Welche Anforderung stellen die neuen eHealth-Anwendungen an die Kommunikationsinfrastruktur?

Gerhard Pisl, Stefan Resch, Siemens AG

Nach § 291a SGB V sind die verpflichtenden Kernanwendungen der elektronischen Gesundheitskarte die elektronische Übermittlung ärztlicher Verordnungen und die Verwaltung der Versichertendaten.

Darüber hinaus muss die Karte (eGK/HBA) weitere Funktionen unterstützen, welche der Versicherte auf freiwilliger Basis nutzen kann. Hierbei handelt es sich um

- die Bereitstellung von Notfalldaten
- Daten der Arzneimitteldokumentation eines Versicherten
- den elektronischen Transport von Arztbriefen
- das Führen einer elektronischen Patientenakte
- ein Patientenfach
- die Patientenquittung.

Hinzu kommen werden noch so genannte Mehrwertdienste, deren Unterstützung aber nicht explizit im Rahmen des § 291a gefordert ist.

Aus den datenschutzrechtlichen Vorgaben sowie im Hinblick auf die Akzeptanz durch die Nutzer, ergeben sich aus den geplanten Anwendungen eine Reihe von Anforderungen an die Kommunikationsinfrastruktur. Schlagwortartig sind in diesem Zusammenhang die Eigenschaften Verfügbarkeit, Interoperabilität, Wirtschaftlichkeit und Sicherheit zu nennen. Insbesondere der Sicherheit kommt aufgrund der gesetzlichen Vorgaben, aber auch in Bezug auf die Akzeptanz durch die Versicherten, welche letztendlich mitentscheidend für den Erfolg des Gesamtprojektes sind, eine herausragende Bedeutung zu.

Da es sich bei den zu bearbeitenden Daten in erster Linie um Personen spezifische Daten handelt, sind gesetzliche Vorgaben des Datenschutzes bei Zugriff, Transport und Verarbeitung zu beachten, die sich in der IT-Sicherheit des Gesamtsystems wieder finden.

Zusammenfassend sind folgende Forderungen bei Zugriff, Transport und Verarbeitung der Daten besonders beachtenswert:

- Authentizität der beteiligten Personen/Prozesse: Der Zugang zu den Systemen wird nur durch 2-Faktor-Authentifizierung gewährt.
- Autorisierter Zugriff und Verarbeitung: Wird von einer dem System bekannten Person (oder Prozess) ein Dienst angefordert, so muss festgestellt werden, ob die Person überhaupt dazu autorisiert ist
- Integrität der Daten: Das Gesamtsystem muss Mechanismen enthalten, die ein versehentliches oder unautorisiertes Ändern/Manipulieren der Daten verhindert und somit die Integrität der Daten schützt
- Vertraulichkeit der Daten: Werden die Daten über öffentliche Netze transportiert, so dürfen sie durch Abhören nicht kompromittiert werden
- Einfache Bedienung: Die Systeme müssen möglichst einfach bedient werden können. Das gilt im Speziellen für wiederholtes Log-In an unterschiedlichen Systemen (Single Sign On)
- Zukunftssicherheit: Die immer wieder kehrende Funktionalität des Log-In/Authentifizierung, der Verschlüsselung, der Autorisierung etc. müssen in einer gemeinsamen Sicherheitsinfrastruktur zusammengefasst werden, die für die Applikationen weitestgehend transparent ist. Somit ist die einfache Integration von Neu- wie auch Altsystemen gewährleistet. Auch Teile der Infrastruktur müssen austauschbar sein, ohne die Funktionalität der angrenzenden Module in Mitleidenschaft zu ziehen (Investitionsschutz)

Um diesen Forderungen gerecht zu werden, ist eine IT-Sicherheitsinfrastruktur als Plattform für Fachapplikationen zu etablieren. Grundforderung an eine Infrastruktur ist eine möglichst allgemeine und wenn möglich bereits standardisierte Schnittstelle zur Aufnahme der Systeme, welche hierauf aufsetzen sollen. Ferner müssen die Schichten der Sicherheitsinfrastruktur so transparent sein, dass diese von den aufgesetzten Applikation nicht wahrgenommen werden. Dies garantiert auch die Aufnahme und Sicherung von bereits vorhandenen Applikationen (Legacy Applications).

Architektur „Allgemeingültige IT-Sicherheitsinfrastruktur“

Im Folgenden wird die Architektur „Allgemeingültige IT-Sicherheitsinfrastruktur“ in groben Zügen skizziert und erläutert.

Hierbei handelt es sich um eine modulare und dadurch hochflexible Architektur für den Datenaustausch zwischen Client- und Server-Applikationen über öffentli-

Autoren: Gerhard Pisl, Stefan Resch
Titel: Welche Anforderungen stellen die neuen eHealth-Anwendungen an die Kommunikationsinfrastruktur?
In: Jäckel (Hrsg.) Telemedizinführer Deutschland, Bad Nauheim, Ausgabe 2006
Seite: 334-336

che Netzwerke (Internet). Die modulare Trennung der einzelnen Schichten ist insbesondere aus Sicht der Systemwartung und somit der Systemverantwortlichkeit besonders wichtig.

Einheiten der „Allgemeingültige IT-Sicherheitsinfrastruktur"

(siehe Abb. 1)

1. **Teilnehmerzertifikate:**
   Um alle Teilnehmer in der digitalen Welt identifizieren/authentifizieren und dadurch zuordnen zu können, werden diese mit digitalen Public Key Zertifikaten ausgestattet. Die Schlüssel/Zertifikate werden auf einer Smart-Card (eGK/HBA) ausgeliefert und haben somit eine fälschungssichere Ausweisfunktion.
2. **Umfassende Netzwerk-Schicht (ISO/OSI Layer 3):**
   Die „Umfassende Netzwerk-Schicht" ist ausschließlich für die netzwerktechnische Verbindung zuständig. Es wird hier noch keine Aussage über den Verwendungszweck und die Interessen/Absichten der Benutzer gemacht. Der Raum, der hier eröffnet wird, bietet die größtmöglichen Freiheiten der Kommunikation. Dieser ist am besten vergleichbar mit dem Lebensraum der Weltgemeinschaft, ein annähernd rechtsfreier Raum, in dem nur ganz wenige rudimentäre Gesetze gelten.
3. **Umfassende Vertraulichkeits-Schicht (ISO/OSI Layer 3+):**
   Hingegen hat die „Umfassende Vertraulichkeits-Schicht" (VPN) die Aufgabe, einen Raum mit bestimmten Regeln (Gesetzen) zu definieren. Hier bewegen sich nur Benutzer mit ähnlichen Interessen/Absichten. Auf dieser Ebene stehen dem Benutzer bereits allgemeine anonyme Dienste (wie DNS, Suchdienste etc.) für dieses Netz zur Verfügung. Als Analogie wäre hier ein nationaler Raum (Land) der passende Vergleich, in dem es Bundesbürger, aber auch Besucher gibt. Die Gesamtheit der Nutzer in diesem Raum muss sich aber an nationale Gesetze halten und es stehen allgemeine anonymisierte Dienste wie Telefondienste zur Verfügung.

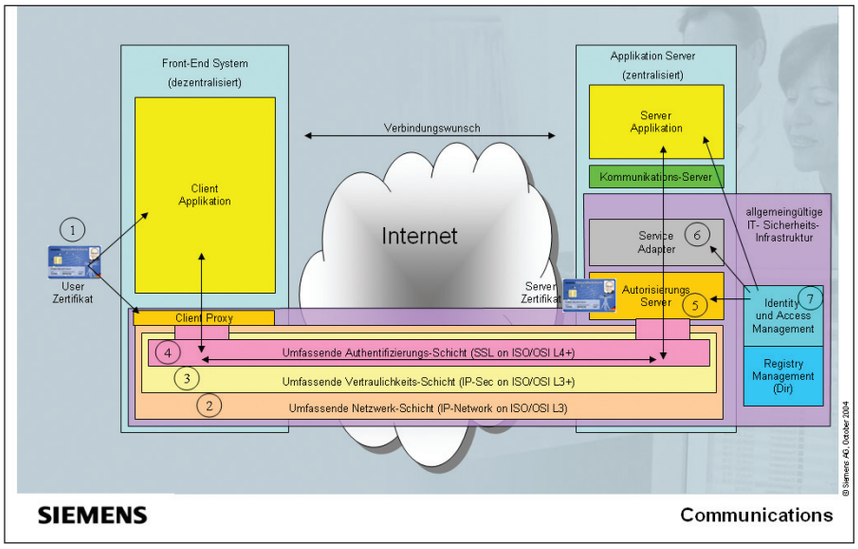

Abbildung 1: *Allgemeingültige IT-Sicherheitsinfrastruktur. Mehrstufige Sicherheit.*

4. **Umfassende Authentifizierungs-Schicht (ISO/OSI Layer 4+):**
   Soll nun ein konkreter nicht anonymisierter Dienst (Applikation) benutzt werden, so ist es die Aufgabe der „Umfassenden Authentifizierungs-Schicht" (SSL-Authentifizierung) die Identität des Nutzers mittels Smart-Card (eGK/HBA) zu ermitteln. Ferner verfügt diese Schicht auch noch über unabhängige Vertraulichkeitsmerkmale (Verschlüsselung), welche die mehrstufige Sicherheit dokumentieren. In unserer Analogie würde dies der Inanspruchnahme kostenpflichtiger Dienste wie z. B. die des Arztes (oder Notars) entsprechen. Das Vorzimmer (Sekretärin/Sprechstundenhilfe) wird zunächst die Identität mit Hilfe eines Ausweises feststellen. Dies findet übrigens auch nicht auf der Straße, sondern in einem abgeschlossenen Raum statt, der bereits eine gewisse Privatsphäre bietet.
5. **Zugangs- Autorisierungs-Schicht:**
   Bevor der Dienst geleistet wird, findet durch den Dienstanbieter („Umfassende Autorisierungs-Schicht") eine Autorisierungsprüfung statt. Diese stellt fest, ob die betreffende Person diesen Dienst überhaupt benutzen darf und befragt zu diesem Zweck das Role-Access-Management. In unserer Analogie wird diese Aufgabe ebenfalls vom „Vorzimmerpersonal" erledigt (z. B. Prüfung des Versicherungsverhältnisses).
6. **Netzwerk basiertes Single Sign On:**
   Um den Dienst nun endgültig zu leisten, wird der Anwender beim Dienstleister registriert (eingeloggt). Zu diesem Zweck wird der Verbindungswunsch nebst einer eindeutigen Nutzeridentifizierung an den Dienst weitergereicht (SSO-Service Adapter). Analog entspricht dieser Vorgang der Übergabe der Personendaten/Akte an den behandelnden Arzt/Notar.
7. **Identity-, Access- und Role-Management:**
   Die Daten, die für die Berechtigungsprüfungen nötig sind, werden im Identity-, Access- und Role-Management zentral konsolidiert und verwaltet. Das System wird nicht in zwingender Weise zentral administriert, sondern importiert Daten aus den angeschlossenen Quellsystemen und gibt diese bei Bedarf an autorisierte Systeme weiter. Analog entspricht dieses System einer Registratur (Aktenschrank).

Nach all diesen Prüfungen wird zwischen Applikation und Client/Nutzer eine transparente vertrauliche Verbindung hergestellt und die Dienstleistung geliefert. In Sonderfällen kann die Applikation noch einmal einen eigenen Authentifizierungsvorgang fordern. Hierzu

kann ebenfalls das Nutzer-Zertifikat auf der Smart-Card benutzt werden. Dieser Vorgang wäre analog zum Gespräch mit dem Arzt oder Notar in der Privatsphäre des Behandlungsraums zu sehen. Auch ein Notar würde, abhängig vom zu leistenden Dienst, sich abermals von der Identität des Klienten überzeugen.

Kontakt

Dr. Stefan Resch
Siemens Medical Solutions
Karlheinz-Kaske-Str. 2
91052 Erlangen
Tel.: +49 (91 31) 84 - 23 09
Fax: +49 (91 31) 84 - 36 72
stefan.resch@siemens.com

Gerhard Pisl
Siemens Communications
Richard-Strauss-Str. 76
81679 München
Tel.: +49 (89) 6 36 - 5 00 60
Fax: +49 (89) 92 21 - 17 36 77
gerhard.pisl@siemens.com