA Core) von den Ebenen in Verantwortung des Bereichs trennt (Ebene 2 Datenspeicher, Ebene 3 GDAs)
  - kann redundant betrieben werden (Loadbalancer erforderlich)
  - Remotesupport durch Hersteller (BRZ) nach Kundenanforderung und -freigabe möglich
  - Updates bequem menübasiert
  - übermittelt seine Logfiles permanent (ELK)

## Sicherheitsschichten

Jeder Zugriff in ELGA wird auf mehreren Sicherheitsschichten geprüft.

Eine zentrale Rolle spielen dabei private PKIs zur Absicherung der gemeinschaftlichen Kommunikation und der jeweiligen bereichs-internen Kommunikation.

Zusätzliche wird der Verkehr durch WAFs geprüft.



Quelle: WAF Dokumentation, ©BRZ

**Mag. Alexander Stromberger**