

Positionspapier: Portalverbund und eHealth

e-Government Arbeitsgruppe
„Integration und Zugänge“
(AG-IZ)

Dr. Wilfried Connert
Franz Hoheiser-Pförtner, MSc
Rainer Hörbe
Peter Pfläging

Juli 2009

Inhalt

Zielsetzung

Wozu PV?

Was ist der PV?

Warum PV?

Nutzen

Erweiterung der Architekturvision

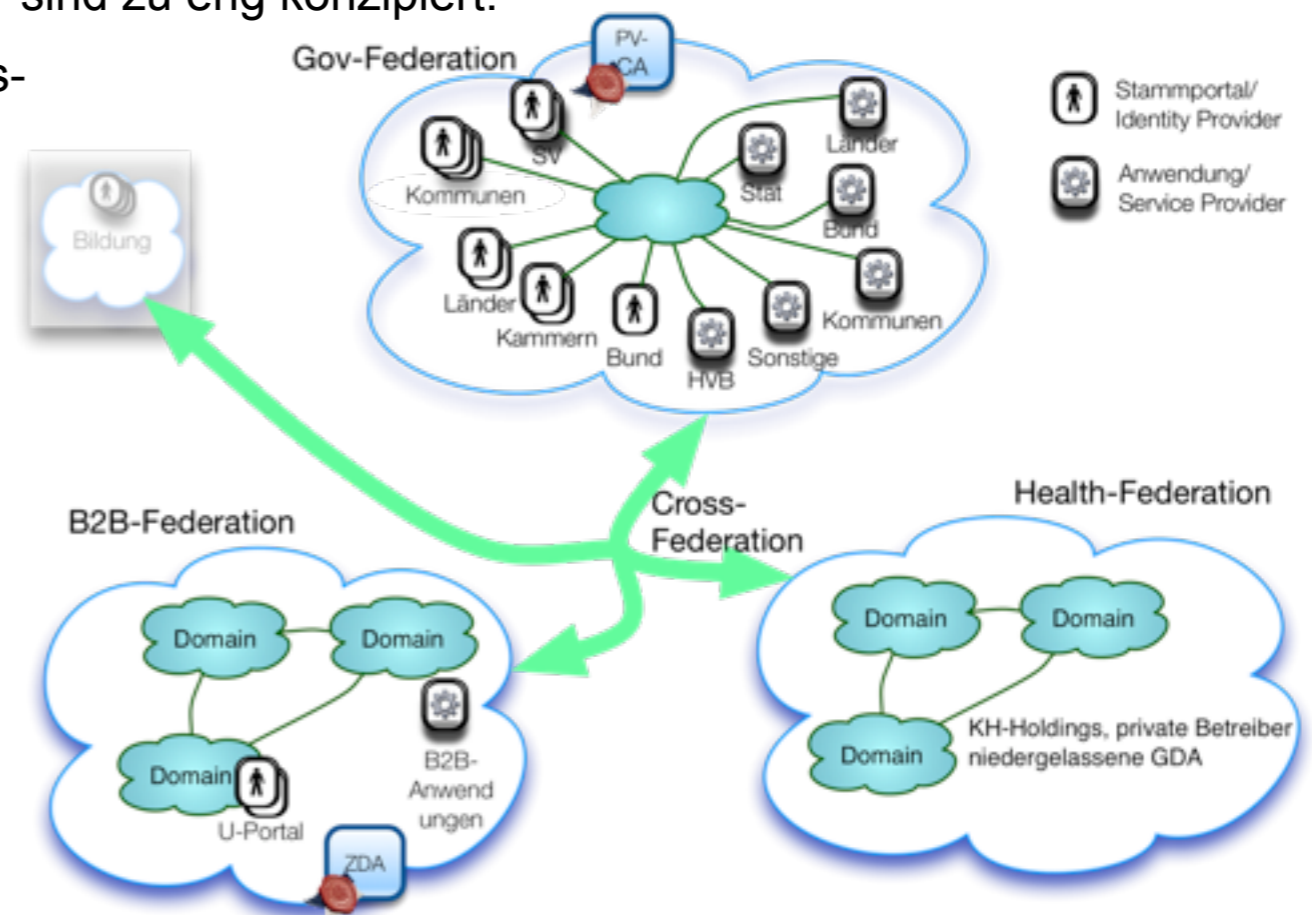
Zielsetzung

- zu kommunizieren, warum das Konzept des Portalverbunds ein Baustein für eHealth werden soll
- die wesentlichen Konzepte des Portalverbunds darzustellen
- zu diskutieren, welche Schritte für eine Umsetzung unternommen werden müssen

Wozu der Portalverbund benötigt?

- Status Quo: IAM-Systeme im Gesundheitswesen sind redundant und nicht interoperabel
- Vernetzung geht über den Datenaustausch zwischen GDA hinaus. Die IAM-Systeme der verschiedenen Bereiche müssen interoperabel sein.
- Im Rahmen von ELGA ist ein Federated Identity + Access Management

- Im Gesundheitswesen werden für unterschiedliche, sich vielfach überschneidende Benutzergruppen separate Identitäts- und Zugriffsmanagementsysteme verwendet. Beispiele sind GIN/eHI-Net, ELDA, SV-Portal, Bürgerkarte/GDA-Token, Verwaltungs-PV, ELGA-Portal, Befundprovider, Kammern, Netzwerke der KH-Träger.
- Gesundheitsdienstleister sind mit anderen GDA (einschließlich Government bei Übermittlung von Gesundheitsdaten), Government, Landesvertretung, Forschung und Wirtschaft vernetzt, auch international. Branchenspezifische Lösungen - nur für das Gesundheitswesen - sind zu eng konzipiert.
- Um Vernetzung, Prozessintegration zwischen GDA und die Einführung neuer Anwendungen zu fördern ist eine Architektur für ein föderiertes Identitätsmanagement notwendig



Was ist der Portalverbund?

- Teilnehmer bilden einen „Circle of Trust“
- Anwendungen delegieren die Verwaltung und Authentifizierung an Identity Provider

Definition: „Mit „Portalverbund“ ist eine rechtliche, organisatorische und technische Kooperation der Teilnehmer gemeint, bei der ein Anwendungsverantwortlicher einem Identity und Attribute Provider vertrauen kann, dass die Identität und die Attribute von Benutzern einer vereinbarten Sicherheitsstufe entsprechen.“

IT-technisch gesehen handelt es sich um ein „Federated Identity Management“, wo die Partner mit vertraglich geregelten Vertrauensstellungen einen „Circle of Trust“ bilden.

Aus der Sicht des Sicherheitsmanagements regelt der Portalverbund die Authentifizierung und Autorisierung externer Zugriffe auf rechtlicher und technischer Ebene.

Portalverbund

	Recht	Organisation	Technik
Registry		Einheitliche Semantik und Prozesse; Normen-Konformität	LDAP/UDDI, ..
Access Security	Verträge	Policy Administration	Policy Enforcement, IT-Grundschutz
Network Security		Network Policy, CERT	Firewall, Sec. Admin
Connectivity		(SLA)	Internet

Warum der Portalverbund?

- Portalverbund = Federated Identity Management
- offen für verschiedene technische Protokolle
- Ausgereiftes Konzept
- Authentifizierung *und* Autorisierung
- Der Portalverbund implementiert das Konzept föderierter Identitätsmanagementsysteme und ist offen für verschiedene technische Protokolle nach Industrienormen wie SAML, OpenID und WS-Trust.
- Die Implementierung in der Verwaltung ist ausgereift und seit Jahren im Betrieb.
- Der Portalverbund erweitert IDM-Systeme zur Authentifizierung um delegierte Zugriffsberechtigungen

Nutzen des Portalverbunds

- einheitliche Zugriffskontrolle, optimierte Benutzer- und Rechteverwaltung
- Unternehmensübergreifende Integration von Prozessen
- Reduktion von Komplexität und Kosten

Damit können parallele Geschäftsprozesse und IT-Services konsolidiert werden. Das bedeutet also:

- Die Verwaltung von Benutzern und ihren Rechten erfolgt dezentral, beim Benutzer oder seiner Stammorganisation. In Kliniken bedeutet das (im Ideal) die Verwaltung eines Benutzers und seiner Rechte an nur einem Punkt, egal ob es sich um interne oder externe Anwendungen, gleichgültig, ob es sich um die Bereich Verwaltung, Medizin, Forschung oder Government handelt. Dies reduziert Aufwand bei der Nutzer- und Rechtsverwaltung.
- Es erhöht die Sicherheit, da die Zusammenschau der Rechte einer Person gegeben ist und auf Änderung im Bestand und Verwendung gezielt reagiert werden kann.
- Es muss nicht in jeder Anwendung die Funktionalität einer Benutzer und Rechtsverwaltung implementiert werden.
- Die Anzahl der Nutzungs- und Sicherheitsvereinbarungen wird drastisch reduziert, weil nur mehr eine Vereinbarung pro Identity Provider, und nicht mehr pro Service Provider erforderlich ist.
- Mit der Konsolidierung unterschiedlicher Sicherheitsregimes wird die Komplexität der Sicherheitsmaßnahmen stark reduziert, wodurch bei geringerem Verwaltungsaufwand eine bessere Sicherheit erzielt werden kann.

Erweiterung der Architekturvision

Zielsetzungen

1. Die Stakeholder (GDA, e-Gov, Bildung, Wirtschaft, ..) haben ein klares Verständnis für den Nutzen der Kooperation im Portalverbund und haben interoperable Schnittstellen und Dienste für Identity und Access Management
2. Der PV ist aus einer Sicherheitsarchitektur für Authentifizierung und Autorisierung abgeleitet
3. Die Struktur für Einrichtung, Betrieb und Governance wird kooperativ vereinbart

Anforderungen

1. Benutzeridentitäten konsistent, verlässlich und vertrauenswürdig bereitstellen
2. Unterstützung unterschiedlicher Authentifizierungsverfahren und -protokolle
3. Multi-level Security für Authentifizierung und Anwendung
4. Online-Anwendungen und digitalen Signaturen in einer Architektur unterstützen
5. Benutzer können EPU, KMU oder große Organisationen sein
6. Identitäten, Attribute und Berechtigungen möglichst an der Quelle verwalten
7. Verteilte Systemtopologie zur Unterstützung kritischer Infrastruktur

Prozess

1. Einbeziehung der Stakeholder
2. Abstimmung und Anpassung der Architektur
3. Vertragsvorlage an Anforderungen e-Health anpassen
4. Koordination mit laufenden Projekten (epSOS, ELGA, SV, eGov, ..)
5. Review der technischen und vertraglichen Ergebnisse
6. Verifikation der Ergebnisse in Pilotprojekten

Ergebnis

1. Architektur für Identity Federation im Gesundheitswesen und mit anderen Bereichen
2. Vertragliches Rahmenwerk für Gesundheitsportalverbund sowie Ernennung eines Depositars
3. Bericht über die Pilotierung des Systems

Evaluierung

Um das Risiko zu reduzieren, dass das Konzept zu abstrakt bleibt und nicht praktisch evaluiert wird, ist das Konzepts in Pilotprojekten umzusetzen.

- Bestehende Portal-Infrastruktur im HVB und den Gebietskörperschaften könnte über Gateways eingesetzt werden, um den Initialaufwand zu verringern.
- Besser geeignet sind Projekte, die in der Planungsphase sind.
- ELGA als Leitprojekt ist mit dem PV-Konzept abzustimmen
- Anfrage wegen aktueller Projekte bei Landesgesundheitsfonds, Sanitätsbehörden, BMG, AGES, etc.
- e-Medikation bietet sich an

Evaluierungsziele

- Kompatibilität mit eHealth-Normen (z.B. IHE XUA)
- Konformität mit dem Rechtsrahmen