Schweizerische Post

E-Health-System vivates

Die Schweizerische Post verteilt nicht nur Briefe und Pakete. Immer mehr wird sie zur Gesamtdienstleisterin, wenn es um den zuverlässigen, wertsteigernden und nachhaltigen Transport von Informationen geht. Vor diesem Hintergrund hat sich die Post vor einigen Jahren zum Ziel gesetzt, ein E-Health-System aufzubauen, mit dem Patientendaten sicher zwischen verschiedenen Akteuren im Gesundheitssystem ausgetauscht werden können. Damit die Sicherheit der heiklen Daten jederzeit gewährleistet ist, setzt die Schweizerische Post bei ihrem E-Health-System Vivates auf die Airlock Suite von Ergon.

Sichere Patientendaten

Ein Patient bewegt sich oft zwischen verschiedenen Leistungserbringern. So hat er beispielsweise einen Hausarzt, der ihn zu einem Spezialisten überweist. Dieser stellt fest, dass ein chirurgischer Eingriff nötig ist – der Patient muss ins Spital. Heute ist es oft so, dass der Patient seine Informationen, zum Beispiel Röntgenaufnahmen, selber von einem Arzt zum nächsten tragen und immer wieder die gleichen Fragen und Untersuchungen über sich ergehen lassen muss. Ein Patientendossier, in das jeder behandelnde Arzt Einsicht hat und Untersuchungsergebnisse eintragen kann, erleichtert den Prozess.

Allerdings sind Patientendaten heikel: Niemand will, dass jeder seine Krankengeschichte nachlesen kann. In Europa gelten Patientendaten deshalb als «besonders schützenswert» – das bedeutet, die Sicherheitsanforderungen sind höher als bei Banken: Der Zugriff für jeden Akteur muss einzeln freigegeben werden. Die Autorisierung erfolgt entweder durch den Patienten oder nach dem Zuweisungssystem: Jeder der Dokumente ins Dossier legt, definiert zugleich, an wen die Dokument gerichtet sind und autorisiert so implizit den Adressaten.

Zugriff im Notfall

Sicherheit im Gesundheitswesen bedeutet aber nicht nur die Sicherstellung der Vertraulichkeit. Ist ein Notfall da, muss der Arzt unbedingt schnellen Zugriff auf die relevanten Patientendaten haben. Sonst kann es unter Umständen fatale Folgen für den Patienten haben: Erhält beispielsweise jemand ein Medikament, auf das er allergisch ist, kann dies einen gefährlichen allergischen Schock auslösen. Doch auch dafür bietet Vivates eine Lösung: Der Arzt kann einen Notfall deklarieren und erhält dann für eine begrenzte Zeitdauer Zugriff auf die Daten. Um Missbrauch zu verhindern, werden sowohl der Patient als auch sein Vertrauensarzt aber gleichzeitig alarmiert.

Ein flexibler Authentisierungslayer

Das E-Health-System Vivates wurde in vier Gemeinden im Kanton Genf getestet und im Jahr 2013 auf weitere Kantone ausgeweitet. Bald zeigte sich, dass die verwendete Authentifizierungslösung zwar die nötige Sicherheit bot, aber bei künftigen Anforderungen an Flexibilität und Verwaltbarkeit an seine Grenzen kam. Aufgrund des föderalistischen Systems der Schweiz hat jeder Kanton leicht andere Gesetze – die Verwaltung der verschiedenen Instanzen wurde schlicht zu aufwendig. «Unser System muss einfach skalierbar sein, da jeder Kunde eine neue Umgebung und damit auch neue oder geänderte Anforderungen mit sich bringt. Wir können folglich den Authentisierungslayer nicht bei allen Kunden identisch installieren, sondern wir müssen individualisierte Konfigurationen bereits stellen können. Hier hilft eine automatisierte Verwaltung», sagt Michael Doujak, Leiter Entwicklung vivates bei der Post.

Spitäler und Gesundheitsorganisationen haben gewöhnlich bereits ein eigenes Identifikationstoken – sei dies SuisseID, IDP oder ein proprietäres System. Für das Patientendossier sollte jede Organisation bei seinem Token bleiben können. «Wir verwenden hier den Begriff transitives Vertrauen. Der Gesundheitssektor kennt seine Mitarbeiter und managt den Zugriff – es ist also keine Duplikation der Identifikation nötig», erklärt Michael Doujak.

«Es sind mehr Authentifizierungslösungen, als wir zunächst projektiert hatten», sagt Michael Doujak. «Trotzdem konnten wir auch diese Phase on time und on budget abschliessen – das ist selten bei so grossen Informatikprojekten.»

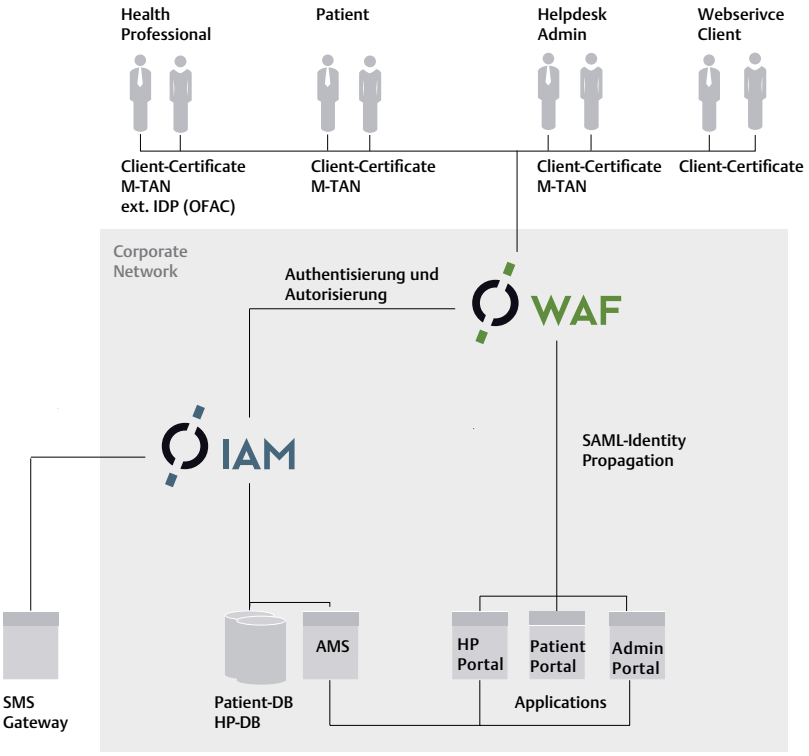
Michael Doujak, Leiter Entwicklung vivates bei der Post

Zudem sind ganz unterschiedliche Akteure beteiligt – vom grossen Spital mit eigener IT-Abteilung über kleinere Organisationen wie Apotheken bis hin zu Einzelpersonen, dem selbständigen Arzt oder aber auch dem Patienten. Alle müssen Zugang zum System haben. Auch waren die Anforderungen an das Design hoch – die Landing Page musste nicht nur ansprechend und einfach zu bedienen sein, sie sollte sich auch je nach Anforderung anpassen.

Plug-In-Tauglichkeit überzeugt

Nachdem die Post verschiedene Schweizer Anbieter geprüft und ihre Technik getestet hatte, fiel die Wahl auf die Airlock Suite von Ergon. Ausschlag gab zum einen die hohe Plug-In-Tauglichkeit mit verschiedensten Identifikationssystemen, die Ergon bereits in vergangenen Projekten beweisen konnte. So konnte die Kompatibilität sichergestellt werden.

Bild 1 Michael Doujak, Leiter Entwicklung vivates bei der Post



Zum anderen sprach für die Airlock Suite auch die einfache Administration, die flexible Handhabung verschiedener Konfigurationen und die Fähigkeit, Upgrades (speziell auch für Security Patches) im laufenden Betrieb ausrollen zu können. Airlock WAF dient dabei als Authentisierungslayer gegenüber den Patienten, Ärzten, Dienstleistern und Administratoren. Airlock IAM managt die Identitäten. Die Trennung von Authentisierung und Identity Propagation ermöglicht eine hohe Flexibilität beim Zugriff.

Ergon betrat mit dem E-Health-Projekt Neuland: Spezifische Anforderungen aus dem Gesundheitsbereich brachten spezielle Herausforderungen. So gab es einige externe Nicht-Standard-IDPs, die es zu integrieren galt, wie beispielsweise OFAC. «Viele Anwendungen tauchten hier zum ersten Mal für uns auf», sagt Adrian Berger, Abteilungsleiter bei Ergon. «Beispiele sind die Vertretung von nicht zurechnungsfähigen Personen; das Dual Carding, wodurch zwei SSL-Sessions gleichzeitig laufen können müssen oder eben die Notfälle, bei denen bestimmte Daten sofort zur Verfügung stehen müssen.»

On time, on budget

Der Zeitplan der Entwicklung war trotz des komplexen Themas eng: Im März 2013 war die Ausschreibung des Projekts, im Mai startete die Evaluation – und Ende 2013 musste die alte Sicherheitsplattform bereits abgelöst sein. Um diesen engen Zeitplan zu halten, wurde das Projekt in zwei Phasen aufgeteilt. Die erste Phase, die termingerecht und im Budget im Dezember 2013 abgeschlossen wurde, hatte einen reduzierten Scope bei den Authentifizierungstoken; erst die Smart-Card wurde realisiert. In der zweiten Phase wurden zahlreiche weitere Authentifizierungslösungen integriert. «Es sind mehr, als wir zunächst projektiert hatten», sagt Michael Doujak. «Trotzdem konnten wir auch diese Phase on time und on budget abschliessen – das ist selten bei so grossen Informatikprojekten.» Ganz abgeschlossen ist die Entwicklung aber noch nicht: «Je weiter wir das Dossier ausrollen, desto mehr Anforderungen kommen hinzu», so Doujak weiter.

Bild 2 vivates-Infrastruktur

Flexibilität im Zentrum

Interview mit Adrian Berger, VP Finance Ergon

Auf welche Besonderheiten sind Sie im Bereich Sicherheit für ein E-Health-System getroffen?
Verglichen mit Banken und Versicherungen sind die Anforderungen strenger: Der Datenschutz ist noch rigider und stärker geregelt. Gleichzeitig muss es aber Mechanismen für Notfallsituationen geben, wenn z.B. ein Arzt sofort Zugang zu den Daten braucht, um ein Leben zu retten. Diese Dualität machte das Projekt sehr spannend für uns – wir waren hier Lernende.

Was ändert sich für die Benutzer mit der Umstellung?
Im Moment noch nichts – das war genau das Projektziel. Die bestehende Lösung wurde ersetzt, so dass alle vorhandenen Authentifizierungsmittel weiter verwendet werden können. Ansonsten wäre die Umstellung bei den Endkunden wohl nicht auf Akzeptanz gestossen. Wir konnten hier aber eine Basis für eine noch höhere Flexibilität in der Zukunft legen. Unterdessen wurden zum Beispiel bereits Authentisierungslösungen über das Mobiltelefon integriert und live geschaltet.

Wie wichtig ist in diesem Projekt die Flexibilität der Lösung?
Man kann sagen, die Flexibilität steht hier im Zentrum. Das Gesundheitswesen in der Schweiz ist stark segmentiert, dem entspricht unsere Lösung. Zum einen hat jeder Kanton eine leicht andere Gesetzeslage, die wir berücksichtigen müssen – darum arbeiten wir auch mit verschiedenen Instanzen. Gleichzeitig gibt es viele Organisationen mit eigenen Sicherheitstokens. Das Kantonsspital Aarau hat beispielsweise eine eigene PKI-Lösung, die wir integrieren. Eine wichtige Anforderung war, dass sich die Lösung gut in die Breite skalieren lässt. Die Flexibilität der Airlock Suite ermöglicht dies.

Ergon Informatik AG
Merkurstrasse 43
CH–8032 Zürich

+41 44 268 89 00
www.airlock.com
twitter.com/ErgonAirlock

---

smart people – smart software

1984 gegründet und mit aktuell 235 Mitarbeitenden gehört Ergon Informatik AG heute zu den traditions- und erfolgreichsten Informatikdienstleistern der Schweiz. Über 80% aller Mitarbeitenden sind Softwareentwickler mit Hochschulabschluss. Die meisten davon sind Informatikingenieure der ETH Zürich, einer der zehn Top-Universitäten der Welt. Zudem wurde Ergon Informatik AG mehrfach für ihre nachhaltige Personalpolitik ausgezeichnet.

Ergon Informatik AG ist breit diversifiziert und erbringt Dienstleistungen für unterschiedlichste Branchen. Herausragende Kompetenzen weist Ergon im Bereich Finanzdienstleistungen, E-Banking, Telekommunikation und Security aus. 1997 hat Ergon das erste E-Banking der Schweiz entwickelt. Das Security-Produkt Airlock ist seit dem Jahr 2002 am Markt und heute bei über 300 Kunden weltweit im Einsatz.

Weitere Informationen unter www.ergon.ch