Die SSP – Security Service Platform

Claus-Werner Brill

Ausgangspunkt

Die Telematik gilt als eine Schlüsseltechnologie zur Fortentwicklung des Gesundheitswesens. In den vergangenen Monaten und Jahren haben sich immer weitere Kreise dieses Themas angenommen, die telematische Lösungen aktiv mitgestalten möchten. Fast täglich flattern neue Konzepte und Vorschläge auf den Tisch der beteiligten Ministerien, Verbände, Unternehmen und Organisationen.

Allein zu dem Thema Elektronisches Rezept existieren mittlerweile für Deutschland etwa 20 unterschiedliche Konzepte, ohne dass mit jeder dieser Varianten ein grundsätzlich neuer Ansatz verfügbar wäre. Möchte man wenigstens die aussichtsreichsten Kandidaten aus dieser stattlichen Zahl in vergleichenden Modellversuchen testen, steht man vor einem großen Problem: Es existieren bundesweit rund 250 unterschiedliche Arzt- und Apotheken-DV-Systeme und für jeden Modellversuch ist es prima vista erforderlich, eine eigene Einbindung für jedes beteiligtes Softwarehaus vorzunehmen. Das ist mit den bisher vorhandenen Konzepten finanziell und technisch kaum zu leisten.

Hinzu kommt, dass das Elektronische Rezept nur eine von zahlreichen Anwendungen ist, die in Zukunft Sicherheitstechnologien nutzen werden. Eine Fülle weiterer Applikationen wird in ganz ähnlicher Weise, wie das beim Elektronischen Rezept der Fall ist, auf Sicherheitstechnologie aufsetzen. Die bestehenden Anwendungen müssen dabei eine Anbindung an Karten- und Sicherheitskomponenten erfahren. Diesen Herausforderungen kann man begegnen, wenn man eine generische, universelle und modular aufgebaute Middleware-Komponente zum Einsatz bringt.

Die WuV[1] hat in den vergangenen Jahren ein Softwaremodul (Health Card Server, HCS) als Prototyp erstellt, das die Datenströme und die Sicherheitsfunktionen für das Elektronische Rezept und die Arzneimitteldokumentation realisiert. Dieses Produkt wurde national und supranational in die fachliche und politische Diskussion eingebracht; die Applikationen sind mittlerweile auch Gegenstand weltweiter Standardisierungsarbeiten.

Nun wurde der Health Card Server (HCS) zur Security Service Platform (SSP) weiterentwickelt, um durch diese Middleware die Sicherheitsfunktionen und das Handling von Chipkarten für unterschiedlichste Applikationen zur Verfügung zu stellen und eine leichte Integration zu ermöglichen.

Aufgaben

Die SSP soll insbesondere folgende Aufgaben übernehmen:

- einfache Integration von Sicherheitsfunktionen und Chipkartenhandling in EDV-Systeme;
- Bereitstellung von sicheren Kommunikationswegen;
- Management der Ressourcen einer Telematik-Plattform;
- Bedienung der gegenwärtigen, heterogenen Systemlandschaft und Offenheit für neue Entwicklungen;
- Offenheit für die Übernahme applikationsnaher Aufgaben im Rahmen einer Gesundheitsplattform (Qualitätssicherung).

Die SSP ist zwar aus den Bedürfnissen des Gesundheitswesens entstanden, sie ist jedoch auch für beliebige andere Bereiche einsetzbar, bei denen ein Bedarf für eine vertrauenswürdige Kommunikationsplattform existiert.

Leistungsmerkmale

Die SSP zeichnet sich durch folgende Leistungsmerkmale aus:

- plattformunabhängige Applikation (Programmiersprache Java);
- modularer Aufbau: Kernkomponente ist ein eigenständiges, relativ umfangreiches Basismodul, das um beliebig viele kleine, anwendungsspezifische Module erweitert werden kann;
- Basismodul: stellt alle kryptographischen Grundfunktionen (Ver- und Entschlüsseln, Authentifizieren, Signieren, Verifizieren) sowie Kommunikationsfunktionen (kanalorientiert und paketorientiert) zur Verfügung und übernimmt das Management der Ressourcen;
- UnterstützungunterschiedlicherSchnittstellen, Sicherheitstoolkits, Datenformate und Darstellungskomponenten;
- Unterstützung von Client-Server-Modellen zur Realisierung eines Remotezugriffs auf Sicherheitskomponenten.

Die bisher im HCS integrierten Applikationen Elektronisches Rezept und Arzneimitteldokumentation werden als Zusatzmodule innerhalb der SSP implementiert. Sollen verschiedene Varianten für das eRezept erprobt werden, ist es lediglich erforderlich, das entsprechende ER-Modul auszutauschen bzw. zu ergänzen. Erst die einheitliche technische Basis ermöglicht die Vergleichbarkeit verschiedener Modelle im Rahmen von Modellversuchen. Bei Einbindung weiterer Anwendungen werden entsprechende applikationsnahe Zusatzmodule integriert.

Im Ergebnis steht mit der SSP eine universelle und generische Middleware zur Verfügung, die den Aufbau kompatibler Kommunikationsstrukturen im Gesundheitswesen und darüber hinaus vereinfacht und fördert.

Autor: Claus-Werner Brill
Titel: Die SSP – Security Service Platform
In: Jäckel (Hrsg.) Telemedizinführer Deutschland, Ober-Mörlen, Ausgabe 2004
Seite: 122-123

Aufbau der SSP

Bei der SSP handelt es sich um eine lauffähige Applikation, die auf der Programmiersprache Java basiert und daher eine Java Virtual Machine auf dem Zielsystem benötigt. Die Systemarchitektur umfasst die Modulgruppen In/Out, Taskmanager und Services (Abbildung 1).

In/Out ❶

Die Modulgruppe In/Out stellt definierte Schnittstellen für die zugreifenden Anwendungen zur Verfügung:

- filebasierte Schnittstelle ⇒ für die Kommunikation mit Warenwirtschaftssystemen und Praxisverwaltungssystemen[2];
- streambasierte Schnittstelle (TCP/IP Socketverbindung) ⇒ ermöglicht die Kommunikation mit anderen Applikationen (via http/SOAP) und durch die Proxyserver-Funktionalität einen sicheren Web-Zugriff;
- PKCS# 11.

Die Modulgruppe kann um weitere Systemschnittstellen ergänzt werden.

Taskmanager ❷

Die Modulgruppe Taskmanager übernimmt die Bearbeitung und Kontrolle eines Auftrags. Um Kollisionen zu vermeiden, wird der Zugriff auf die der SSP zur Verfügung stehenden Ressourcen (Sicherheitstoolkit, Smart Cards) gesteuert.

Services ❸

Unter Services versteht man Komponenten, die die Funktionalität der SSP zur Verfügung stellen. Das Basismodul umfasst folgende Services:

- Zertifikatsverwaltung
- HPC (Health Professional Card) ⇒ stellt die gesamte Funktionalität der HPC bereit; einzelne Funktionen können auch mit Chipkarten, die nicht den vollen Leistungsumfang der HPC abdecken, genutzt werden (Beispiel: Funktion „Signieren“ mit einer entsprechenden Signaturkarte)
- Email
- Transport ⇒ stellt diverse, auf TCP/IP basierende Wege für kanal- und paketorientierte Kommunikation bereit (http, FTP, SOAP über http, SMTP, POP3 – alle optional via SSL)
- Authentisieren
- Darstellungskomponente + Fehlerdarstellung
- In/Out zum Sicherheitstoolkit (STK) ⇒ repräsentiert die Gesamtfunktionalität des STK, die mittels diverser Interfaces zum STK bereitgestellt wird.

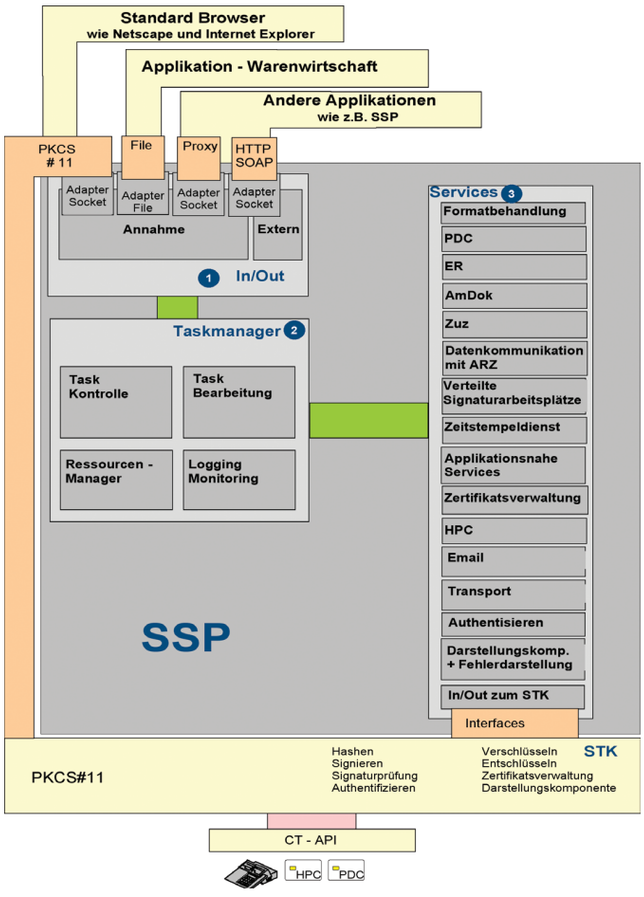

Abbildung 1: *Systemarchitektur der SSP mit für das Telematik-Projekt der ABDA relevanten Zusatzmodulen*

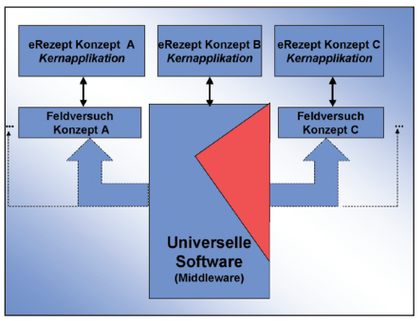

Abbildung 2

Die erste anwendungsspezifische Implementierung steht im Kontext mit dem eRezept und dem Arzneimittelpass. Folgende Module werden dazu ergänzt:

- Formatbehandlung ⇒ konvertiert und prüft die unterschiedlichen zum Einsatz kommenden Datenformate (ASN.1, XML)
- PDC (Patient Data Card)
- ER (eRezept)
- AmDok (Arzneimitteldokumentation)
- Zuz (Zuzahlungsfunktion)
- Datenkommunikation mit dem ARZ (ARZ = Apothekenrechenzentrum) sobald verfügbar:
- verteilte Signaturarbeitsplätze ⇒ Realisierung der Signaturfunktion remote über ein Inhouse-Netz

Das Modul Zeitstempeldienst wird bei Bedarf realisiert, die applikationsnahen Services (z.B. Plausibilitätsprüfungen im Zusammenhang mit dem eRezept) im Zusammenhang mit den jeweiligen Anwendungen.

Fußnoten

1 WuV – Werbe- und Vertriebsgesellschaft Deutscher Apotheker ist eine 100%ige wirtschaftende Tochter der ABDA-Bundesvereinigung Deutscher Apothekerverbände.

2 Die Befehlssyntax ist an den VCS-Standard angelehnt, eine VCS-Konformität kann durch einen entsprechenden Service (s.u.) realisiert werden.