Eine wichtige neue Kernkompetenz bei Leistungserbringern im medizinischen Bereich

Identity Management schafft ein klares Fundament

Mit der zunehmenden Umsetzung von eHealth-Projekten in der Schweiz wird die digitale Identifikation der Behandelnden sowie die Verwaltung ihrer Zugriffsberechtigungen auf Systeme und Daten zu einer wichtigen Aufgabe – auch und insbesondere bei den Leistungserbringern.

Digital gesehen werden die Behandelnden von den Organisationen heute noch oft als Attribut ihrer Lohn- respektive Honorarabrechnung, als Benutzer-Account oder als Planungsobjekt in den Verzeichnissen der Informatiklösungen geführt. Als Konsequenz bilden die Systeme die Behandelnden nur unvollständig und primär als Objekt administrativer Massnahmen ab.

Im Kontakt mit den Patienten sind die Behandelnden jedoch ein aktives Subjekt mit komplexen Beziehungen zum Behandelten. Mit der Digitalisierung dieses Behandlungskontextes, der sich in der elektronischen KG respektiv dem elektronischen Patientendossier niederschlägt, ist es darum wesentlich, die Behandelnden auch digital gesehen als handelnde Subjekte/Identitäten mit diversen Attributen, Rollen und mit ihren Beziehungen zu den Patienten abzubilden.

Die dafür erforderlichen organisatorischen, prozessualen und technischen Massnahmen werden typischerweise unter dem Begriff Identity- und Accessmanagement (IAM) zusammengefasst. Für die technische Unterstützung von IAM existieren Standardsoftware-Bausteine. Als Hilfsmittel automatisieren und vereinfachen diese die notwendigen Schritte hin zu einer ganzheitlichen Berechtigungsverwaltung.

Identifikation von Behandelnden im Behandlungskontext

In Bezug auf die elektronischen Patientendossiers sind die Behandelnden in zweifacher Hinsicht zu identifizieren.

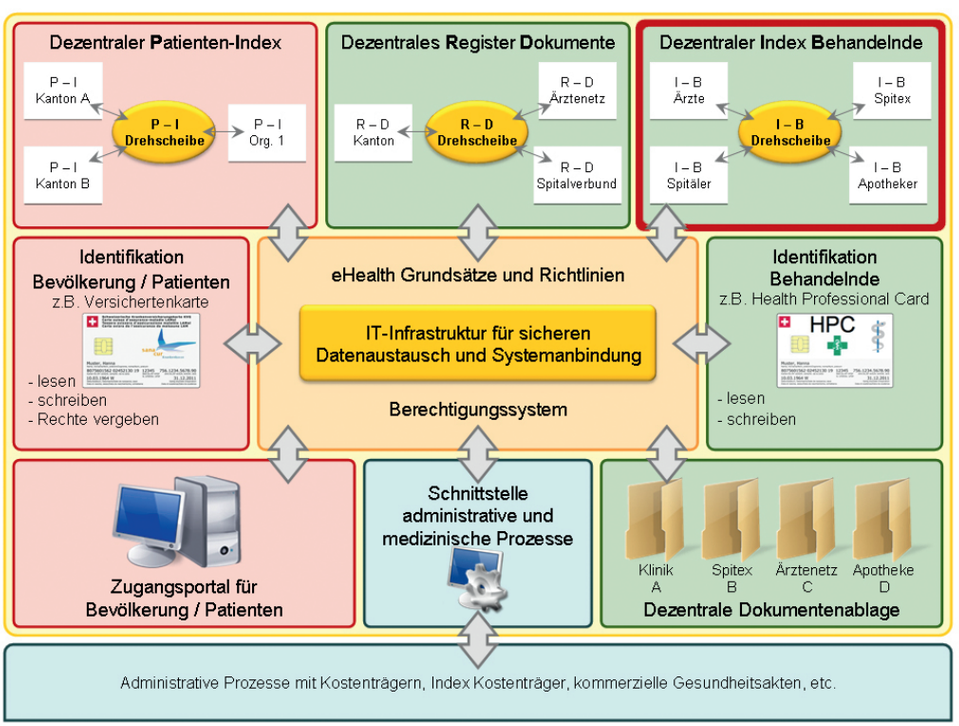
a) Als Zugangsberechtigte einer Domäne (= Unternehmen = Gemeinschaft Behandelnder) mit Zugang zu Systemen, Ressourcen und Informationen
b) Als domänenübergreifende Zugriffsberechtigte auf Patientendossiers

Als Zugangsberechtigter ist für den Behandelnden innerhalb der Domäne, etwa einem Spital, der Zugang zu Systemen und Informationen zu regeln. Der Patient gibt mit dem Eintritt in eine Institution (Spital, Arztpraxis, Gruppenpraxis) im Allgemeinen sein Einverständnis, dass alle Behandelnden der Domäne auf seine Unterlagen zugreifen können, sofern diese in den Behandlungsprozess involviert sind. Die Institution regelt den Zugriff auf Systeme und Daten in ihrer Zuständigkeit, indem sie die Behandelnden eindeutig identifiziert. Sie weist ihnen zudem Rollen und Zugriffsberechtigungen gemäss den definierten Richtlinien der Organisation zu.

Gemäss den eHealth Suisse-Empfehlungen III «Standard und Architektur» soll der Patient den domänenübergreifenden Zugriff von Behandelnden auf sein elektronisches Patientendossier (ePD) selbst regeln können. Zu diesem Zweck werden in einer Gemeinschaft bei Anfragen für den Zugriff auf das ePD eines Patienten immer zwei Arten von Informationen benötigt:

1. eine eineindeutige Identifikation des Anfragenden (Authentifikation) und
2. der Kontext des Anfragenden, der ihn zum Zugriff auf die persönlichen Daten der Patienten berechtigt

Abbildung 1: Dezentraler Index Behandelnde (Quelle: eHealth Schweiz, Standards und Architektur-Empfehlungen I)



Für Letzteres müssen die bei der Anfrage mitgelieferten Berechtigungsattribute mit den jeweiligen Profileinstellungen des Patienten abgeglichen werden. Dies um zu prüfen, ob die Berechtigungsinformationen des Anfragenden für eine Autorisierung der Anfrage ausreichend sind.

Dezentrale Berechtigung bringt hohe Komplexität und grossen Aufwand

Die Empfehlungen III von eHealth Suisse sehen auch vor, das die Einwilligungen und Berechtigungsvergaben der Patienten dezentral in den so genannten «Stammgemeinschaften» erfolgen. Dabei handelt es sich um dezentrale Gemeinschaften, die aber zentral gesteuert werden. Auch die Nachvollziehbarkeit, Historisierung und das Audit der erfolgten Zugriffe durch Behandelnde sollen jeweils innerhalb der Gemeinschaften sichergestellt werden.

Die Entscheidung gegen ein zentrales Berechtigungsmanagement und für die Einführung autonomer Berechtigungssteuerungen in den jeweiligen Stammgemeinschaften hat je nach Perspektive Vor- und Nachteile: Aus Sicht eines effektiven und nachvollziehbaren IAM bringt die Umsetzung der Empfehlungen III jedoch eine hohe Komplexität und einen grossen Aufwand für die Pflege der Stammdaten mit sich – dies erst recht, wenn die Berechtigungen auch durch den Patienten selbst gemanagt werden sollen.

Best Practice Beispiele von umgesetzten Identity Management-Lösungen in anderen Branchen zeigen zwei Varianten zur Reduktion der Komplexität für den einzelnen Benutzer:

1. Revidieren der getroffenen Entscheidung und Einführen eines zentralen, schweizweiten Identitäts- und Berechtigungs-Services für die Administration des Zugriffsmanagements auf Patientendaten
2. Nutzung von so genannten Identity Federation-Technologien, um zumindest die domänenübergreifenden Autorisierungsattribute über einen zentralen Punkt im Netzwerk der Stammgemeinschaften abrufen und nutzen zu können

Aktuell gibt es in der Schweiz neben dem Mitgliederverzeichnis der FMH (ca. 35'000 Einträge) und dem Zahlstellenregister (ZSR) der SASIS (ca. 77'000 Einträge) für die Rechnungskontrolle eine Handvoll weiterer – für diese Aufgabenstellung geeignete – Personenregister. Diese beinhalten zwar einen signifikanten Bestand an Personendaten der Behandelnden (sogenannte Health Professionals). Sie sind aber ursprünglich nicht für diese Anwendung gedacht, und deshalb nur bedingt als Basis für den dezentralen Index für Behandelnde (Health Professional Index) nutzbar.

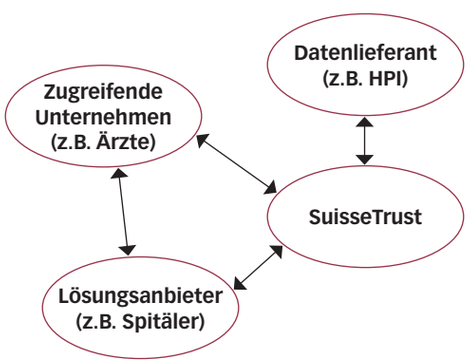
Daraus resultieren Fragestellungen zur weiteren Ausgestaltung der notwendigen Schnittstellen zwischen administrativen und medizinischen Prozessen. Diese sind aktuell ebenso Gegenstand der Entwicklung der Empfehlungen IV «Standard und Architektur» von eHealth Suisse wie ein Leitfaden für die Umsetzung der bisher erarbeiteten Empfehlungen I bis III.

Mögliche Architekturansätze aus dem eGovernment

Die organisatorischen und technischen Anforderungen an ein IAM im eGovernment der Schweiz wurden durch ein Gremium in einer konzeptionellen Phase per 31. Dezember 2010 als Lösungsarchitektur eGov IAM CH definiert und im Detail beschrieben.

Im Auftrag des Informatiksteuerungsorgan Bund (ISB) als zentralem Initiator der Bundesverwaltung wurde von Januar 2011 bis Mai 2011 unter dem Arbeitsnamen «SuisseTrustCAS» ein Grobkonzept für einen Identitäts-Service «aus der Cloud» erstellt.

Abbildung 2: Ursprüngliches Grundmodell SuisseTrustCAS



Für die Erstellung des Konzeptes wurden Lösungsanbieter, mögliche Identity Provider und potentielle künftige Nutzer in die Definition der Anforderungen involviert. Dieser so genannte Claim Assertion Service (CAS) bildet das Fundament für eine domänenübergreifende Autorisierung von extern zugreifenden Benutzern im eGovernment.

Die Abbildung 2 wurde auf das Gesundheitswesen angepasst: Analog zu Mitarbeitern von Unternehmen mit Zugriff auf eGovernment-Daten, müssen die Ärzte einen nachvollziehbaren und autorisierten Zugang zu den von Spitälern verfügbar gemachten Patientendaten besitzen.

Die Kernfunktionalität der Architektur liegt im sicheren Zugriff auf das Patientendossier. Denn die nachzuweisenden Eigenschaften des behandelnden Arztes werden als Identity-Attribut aus der Cloud, also von der Plattform SuisseTrust-CAS, abgerufen. Dies genau in dem Moment, in dem der Zugriff des jeweiligen Arztes auf das Patientendossier erfolgen soll.

Von September 2011 bis Ende März 2012 wurde das Grobkonzept im Rahmen einer Machbarkeitsstudie für das eGovernment unter der Bezeichnung «SuisseTrust-IAM» erweitert. Es wurde erfolgreich in eine Testumgebung implementiert und mit verschiedenen Services privatwirtschaftlicher und kantonaler (öffentlicher) Provider verbunden. Auch der Zugriff von Einzelpersonen ohne direkte Zuordnung zu einer Organisation wird seit diesem Zeitpunkt abgedeckt.

Bei der realisierten Architektur handelt es sich um einen Lösungsansatz, der über verschiedene Domänen hinweg die Möglichkeit bietet

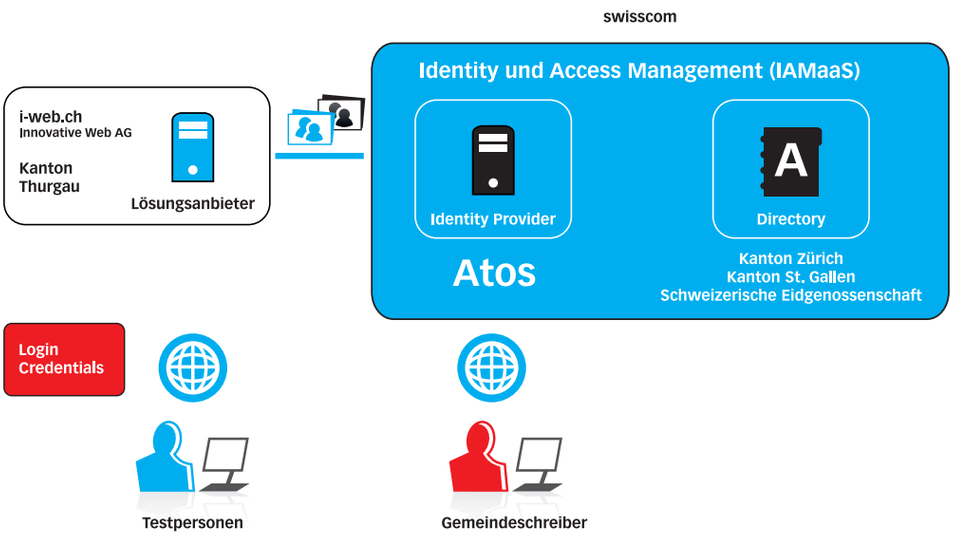
1. die Identität eines Benutzers durch verschiedene, bereits vorhandene Authentisierungsmethoden (z.B. SuisseID, HPC, OneTime Passwort, SMS TAN) zu verifizieren und

Atos – neue Rezepte für eine gesunde IT

Mit weltweit rund 74'000 Mitarbeitenden und einem Jahresumsatz von 8,6 Milliarden Euro zählt Atos zu den führenden europäischen Anbietern von IT-Services. In der Schweiz bietet die Atos AG nach der Übernahme von Siemens IT Solutions and Services im Sommer 2011 weiterhin innovative Lösungen aus einer Hand: 500 Spezialisten unterstützen öffentliche und private Organisationen mit professionellen IT-Lösungen und Services – auch im Gesundheitsbereich.

Mit ihrer langjährigen Erfahrung im weltweiten und im Schweizer Gesundheitswesen sowie in der Spital-IT unterstützen die Business Technologists von Atos Spitäler, Kliniken, Praxen und andere Institutionen mit ihrem profunden Fachwissen bei den aktuellen Herausforderungen im Schweizer Gesundheitswesen. Atos ist es als IT-Unternehmen ein besonderes Anliegen, die Abläufe der Fachspezialisten nahtlos mit der bestmöglichen IT zu unterstützen.

Abbildung 3: Umgesetzte Machbarkeitsstudie im Bereich eGovernment



2. die für einen autorisierten Datenzugriff durch Bürger oder Verwaltungsmitarbeiter notwendigen Attribute über die Grenzen der jeweiligen Domänen hinweg zu überprüfen.

Identische Lösungen für identische Anforderungen

Grundsätzlich entsprechen die Anforderungen an eine organisationsübergreifende Berechtigungsverwaltung im Bereich eGovernment in sehr weiten Teilen den Anforderungen, die von eHealth-Suisse in den Empfehlungen III definiert wurden.

Da es für die technische Realisierung der idealerweise schweizweit nutzbaren Identity-Services nicht von Belang ist, ob es sich um:

a) einen Bürger beim Zugriff auf Daten der öffentlichen Verwaltung,
b) einen Patienten oder Health Professional beim Zugriff auf ein virtuelles Patientendossier,
c) den Mitarbeiter eines Unternehmens beim Zugriff auf Informationsdienste eines anderen Unternehmens handelt,

wäre es zweckmässig, die erforderliche Infrastruktur nicht mehrmals aufzubauen. Sie könnte im Gegenteil einmal schweizweit nutzbar gemacht und für die verschiedenen Anwendungsszenarien (z.B. eGov, eHealth, eEconomy) mit den jeweils relevanten Schnittstellen integriert werden. So können beispielsweise die unterschiedlichen Rollen der Akteure für den Zugriff auf die verschiedenen Vertraulichkeitsstufen (vgl. Abbildung 4) als Attribut durch den zentralen Service SuisseTrust zur Verfügung gestellt werden.

Fazit

Aus der Sicht der Autoren lassen sich die heute in der Implementierung stehenden Funktionsbausteine der eGovernment IAM-Architektur auch auch für die Anwendungsszenarien des Gesundheitswesens uneingeschränkt nutzen.

Die Benutzer von eGov, eHealth und von weiteren Services werden den Anbietern der jeweiligen Dienste dankbar sein, wenn die Administration für alle Services übergreifend an einem Ort durchgeführt werden kann – insbesondere wenn dies in benutzerzentrierter Art und Weise durch die Benutzer (Bürger, Patienten, Versicherungsnehmer) in Eigenregie durchgeführt werden soll.

Autoren

Enno Hoffmann
Ist seit 2000 zunächst bei Siemens und seit 1.7.2011 durch die Umfirmierung der Siemens IT Solutions and Services AG bei der Atos AG in der Schweiz als Spezialist für Identity und Accessmanagement branchenübergreifend tätig.

Jürg Lindenmann
Bietet als selbständiger Berater und Inhaber von healtH-it Unterstützung und Beratung an der Schnittstelle zwischen Unternehmensbedürfnissen und der IT im Gesundheitswesen an. Weitere Informationen zur Person: www.health-it.ch

Weitere Informationen

Atos AG, Freilagerstrasse 28, 8047 Zürich
Telefon 058 702 1111
isrm@atos.ch, ch.atos.net/isrm

Abbildung 4: Berechtigungen beim Patientendatenzugriff (Quelle: eHealth Schweiz, Standards und Architektur-Empfehlungen III)

Vertraulichkeitsstufe des Dokumentes / Rollen	Administrative Daten	Nützliche Daten	Medizinische Daten	Stigmatisierende Daten	Geheime Daten
2.1 Mein Behandelnder	Ja	Ja	Ja	Option	Nein
2.2 Behandelnder des Vertrauens	Ja	Ja	Ja	Option	Option
2.3 Behandelnder allgemein	Ja	Ja	Nein	Nein	Nein
2.4 Notfall-Behandelnder	Ja	Ja	Ja	Option	Nein

Ja	Zugriff möglich
Nein	Zugriff nicht möglich
Option	Zugriff je nach individueller Einwilligung; Grundeinstellung: Nein

Empfehlung 6
Rechte unter Verwendung der Rollen