PORTALVERBUNDKOMMUNIKATION IM ÖSTERREICHISCHEN GESUNDHEITSWESEN

Hoheiser-Pförtner F[1], Hörbe R[2]

Kurzfassung

Die Portalverbundkommunikation im österreichischen Gesundheitswesen ist eine Empfehlung zur Erweiterung der Portalverbundkommunikation des E-Governments Bund-Länder-Gemeinden in der Republik Österreich. Der Portalverbund im österreichischen Gesundheitswesen stellt einen einheitlichen Rahmen für den Zugriff auf verschiedene Informationssysteme der Gesundheitsdiensteanbieter und eine dezentrale Verwaltung der zugehörigen Rechte dar. Damit haben die Gesundheitsdiensteanbieter die Möglichkeit, dass der Benutzer und seine Rechte unabhängig von der Anzahl der verwendeten Anwendungen an einer Stelle – dort wo der Benutzer personell zugehörig ist – verwaltet wird. Zur Sicherstellung einer einheitlichen Sicherheitspolitik sowie der Festlegung der organisatorischen Zuständigkeiten müssen sich die Teinehmer am Portalverbund zur Einhaltung der Regelungen der Portalverbundvereinbarung verpflichten. (Bei allen personenbezogenen Bezeichnungen gilt die gewählte Form für beide Geschlechter)

1. Einleitung

Für ein einheitliches E-Health ist eine gut funktionierende, über lokale Grenzen hinweg reichende Kooperation der Gesundheitsdiensteanbieter ausschlaggebend. Durch den Zusammenschluss von Gesundheitsportalen werden Anwendungen einzelner Gesundheitsdiensteanbieter im Verbund zugänglich gemacht. Welche Anwendung über welches Portal zugänglich gemacht wird, bestimmt der Gesundheitsdiensteanbieter. Der Gesundheitsdiensteanbieter legt je nach gesetzlichen Bestimmungen fest, welche Organisationseinheiten zugriffsberechtigt sind. Die Zugangsrechte der Benutzer werden nach Aufgabenstellung definiert. Die Betreiber von Anwendungsportalen delegieren die Authentifizierung und Zugangsautorisierung an Stammportale anderer Gesundheitsdiensteanbieter im Portalverbund. Als Vorteile ergibt sich ein reduzierter Aufwand für die Benutzerverwaltung und eine einfachere Verwaltung der Zugangsrechte durch einen „Single Point of Administration“. Das Führen paralleler Verzeichnisse ist somit nicht mehr notwendig. Bisherige Parallelentwicklungen können in Zukunft vermieden und Kosteneinsparungen für alle Beteiligten erzielt werden. Der erweiterte Portalverbund ist ein Zusammenschluss von Gesundheitsportalen zur gemeinsamen Nutzung bestehender Infrastrukturen. Gesundheitsportalverbundbetreiber sind angehalten, die Portalverbundvereinbarung umzusetzen. Das Verbundsystem erlaubt teilnehmenden Organisationen, ihre eigene Benutzerverwaltung auch für externe Applikationen einzusetzen. Die Applikationsbetreiber ersparen sich dadurch die Benutzerverwaltung von externen Nutzern.

1 Wiener Krankenanstaltenverbund, Generaldirektion, IKT-Koordination, Wien

2 BEKO Informatik,Wien

Die Applikationen selbst sind Web-Anwendungen, die sich auf Hypertext Transfer Protocol (HTTP) oder Simple Object Access Protocol (SOAP) stützen. Über den Portalverbund können mehrere Applikationen über einen Punkt erreicht werden. Auf Gesundheitsanwendungen im Portalverbund können nur Nutzer zugreifen, die von ihrem Stammportal dazu autorisiert worden sind. Dabei wird geprüft, ob das Rechteprofil mit den Zuständigkeiten der zugriffsberechtigten Stelle übereinstimmt. Die Nutzerverwaltung verbleibt bei der jeweiligen personalführenden Stelle. Die Kommunikation im Portalverbund ist durch das Portalverbundprotokoll und durch die Festlegung von Sicherheitsklassen geregelt.

2. Portaldefinition

Portale dienen zur Aggregation und Präsentation von Inhalten. Dabei kann diese Darstellung in personalisierter Weise oder in allgemeiner Form erfolgen. Portale stellen nicht nur Informationen sondern immer mehr auch Applikationen bereit, um ihren Benutzern eine zentrale Kommunikations- und Informationsplattform zu vermitteln.

3. Portalverbund im E-Government

Der Einsatz von Anwendungsportalen ist eine wichtige Komponente des Konzepts für E-Government von Bund, Ländern und Gemeinden.

Grundsätzlich haben Portale im Portalverbund des E-Government den Nutzen, dass mehrere Anwendungen über einen Punkt adressiert werden und der Benutzer sich nur einmal authentisieren muss. Die Richtlinien für die Zugriffe werden außerhalb der Anwendungen am Stammportal administriert und erzwungen.

4. Verwaltungsvereinfachung „Single Point of Administration“

Mit „Single Point of Administration“ wird die redundante Verwaltung von Benutzern, ihren Rechten und Verrechnungsattributen am Anwendungsportal ersetzt. Es ergeben sich daher folgende Vorteile:

- Die Verwaltung der Benutzer wird technisch und organisatorisch bei der jeweiligen personalführenden Stelle belassen, um eine Verwaltungsvereinfachung zu erzielen. Die Arbeitsabläufe für Beginn, Änderung und Beendigung von Dienstverhältnissen so wie organisatorischen Veränderungen werden damit erheblich vereinfacht.
- Durch den Wegfall redundanter Benutzerdatenbanken erzielt man eine bessere Datenkonsistenz und in der Folge einen besseren Datenschutz.
- Benutzer erhalten rascher Zugriff auf Anwendungen.
- Durch die Verwendung eines Anwendungsportals auch für interne Anwendungen ergeben sich weitere Synergieeffekte, weil die Benutzer und ihre Rechte an einer Stelle für interne und externe Anwendungen administriert werden.

5. Implementierung Portalverbund

Die Basis des Portalverbundprotokolls ist HTTP oder SOAP. Zur Authentifizierung wird das Stammportal als Proxy für Zugriffe auf Anwendungsportale verwendet. Die Protokollbindung für SOAP verwendet und erweitert die Spezifikation Web Services Security [1]. Details der Implementierung sind in der gültigen Fassung im Portalverbundprotokoll [2] beschrieben. Das Portalverbundprotokoll unterstützt die Implementierung von WebServices. Gegenüber bisherigen Konzepten für verteilte Anwendungen liegt der Vorteil von WebServices neben der Plattformneutralität und

Offenheit in der Einfachheit und Robustheit. WebServices werden in den nächsten Jahren auch im Gesundheitswesen vermehrt eingesetzt, weil sie erstmalig in größerem Umfang eine Maschine-Maschine-Kommunikation ermöglichen. Die hierbei verwendeten Spezifikationen sind zwar zum Teil noch in der Entwicklung und Abstimmung beim World Wide Web Consortium (W3C), gewinnen aber weltweit schnell an Bedeutung. Zwischenzeitlich haben sich bereits Initiativen gebildet, die auch im Rahmen der Weiterwicklung eine zukünftige Interoperabilität gewährleisten sollen.

6. Vertrauensverhältnisse

Der Anwendungsverantwortliche der Anwendung A_1 delegiert die Funktionen Authentifizierung und Autorisierung der Benutzer an den Betreiber des Stammportals. In diesem Zusammenhang wird die Summe der für die Anwendung A_1 möglichen Rechte und Einschränkungen definiert. Das Anwendungsportal und das Stammportal authentisieren einander über Zertifikate.

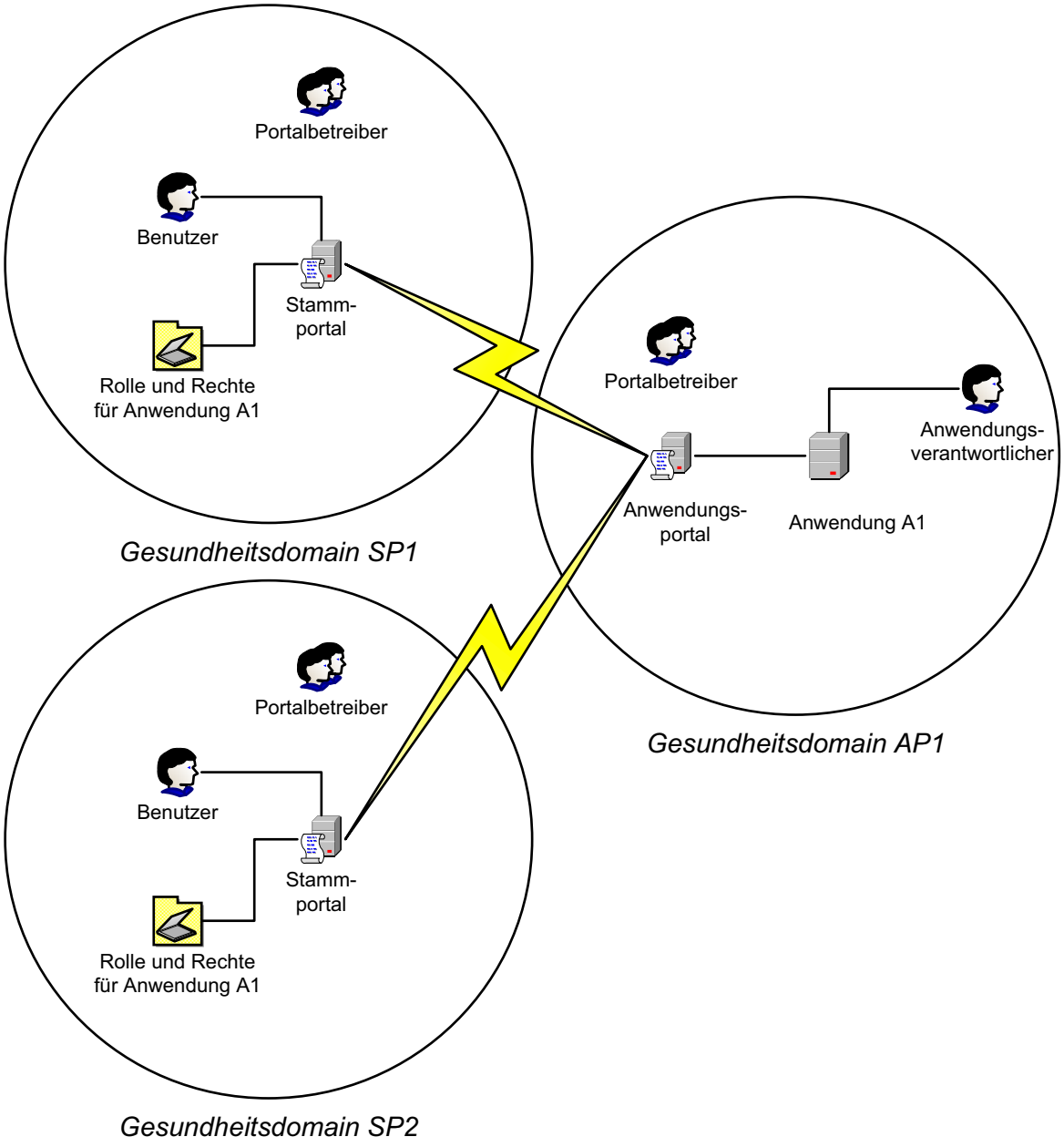

Abbildung 1

Der Anwendungsverantwortliche hat mit den Organisationen SP1 und SP2 eine Anwendungsvereinbarung für die Anwendung A_1 geschlossen. In der Folge wird dem Stammportal SP1 und SP2 am Anwendungsportal AP1 die in der Nutzungsvereinbarung definierten Rechte eingeräumt. Die Stammportalbetreiber von SP1 und SP2 definieren, welchen Benutzern der Organisation der Zugriff auf die Anwendung eingeräumt wird.

7. Sicherheitsklassen

Die Definition und Abbildung von Sicherheitsklassen ermöglicht es einer Anwendung zu prüfen, ob ein Benutzer die für die Nutzung der Anwendungsfunktion erforderlichen Sicherheitsauflagen erfüllt, auch wenn für Benutzer und Anwendungsbetreiber unterschiedliche Sicherheitsnormen gelten. Der Schutzbedarf von Anwendungen einerseits und Sicherheitsmaßnahmen der Benutzer und ihrer Systeme andererseits werden in einem Schema mit Sicherheitsklassen kategorisiert. Die Prüfung der Sicherheitsklasse des Benutzers erfolgt zum Zeitpunkt des Zugriffs auf die Anwendung automatisch. Die Anwendung kann damit sicherstellen, dass der Benutzer mindestens die Anforderungen der von der gewünschten Anwendungsfunktion vorgegebenen Sicherheitsklasse erfüllt. Wenn nun eine Anwendungsfunktion eine höhere Sicherheitsklasse verlangt als der Benutzer hat, wird der Zugriff abgelehnt. Die Vereinbarung von Sicherheitsklassen, die von der personalführenden Stelle dem Benutzer zugeordnet wird, gewährleistet eine adäquate Sicherheit für die Anwendungen bei Auftrennung der Verantwortung für Anwendungs- und Benutzersicherheit.

8. Technische Lösung

Für die Implementierung des Portalverbundes sind verschiedene Technologien erforderlich. Geeignete Literatur ist unter [3, 4] zu finden.

9. Service oriented Architecture

Einer der Gründe, warum das neue Schlagwort von „service oriented architecture“ (SOA) auf Basis von Web-Services derzeit so populär wird ist, dass SOAP das erste Mal erlaubt, das Web als universelle Middleware einzusetzen, ohne auf teure und proprietäre Lösungen angewiesen zu sein. Dies ist nicht neu und wurde beispielsweise durch das Konzept des „Client/Server Computing“ bereits in den späten 80ern definiert, damals auf der Basis von RPC und proprietärer Middleware. Multi-Tier Programming (z.B. 3-Tier Architecture) verwendet das gleiche Prinzip.

10. Von Verbindungssicherung zur Dokumentsicherung

Mit der Verwendung von XML als „Middleware“ ging auch eine Entwicklung eines neuen Sicherheits-Paradigmas einher, nämlich der Übergang von einem verbindungsorientierten Sicherungskonzept zu einem dokumentorientierten Ansatz, der das XML Objekt als semantische Einheit sichert und von der Übertragung und dem Wirkungsort unabhängig macht. Bedeutungsvoll sind dabei folgende Eigenschaften:

- Identitätsmanagement ist über Domain Grenzen hinweg möglich, was mit „Identity Federation“ und „Identity Association“ beschrieben wird.
- Die Sicherungseigenschaften (security context) bleiben an die authentifizierte Person gebunden, und es wird eine rollenbasierte Zugriffskontrolle ermöglicht (RBAC, role based access control). Die Sicherungseigenschaften (security context) bleiben an die Dokumente oder Daten gebunden, auch wenn sie mehrfach Grenzen von Sicherheits- und Verwaltungsbereichen (Domains) überschreiten.

11. Spezielle Anforderungen von SOAP an Vertraulichkeit und Integrität

SOAP muss besonders geschützt werden, da es Daten in einer allgemein verständlichen Form (als tagged text) transportiert. Durch die textliche Repräsentation mit vielen möglichen Varianten (mehr Leerzeichen, andere Zeilenumbrüche, verschiedene Kodierungen, verschiedene Tag-Schreibungen) ist außerdem die Sicherstellung einer unveränderten Übertragung relativ schwierig, jedenfalls wesentlich schwieriger, als bei binären Übertragungsformaten. Damit SOAP sicher ist, muss es auf Ebene der Anwendung Mechanismen anbieten, die etwa vergleichbar sind mit den Mechanismen, die auf IP-Ebene durch IPSec mit ESP Protokoll angeboten werden.

12. Web Service Definition Language (WSDL) und Security

WSDL liefert die Beschreibungen von Web-Services, vergleichbar einem Vertrag. Für die Entwickler von Services sind WSDLs wie eine Klasse zu sehen. Obwohl innerhalb von WSDL Sicherheitsdefinitionen möglich sind, sind diese relativ eingeschränkt und bleiben weit hinter dem zurück, was WS-Policy bietet. WS-Policy ist ein (zukünftiger) Standard für die Sicherheit von Webservices und wird etwa in WebSphere 6 bereits unterstützt. Daher wird zukünftig sinnvollerweise WS-Policy für die Beschreibung von Web Service Security verwendet und diese im WSDL referenziert.

13. Anforderungen an eine Authentifizierung in einer SOA

In Zusammenhang mit SOA ergeben sich neue Anforderungen an die Verwaltung von Benutzern und Berechtigungen:

- Nicht mehr einzelne Systeme (oder Systemverbünde), an denen der Benutzer persönlich angemeldet ist und auf denen der Benutzer ein spezifisches Profil hat, sondern Services, die von unterschiedlichen unabhängigen Systemen angeboten werden, sind Dienstanbieter für den Benutzer.
- Um nicht mit jedem dieser Services einzeln verhandeln zu müssen (Anmeldung, Rechteüberprüfung, Anwendung, Abmeldung), ist eine Vermittlungsschicht für die Benutzerverwaltung und Rechteerteilung notwendig geworden.

Dabei ergeben sich Besonderheiten für die Verwaltungsaufgaben von Benutzern und Rechten in einem Netzwerk von Services:

- Es muss eine Vertrauensbasis zwischen den Systemen bestehen, an denen die Benutzer angemeldet sind und den Systemen, auf denen die Services angeboten werden.
- Die Anwendungen müssen eine Übereinkunft über die Vermittlung von Identitätsinformationen und Berechtigungen haben, um die Benutzerinformationen von einem System auf einem anderen gültig werden zu lassen.
- Die Vermittlung dieser Berechtigungen muss auf eine sichere Weise geschehen – zuverlässig und geschützt, und zwar nicht nur auf Netzwerkebene (von Endsystem zu Endsystem), sondern auf der Ebene der Anwendung. Klassische Strategien zur Authentifizierung und Autorisierung sind dabei ungenügend.

14. Strategien der Authentifizierung

Der ursprüngliche Ansatz der Benutzerverwaltung ist auf Einzelsysteme zugeschnitten. Einzelne Anwendungen haben darüber hinaus eine eigene Benutzerverwaltung, etwa Datenbankanwendungen. Um zwischen verschiedenen Systemen zu navigieren, sind auf allen diesen Systemen passende Berechtigungen nötig. In Netzwerk-Umgebungen ist dieser Ansatz durch Lösungen wie Network

Information System (NIS) unter Unix und Domains mit Active Directory unter Windows ergänzt worden. Anstelle einzelner Berechtigungen pro System ist eine Zentralisierung und Verteilung der Rechte getreten. Diese Lösungen erlauben ein „Single Sign On“ mit der Möglichkeit, differenzierte Rechte in Anwendungen und auf einzelnen Systemen zu haben. Die Grenzen von NIS und Active Directory ergeben sich dadurch, dass das Vertrauen innerhalb der Domains uneingeschränkt und die Abgrenzung nach außen naturgemäß strikt sein muss. Kerberos ist ein Ansatz, die Beschränkungen des NIS/Domain Prinzips zu überwinden, indem eine zentrale Instanz über die Berechtigungen auf den beteiligten Systemen Kontrolle ausübt, ohne dass zwischen allen beteiligten Systemen ein gegenseitiges Vertrauen bestehen muss, wie es in Domains Voraussetzung ist. Kerberos erlaubt auch „Single Sign On“, selbst in heterogenen Architekturen. Kerberos verwendet kryptographische Methoden, um abgesicherten Austausch zwischen Anwendungen zu ermöglichen, wie es auch in einer „Service Orientierten Architektur“ erforderlich ist. Zugleich erfordert die Zentralisierung einen hohen Koordinationsaufwand, der zwischen unterschiedlichen Unternehmen oder Behörden nicht leistbar ist. Web-Services, die über verschiedene Domains verteilt sind, schaffen neue Anforderungen: Portale müssen die Authentifizierung übernehmen und Rechteinformationen vertrauenswürdig und zuverlässig weitergeben. Der relativ junge Ansatz von „federated identity“ erlaubt es einem Benutzer, der einmal zuverlässig authentifiziert wurde, ohne weitere Authentifizierung auf anderen Systemen zu agieren und dabei definierte und abgegrenzte Rechte zu haben. Dies ist möglich durch ein genau abgegrenztes Vertrauensverhältnis zwischen Systemen unter Zuhilfenahme von Methoden der Kryptographie. Für „federated identity“ gibt es verschiedene, großteils offene Standards, die im Aufbau sind und erfreulicherweise ein ausreichendes Maß an Konvergenz aufweisen. Die in Entwicklung befindlichen Standards verwenden XML als „Middleware“.

15. Referenzen

[1] A. Nadalin, C. Kaler, P. Halam-Baker, R. Monzillo Web Services Security: SOAP Message Security 1.0 (WS-Security 2004), OASIS Standard 200401, March 2004 http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf

[2] R. Hörbe, Portalverbundprotokol 1.8.9
http://reference.e-government.gv.at/PortalVerbundProtokoll___pvp_1.533.0.html

[3] Thomas Erl, Service-Oriented Architecture, A Field Guide to Integrating XML and Web Services 2004, Prentic Hall, ISBN 0-13-142898-5

[4] J. Rosenberg, D. Remy, Securing Web Services with WS-Security 2004, SAMS, ISBN 0-672-32651-5