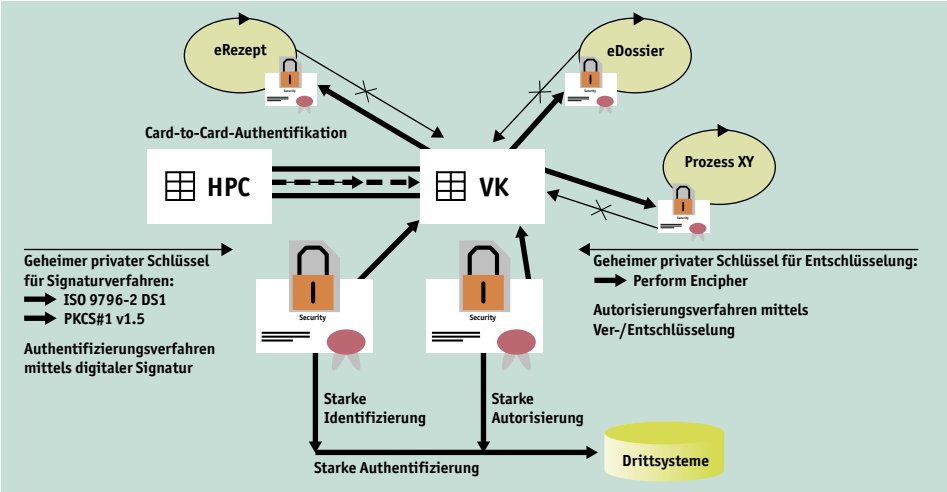
Versichertenkarte: Philosophie und Umsetzung des Konzeptes

Die elektronische Versichertenkarte für die obligatorische Krankenversicherung, die im Verlauf des Jahres 2009 getestet wird, orientiert sich an einem pragmatischen Ansatz. Aufwand und Kosten für Einführung und Handhabung sollen möglichst minimiert werden, dies bei einem möglichst hohen Niveau an Verlässlichkeit und Sicherheit. Ansätze von Gesamtsystemen, wie beispielsweise die Gesundheitskarte in Deutschland, haben sich unter diesen Vorgaben als nicht zielführend erwiesen. Im nachfolgenden Artikel werden die technischen und anwendungsbezogenen Aspekte der Versichertenkarte aus der Optik der mit der Umsetzung betrauten Firma vorgestellt.

Grafik 1

Public-Key-Verfahren der elektronischen Versichertenkarte



Quelle: Stadlin / Die Volkswirtschaft

Angeregt durch die Gründung der Gesellschaft «Gematik» in Deutschland im Jahre 2004, welche im Rahmen der neu einzuführenden deutschen elektronischen Gesundheitskarte ein riesiges Regelwerk aufzubauen begann, befasste sich das Bundesamt für Gesundheit (BAG) mit der konkreten Einführung der elektronischen Versichertenkarte. Diese wurde durch die Verordnung über die Versichertenkarte für die obligatorische Krankenpflegeversicherung (VVK) vom 14.02.2007 bezüglich Inhalt und Anwendung definiert. Zur möglichst raschen Umsetzung der VVK und zur Einführung der Chipkarte beauftragte das BAG die Firma Arpage AG[1] im April 2007, in Zusammenarbeit mit der entsprechenden Fachgruppe des eCH-Vereins einen technischen Standard auszuarbeiten. Bereits Anfang Februar 2008 konnte der Standard[2] genehmigt werden. Dabei soll die Versichertenkarte auch als Katalysator für die zukünftigen Entwicklungen im Gesundheitswesen dienen.

Peter Stadlin
Arpage AG

Technische Komplexität sicherer Betriebssysteme

Im Gegensatz zur heutigen Versichertenkarte enthält die elektronische Versichertenkarte einen kleinen Datenspeicher, einen Mikroprozessor, eine elektronische Kommunikationsschnittstelle und ein Chipkartenbetriebssystem. Die technische Komplexität solcher sicheren Betriebssysteme ist relativ hoch.

Prozessor-Chipkarten verfügen über einen Mikroprozessor, über den man auf die gespeicherten Daten zugreifen kann. Es gibt oft keine Möglichkeit, auf den Datenbereich direkt zuzugreifen. Der Umweg über den Mikroprozessor erlaubt es, die Daten auf der Karte über kryptografische Verfahren vor fremdem Zugriff zu schützen. Die Chipkarten können als sicherer Informations- oder Schlüsselspeicher dienen, aber sie bieten auch verschiedene Sicherheitsdienste wie Authentifikation, Verschlüsselung/Entschlüsselung, Signatur, Zertifikatsverifikation usw. an. Da die privaten Schlüssel auf der Chipkarte nicht auslesbar gespeichert sind, ist das Erspähen des Schlüssels nicht möglich. Deshalb ist die Signaturerzeugung, die Entschlüsselung eines Autorisierungsdatenobjektes oder die Zertifikatsverifikation auf der Chipkarte sehr sicher.

Das hier verwendete Public-Key-Verfahren[3] (siehe *Grafik 1*) beruht auf zwei Schlüs-

1 Die Firma Arpage AG ist unter anderem Technologielieferant der Health Info Net AG, welche seit 1996 eine gesicherte elektronische Extranet-Plattform im Gesundheitswesen betreibt und bereits 11 000 Ärzte und 110 Spitäler eingebunden hat.
2 eCH0064 «Spezifikationen für das System Versichertenkarte».
3 Zurzeit werden häufig folgende Algorithmen benutzt: RSA, ElGamal und elliptische Kurven (ECC).

Kasten 1

Definition von eHealth

Unter eHealth oder Electronic Health versteht man den Einsatz von Informations- und Kommunikationstechnologien zur Verminderung des administrativen Aufwandes, zum gesicherten Austausch und Zugriff auf Ressourcen und Daten sowie elektronische Mittel zur wirksamen Prozessvereinfachung und -verbesserung im Gesundheitswesen. An diesem heterogenen Gebiet partizipieren im Wesentlichen die Leistungserbringer (Ärzte, Therapeuten, Spitäler usw.), Kostenträger (Versicherte, Versicherungen und Kantone), IT- Dienstleistungsanbieter und Investitionsgüteranbieter sowie die Pharmaindustrie.

Kasten 2

Datencontainer und Funktionalitäten der Versichertenkarte

- *Administrative Daten:* Diese können aus der Versicherten-Chipkarte öffentlich ohne Zugangsschutz ausgelesen werden. Darin sind neben den Angaben über den Versicherten und dessen Versicherungsdaten ebenfalls die Identifikatoren als Kennnummer der Versichertenkarte und als AHV-Nummer des Versicherten enthalten.
- *Notfalldaten:* Der Zugriff auf diese Daten wird durch eine sogenannte Card-to-Card-Authentifizierung mittels einer gültigen Leistungserbringer-Chipkarte (HPC) so eingeschränkt, dass nur berechtigte Leistungserbringer in spezifischen Rollen Zugang zu diesen Daten haben. In diesen Datenobjekten können auch Hinweise auf Personen und technische Ressourcen (Entitäten) abgelegt werden.
- *Schlüsselpaar für Signaturverfahren:* Dieses Schlüsselpaar dient ausschliesslich für Signaturverfahren, welche bei der Card-to-Card-Authentifizierung und für die Authentifizierung auf elektronische Ressourcen verwendet werden. Zur Verfügung gestellt werden sowohl das speichersparsame und sehr sichere Signaturverfahren nach ISO/IEC 9796-2 DS1, welches auch autonome Zertifikatsverifikationen auf der Chipkarte selbst erlaubt, als auch das populäre Signaturverfahren nach PKCS#1 v.1.5, wie es bei der Authentifizierung mittels einer verschlüsselten Verbindung mit http über SSL/TLS angewandt wird. Entsprechende Datencontainer zur Abspeicherung von Zertifikaten wurden ebenfalls auf der Versichertenkarte vorgesehen (X.509, CVC). Die Verwaltung der entsprechenden Zertifikate und Identifikatoren kann seitens der eHealth-Dienstleistungsanbieter mittels innovativer Verfahren und intelligenter Technologien so gelöst werden, dass der Aufwand minimal wird. Damit erlaubt die Versichertenkarte als Träger von Identifikatoren des Versicherten einen stark authentisierten Zugang auf eine grosse Vielfalt von Ressourcen und Diensten, wie u.a. E-Patientendossier, KIS und Versicherungsdienstleistungen.
- *Schlüsselpaar für Autorisierungsverfahren:* Der Umstand, dass die Versichertenkarte über eine Funktion verfügt, die ein zuvor mit ihrem öffentlichen Schlüssel durch einen Antragsteller verschlüsseltes Transaktionsdatenobjekt mit ihrem geheimen und nicht auslesbaren privaten Schlüssel wieder entschlüsseln kann, erlaubt eine starke Autorisierung. Damit können Verfahren für die Zuweisung im Zusammenhang mit elektronischen Rezepten, elektronische Freigaben von Patientendossiers zur Überweisung an andere Leistungserbringer usw. realisiert werden.
- Bezüglich *Zugang zu Funktionen und Daten* unterstützt die Versichertenkarte vollständig die internationalen Standards wie ISO/IEC 7816, PKCS#11 und mit handelsüblichen Lesegeräten den Standard PC/SC.

seln: einem öffentlichen (auslesbar) und einem privaten (geheim und nicht auslesbar). Der eine Schlüssel wird vom anderen abgeleitet. Dabei gibt es bei einem guten so genannt asymmetrischen Verfahren keine Möglichkeit, aus einem Schlüssel den anderen zu berechnen. Wenn man nun eine geheime Botschaft übermitteln will, verschlüsselt man sie mit dem öffentlichen Schlüssel des Empfängers. Nur der Empfänger kann die Botschaft mit seinem eigenen geheimen privaten Schlüssel auf der Chipkarte entschlüsseln. Diese Sachverhalte können zur eindeutigen Identifikation benutzt werden, wobei der geheime private Schlüssel auf der Chipkarte als Identifikator dient.

Schlüsselfunktion der Identifikatoren

Die Versichertenkarte wird von den Versicherern herausgegeben und beinhaltet unveränderbar auslesbare administrative Daten über den Versicherten, die Versicherungsgesellschaft und die Versicherungsart. Ebenfalls sind die eindeutige Kennnummer der Versichertenkarte und die AHV-Nummer des Versicherten unveränderbar auslesbar abgespeichert. Beide Nummern können zur Bildung von Identifikatoren verwendet werden.

Identifikatoren unterliegen ihren eigenen Lebenszyklen. So ist die Kennnummer der Versichertenkarte an die Gültigkeit der Versichertenkarte gebunden. Muss die Versicherung dem Versicherten eine neue Versichertenkarte infolge Änderungen der administrativen Daten herausgeben, so enthält die neue Versichertenkarte eine neue eindeutige Kennnummer; die AHV-Nummer des Versicherten bleibt aber die gleiche. Der Lebenszyklus der Kennnummer der Versichertenkarte ist an die Karte selbst gebunden und hängt mit deren Gültigkeit zusammen, während die AHV-Nummer an den – hoffentlich sehr langen – Lebenszyklus des Versicherten gebunden ist. Auf der Versichertenkarte sind zwei Schlüsselpaare gespeichert mit je einem geheimen, nicht auslesbaren, aber kryptografisch anwendbaren privaten Schlüssel. Diese beiden privaten Schlüssel mit ihren dazugehörenden öffentlichen Schlüssen sind damit zwei weitere Identifikatoren mit entsprechenden Lebenszyklen.

Diese Schlüssel «verbrauchen» sich aus sicherheitstechnischer Betrachtung in Abhängigkeit ihrer Schlüssellänge bei gegebenem Public-Key-Verfahren. Sie unterliegen deshalb als Identifikatoren einem meist sehr viel kleineren Lebenszyklus als etwa die AHV-Nummer des Versicherten und werden deshalb bezüglich Lebenszyklus an die Lebensdauer der Versichertenkarte gebunden. Im eHealth-Bereich des Gesundheitswesens gibt es viele Prozesse und Ressourcen, welche jeweils mittels eines eigenen Identifikators eindeutig referenziert werden. Es gibt nun Ansätze von Gesamtsystemen, welche zusätzlich auch solche Prozess- und Ressourcenidentifikatoren in Form von Schlüsselpaaren mit wiederum eigenen Lebenszyklen auf einer elektronischen Gesundheitskarte abspeichern möchten. Damit werden der Verwaltungsaufwand und die Unterhaltskosten einer solchen Chipkarte unserer Meinung nach massiv erhöht (Widerruf von Chipkarten infolge von Prozess- und Ressourcenänderungen und deren Lebenszyklen).

Grundsätze zur Reduktion von Aufwand und Kosten

Um den Aufwand und die Kosten für die Versichertenkarte möglichst zu minimieren, wurden folgende Grundsätze definiert:

1. Möglichst wenige Schlüsselpaare (zwei genügen vollständig);
2. die Lebenszyklen der Schlüsselpaare stehen zueinander in einer Beziehung (Kohärenz);
3. möglichst wenige Träger von Identifikatoren (Chipkarten) im eHealth-Bereich (Versichertenkarte als elektronischer Ausweis des Versicherten soll einen grossen Teil der Anforderungen abdecken).

Die technische Umsetzung der Versichertenkarte gemäss VVK wird im Standard definiert. Die erweiterten Funktionalitäten, welche für sogenannte kantonale Modellversuche genutzt werden können, sind nicht spezifisch in diesem Standard definiert.

Zusammenfassend genügt unserer Meinung nach die vorhandene Versichertenkarte den Anforderungen im eHealth-Bereich vollauf. Eine Weiterentwicklung zu einer elektronischen Gesundheitskarte erachten wir als nicht notwendig.

Ausblick

Die Arpage AG unterstützt Santésuisse sowie die Herausgeber der Leistungserbringerkarte HPC bezüglich der Umsetzung. Die Erarbeitung der sehr technischen Detailspezifikationen der Versichertenkarte und die Kommunikationsspezifikationen für die Card-to-Card-Authentifizierung sind in Arbeit und sollten Ende November 2008 fertiggestellt sein. Erste Testkarten sind Ende 2008 voraussichtlich verfügbar, sodass die Versichertenkarte Anfang 2009 getestet werden kann. ▮