PaDok® - Patientenbegleitende Dokumentation

Ein Konzept zum sicheren Austausch vertraulicher medizinischer Daten

Das Konzept von PaDok basiert auf dem Bereitstellen[1] von Daten[2] auf einem gemeinsamen Server[3] und dem Weiterleiten[4] dieser Daten an einen autorisierten[5] Empfänger.

1) Bereitstellen von Daten läßt die frei Wahl des Empfängers offen:

Eine Übertragung von Daten erfordert Sender und Empfänger. Bei den typischen Vorgängen des medizinischen Praxisalltags, wie Überweisung, Einweisung, Rezept oder Verordnung häuslicher Pflege ist der Empfänger jedoch beim Erzeugen der Nachricht nicht zwangsläufig bekannt. Er kann wegen des gesetzlichen Rechts auf freie Arzt- (und Apotheker-, Krankenhaus-) Wahl durch den Patienten bestimmt werden. Deshalb können Nachrichten nur für eine berechtigte **Gruppe** (z.B. Radiologen, Orthopädische Kliniken, Apotheken, ...) **bereitgestellt** werden. Diese Bereitstellung erfolgt bei PaDok auf einem regionalen Server.

Zum Übertragen auf den Server werden die Daten digital signiert, anschließend nach einem besonderen Verfahren verschlüsselt, sowie mit einer weiteren. äußeren Signatur zur Integritätsprüfung versehen.

2) Absender trägt die Verantwortung für die Auswahl der Daten:

„... personenbezogene medizinische Daten dürfen nur zum **bestimmungsgemäßen Gebrauch** (also im Zusammenhang mit einem konkreten Behandlungs-Auftrag) übertragen, bearbeitet und gespeichert werden ...“

Diese gesetzliche Forderung verlangt eine fallbezogene, bewußte Auswahl von Informationen, die einer weiterbehandelnden Einrichtung zu einem bestimmten Patienten zur Verfügung gestellt werden sollen. Die Auswahl dieser Informationen unterliegt der Sorgfaltspflicht desjenigen Arztes, der die Daten lokal in seinem Datenbestand verwaltet.

PaDok bietet ein Schnittstelle, solche im lokalen Praxis-Verwaltungssystem ausgewählten Daten an einen Austausch-Server zu übermitteln.

3) Der PaDok-Server spielt den Mittler zwischen Sender und Empfänger:

Der Server überprüft die äußere Signatur aller eingehenden Nachrichten, wobei diese Signatur entfernt wird. Die Verschlüsselung und die innere Signatur der Nachrichten bleibt erhalten.

4.) Weiterleiten von Nachrichten erfordert die Identifikation des Anforderers

Nachrichten können an einen festen Adressaten gerichtet sein (z.B. Arztbrief). Solche Nachrichten sind mit dem public Key des (bekannten) Empfängers verschlüsselt und werden in dieser verschlüsselten Form bis zum Abruf zwischengelagert. werden solche Nachrichten vom richtigen Adressaten angefordert, werden sie, durch eine zusätzliche äußere Signatur des Servers gesichert, in unveränderter Form weitergeleitet.

Nachrichten, die an eine Adressatengruppe (Radiologen, ...) gerichtet sind, sind nach einem speziellen, zum Patent angemeldeten Verfahren verschlüsselt. Eine Entschlüsselung ist weder mit dem Key des Servers noch mit dem irgendeines Arztes möglich. Wenn einer der berechtigten Empfänger durch die Vorgangskennung der betreffenden Nachricht autorisiert wird, kann der Server die Nachricht so **umschlüsseln**, daß sie für den – jetzt bekannten – Empfänger mit dessen Schlüssel lesbar wird. Das wesentliche dieses ebenfalls zum Patent angemeldeten Umschlüsselungsvorganges ist, daß die Daten dabei niemals in entschlüsselter Form vorliegen oder auch nur die Voraussetzungen für ihre Entschlüsselung gegeben sind.

5) Empfänger werden durch Fachgruppe, Patient und Fall autorisiert

Registrierte Mitglieder eines Ärztenetzes können Nachrichten beim Server abfordern. Dies betrifft Nachrichten, die an eine bestimmte Praxis oder einen bestimmten Arzt adressiert sind, wie z.B. Befundbriefe, Entlassungspapiere etc. Solche Dokumente, die von vornherein einen eindeutigen Empfänger haben, können **direkt** angefordert werden.

Interessanter sind solche Dokumente, für deren Empfang die betreffende Praxis dadurch autorisiert wird, daß der Patient mit seinem Überweisungsschein (Rezept, Einweisung etc.) eine entsprechende „Vorgangskennung“ überbringt und damit eine „1 aus n“-Auswahl trifft. Hier muß der Empfänger sich durch seine Zugehörigkeit zu einer **Leistungsgruppe** und die **Vorgangs-ID** autorisieren, die der Patient ihm mit dem (gesetzlich weiterhin immer noch notwendigen) Papierdokument oder auf einer (vielleicht in absehbarer Zeit verfügbaren) elektronischen Patientenkarte überbringt.

6) Sicherheit geht über alles

Sender, Empfänger und Server müssen über die technischen Möglichkeiten einer digitalen Signatur und einer harten Verschlüsselung verfügen. PaDok verwendet für diesen Zweck die NetKey-Karten der **TeleSec** nach TCOS 2.0 bzw. 2.2.

Die Kommunikation zwischen den PaDok-Clients und dem PaDok-Server erfolgt über den Austausch von „Remote Procedure Calls“, was eine extrem ritualisierte und damit sichere Kommunikation ermöglicht. Standard-Internet-Ports werden für den Austausch nicht benötigt und sollten **nicht aktiviert** sein, um Einbrüchen vorzubeugen.

St. Ingbert, Juli 2000

Fraunhofer Institut Biomedizinische Technik

Juli 2000

Fraunhofer Institut für Biomedizinische Technik
Arbeitsgruppe Medizin-Telematik

Leiter: B. Bresser
Telefon 06894 980 206
Telefax 06894 980 117
Mobil 0173 351 3322
e-Mail bertram.bresser@ibmt.fhg.de

Ensheimer Straße 48
D 66386 St. Ingbert

Zentrale:
Telefon 06894 980 0
Telefax 06894 980 400