

e-card in Austria

Heinz Otter, Leiter Bereich Strategische Projekte, SV-Chipkarten Betriebs- und Errichtungsges .m.b.H.

1 Grundlagen der e-card

1.1 Gesetzliche Basis

Der Hauptverband der Österreichischen Sozialversicherungsträger hat 1999 mit der 56. ASVG-Novelle (Ä§Ä§ 31aff.) den gesetzlichen Auftrag bekommen, das sogenannte "Elektronische Verwaltungssystem (ELSY)" einzuführen und dessen Betrieb sicher zu stellen. Dieses "ELSY" hat die Verwaltungsabläufe zwischen Versicherten, Sozialversicherungsträgern und Dienstgebern usw. zu unterstützen. Es handelt sich somit (zunächst) um ein "Sozialversicherungsverwaltungssystem", dessen erste Applikation (von mehreren möglich, wie z.B. eÜberweisung eRezept) jene des "Krankenscheinersatzes" (Ä§ 31c ASVG) ist.

Die Ausstellung der e-card ist für den Versicherten mit keinen Kosten verbunden. Es ist jedoch eine Chipkarten-Servicegebühr von jährlich a 10 nach Ä§ 135 Abs. 3 ASVG zu entrichten.

1.2 Resultierende Anforderungen an das System

Die gesetzlich explizit definierten Anforderungen sind:

- Die e-card soll als Keycard (= Schlüsselkarte) konzipiert werden. D.h. die e-card ist grundsätzlich nicht Träger applikatorischer (Software-)Funktionen, sie enthält lediglich Identifikationsdaten, welche die Voraussetzung für die Zugriffsberechtigung auf Applikationen bilden.
- Die Forderung nach Nachladbarkeit kostenloser Applikationen begründet den sogenannten multiapplikativen Rahmen der e-card
- Für den Controllingbereich (z.B. der Sozialversicherung) wird gefordert, dass das System e-card als Instrument zur Unterstützung der Transparenz ärztlicher Leistungen und Kosten dient.
- Inhabern von Kartensystemen mit Bürgerkarten-Funktionalität muss es (auch ohne e-card) möglich sein, einen Arzt zu konsultieren.

Weitere Anforderungen betreffen den Stand der technologischen Entwicklung, welche hier im Wesentlichen die Signaturen-Aspekte reflektieren:

- Bürgerkarten-Funktionalität: Die e-card soll Signaturapplikationen gem. SigG/ SigV und der Verwaltungssignaturverordnung VW-SigV enthalten
- Die e-card muss den Zugang zu den e-Applikationen der Sozialversicherungsträger über das eSV-Portal (gemeinsames Projekt der Sozialversicherungsträger) ermöglichen
- Das e-card System muss durch geeignete Mechanismen die Elektronische Abrechnung der Ärzte (gesetzlich verbindlich seit 01.01.2003) ergänzen.

An allgemeinen systemischen Anforderungen sind zu beachten:

- Bzgl. der technischen Ausrichtung der Endanwender ist der IT-Nutzungsgrad ab (Herbst) 2005 zu berücksichtigen (Heim-PC mit Chipkartenleser)
- Bei der Realisierung von Systemkomponenten ist die Umsetzung von einschlägigen Normen und Standards obligatorisch
- Interoperabilität ist entsprechend den Entwicklungen in Europa zu unterstützen.

Schließlich ist noch die Offenheit des Gesamtsystems wesentlich:

- Die Generierung neuer Applikationen ist durch Nachladbarkeit von Daten, Datenstrukturen sowie (Krypto-) Schlüssel-Files in die e-cards sicherzustellen
- Flexibilität bzgl. Innovation und Migration, d.h. der gleichzeitige Betrieb mehrerer "Generationen" von Chipkarten mit unterschiedlichem Funktionsumfang, muss möglich sein.

2 Die e-card mit Anwendungsschwerpunkt eSocial Security und eHealth

Die leistungsstarke Infrastruktur des e-card-Systems ist für eine Vielzahl von Folgeprojekten ausgelegt. Aus heutiger Sicht sind (zumindest) folgende ergänzende Applikationen bzw. Systemerweiterungen in neue Anwendungsbereiche geplant:

- Arzneimittelbewilligungsservice (Ärztliche Genehmigung)
- Vorsorgeuntersuchung (sogenannte VU-NEU)
- Einbindung der Krankenanstalten
- eRezept
- Überweisung/ Zuweisung
- Dienstgeber-Meldewesen
- EKV (EHIC)/ Net@rds
- sichere Befundübermittlung (Datenzugriff bei Dritten)
- Einbindung von sonstigen Vertragspartnern (Anspruchsnachweis)
- Einbindung von Wahlärzten (Versicherungsnachweis)
- Notfalldaten
- Elektronische lebensbegleitende Gesundheitsakte (ELGA)
- Zusatzversicherungen
- Gesundheitsportale

Die genannten Projekte gehören gemeinsam mit ihrer ggf. angewandten Signaturfunktionalität in eine Gesamtkonzeption der österreichischen Gesundheitstelematik eingebunden. Das hierfür relevante Gesundheitstelematikgesetz (GTelG) ist 2005 im Rahmen des Gesundheitsreformgesetzes 2005 in Kraft getreten.

Die Ergebnisse der im Umfeld des Bundesministeriums für Gesundheit und Frauen eingerichteten und seit Mitte 2005 aktiven Arbeitskreise (eHealth-Initiative, ELGA) werden auch für die Reihenfolgeplanung der Projekte Prioritätskriterien liefern.

3 Die e-card mit Anwendungsschwerpunkt für den Bereich E-Government

3.1 Synergetische Auswirkungen neuer Rechtsgrundlagen

Aus volkswirtschaftlicher Sicht ist es sinnvoll, nicht nur ein Sozialversicherungsprojekt zu errichten, sondern die Möglichkeiten verfügbarer Technik (z.B. Elektronische Signaturfunktionen) sowie die Rechtslage für ein allgemeines Bürgerkartensystem zu nutzen.

Mit dem E-Government-Gesetz (E-GovG) sind die Grundlagen für die erforderlichen Standards geschaffen worden (BGBl.I Nr.10/ 2004, 1. März 2004).

Weiterer Ausdruck dieses Zieles ist das Sozialversicherungsänderungsgesetz (SVÄG 2004, BGBl.I Nr.18/ 2004, 1. März 2004), mit welchem dem Hauptverband ausdrücklich aufgetragen wird, die Versicherungsnummern mit den sogenannten bereichsspezifischen Personenkennzeichen nach dem E-GovG zu verknüpfen (§ 31 Abs.4 Z1 ASVG) und außerdem die Bürgerkartenfunktion für das e-card-System nutzbar zu machen.

Das SVÄG 2004 bewirkt rechtlich, dass die e-card keine dedizierte Sozialversicherungskarte mehr ist, sondern ausdrücklich strategischer Teil des E-Government wird.

3.2 Von der SV-Chipkarte zur Bürgerkarte

Die o.e. Gesetze wirken sich auf die Gestaltung der (Signatur-)Zertifikate aus, welche (neben der Krankenscheinersatz-Applikation) auf der e-card zu speichern sind.

Entsprechend der Grundlage des ELSY im ASVG, d.h. im Vollziehungsbereich der Sozialversicherung, war geplant, auf die e-cards Zertifikate aufzubringen, welche zum Zwecke der eindeutigen Identifikation des Signators mit dem Ordnungskriterium Versicherungsnummer verknüpft sind. Diese Lösung hätte ausschließlich der sozialversicherungsinternen Organisation gedient und hierfür genügt.

Wenn eine im öffentlichen, aber auch im privaten Bereich allgemein verwendbare elektronische Ausweismöglichkeit via Signaturzertifikat geschaffen werden soll, ist die Speicherung von Identifikationsdaten und eine daraus resultierende Personenbindung so zu implementieren, dass z.B. die Namensschreibweisen 1 exakten Formalkriterien genügen müssen.

3.3 Prozess zur eindeutigen Identifikation des Signators

Beim Einsatz von Elektronischen Signaturen zur Identifikation und Authentifikation beim telematikgestützten

Datenaustausch garantieren Verfahren nach dem Signaturgesetz u.a. nur die Nachprüfbarkeit der Echtheit einer Signatur. Im Falle von „Personendaten-Gleichheit“ (z.B. unter Berücksichtigung der in praxi unterschiedlichen Schreibweisen von Namen) ist es i.d.R. nicht möglich, den Signator („physisch“) eindeutig zu identifizieren. Somit fehlt in herkömmlichen Zertifikaten allein eine wesentliche Voraussetzung für die automatisierte Abwicklung von Anwendungen im E-Government.

Aus diesem Grunde wird für alle in Österreich gemeldeten Bürger nach dem E-GovG nicht die Versichertendatenbank der Sozialversicherung, sondern das zentrale Melderegister ZMR herangezogen.

In diesem Kontext ist zudem eine wichtige Auflage des Datenschutzes zu erfüllen:

Es muss gewährleistet sein, dass die Aktivitäten eines Bürgers im Rahmen von E-Government unter Nutzung eines bereichsübergreifenden („universellen“) Ordnungskriteriums nicht verfolgt werden können.

Zur Ermittlung dieses sogenannten bereichsspezifischen Personenkennzeichens ist folgend vorzugehen:

- Die Zentrale Melderegister-Nummer ZMR 3 für jede gemeldete Person in Österreich (Datenbank des Bundesministeriums für Inneres) ist die Quelle für das Ableitungsverfahren des bPK (s.u.)
- Die Stammzahl SZ als kryptographische Einweg-Ableitung aus der ZMR identifiziert jede in Österreich gemeldete Person eindeutig
- Das Bereichskennzeichen BKZ kategorisiert die Anwendungsbereiche, welche von E-Government als elektronische Behördenleistungen telematikgestützt zugänglich sind
- Das bereichsspezifische Personenkennzeichen bPK ergibt sich schließlich aus der kryptographischen Verknüpfung (z.B. Hash-Funktion) von SZ & BKZ.

Bei Verwendung des bPK in der Personenbindung, welche zu einem Zertifikat in einer Bürgerkarte gehört, ist es bei Zugriffen auf E-Government-Anwendungen mit dieser Bürgerkarte nicht möglich die Stammzahl rückzurechnen.

3.4 Elemente der österreichischen E-Government-Strategie

3.4.1 „Bürgerkarten-Umgebung“ mit Schnittstelle Security Layer

Die Bedeutung der Security Layer-Schnittstelle erschließt sich aus den Anforderungen an das Protokoll zwischen (zentraler) E-Government-Anwendung und Signaturerstellungseinheit (z.B. Chipkarte). Die Protokollstruktur sollte für eine E-Government-Anwendung so einfach wie möglich sein, also aus einem übersichtlichen „Anfrage (Kommando)/Antwort“-Zyklus bestehen, welcher ausschließlich mit standardisierten Kommandos des „Gov-Servers“ auskommt.

„Oberhalb“ des Security Layers dürfen Abläufe nicht davon abhängig sein, mit welchen Signier-Mechanismen ein elektronischer Signaturvorgang „unterhalb“ des Security Layers abgewickelt wird. Nachfolgend das Prinzip einer beispielhaften Protokoll-Sequenz mit der Aufforderung seitens einer E-Government-Anwendung (im eGov-Server) an den Client (z.B. Heim-PC) ein „Dokument zu signieren“:

- Applikation sendet Kommando -> „Signiere Dokument“
- Bürgerkarten-Umgebung reagiert mit -> Antwort oder Fehlermeldung

Die Kodierung der Protokollelemente erfolgt in XML. Als Konsequenz dieser Protokollgestaltung muss die „Signatur-Client- Software“ eine gekapselte Ausprägung haben, welche in Österreich unter dem Begriff „Bürgerkarten-Umgebung“ bekannt ist. Diese Bezeichnung subsumiert, dass in der Client-Software alle für den endanwenderseitigen Signiervorgang erforderlichen Elemente zusammengefasst werden: PIN-Eingabe, Hashwert-Bildung, vertrauenswürdige Anzeige, Schnittstelle zum Signatur-Token (hier eine Chipkarte) und ggf. Zusatzspeicher.

Der „Security Layer“ inkl. Bürgerkartenumgebung (s. Abbildung 1) wurde von der IKT-Stabsstelle des Bundeskanzleramtes realisiert und ist in Generallizenz des Bundes unter: www.cio.gv.at/identity/bku downloadbar.

3.4.2 Technologie-Neutralität

Ein weiterer Vorteil der Bürgerkartenumgebung besteht in ihrer Technologie- Neutralität. Da unter der Kategorie „Signaturerstellungseinheit“ technologisch unterschiedliche Ausführungen von „Signatur- Token“ zum Einsatz kommen (z.B. Chipkarten, USB-Sticks, Palmtops, Handys), ist es wichtig, die E-Government-Anwendungen funktionen auch von diesen Ausführungsformen zu entkoppeln.

3.4.3 Personenbindung

Diese Kerneigenschaft der E-Government-Strategie wurde bereits unter Abschnitt 3.3 eingehend erläutert. In informatischer Ausprägung handelt es sich bei dem Konstrukt "Personenbindung" um eine XML-Datenstruktur, welche die Stammszahl, öffentliche Schlüssel und häufig verwendete Personendaten wie Name und Geburtsdatum enthält und von der Stammszahlregisterbehörde signiert wird.

Die Personenbindung wird auf der Bürgerkarte gespeichert, ist somit unter der Kontrolle des Bürgers und bestmöglicht die Verknüpfung zwischen Identifikationsdaten (Stammszahl des Bürgers) und Authentifizierungsdaten (Signaturstellungsdaten und Signaturprüfdaten)

3.5 Elektronische Signaturen der e-card

Auf der e-card werden Identifikationsdaten des Karteninhabers und mehrere Signaturapplikationen gespeichert. Für den Datenaustausch zwischen Ordination und Zentralsystem kommt beim "Krankenscheinersatz" die einfach verwendbare SV-Signatur, welche vom Patienten keine PIN-Eingabe verlangt, zum Einsatz.

Um die e-card im Bereich E-Government in Anwendungen nutzen zu können, für welche eine elektronische Unterschrift vorgesehen ist, benötigt man darüber hinaus rechtskonforme elektronische Signaturen gemäß E-GovG, Signaturgesetz (SigG) und Signaturverordnung (SigV) sowie Verwaltungssignaturverordnung (VW-SigV). Das E-GovG (§ 25) sieht vor, dass bis Ende 2007 statt sicheren Signaturen auch Verwaltungssignaturen gem. VW-SigV verwendet werden können.

Die e-card wird für die genannten Einsatzbereiche vorbereitet und nutzt die letztgenannte Möglichkeit, wobei der Hauptverband selbst ab Q4/ 2005 für die auf den ausgegebenen e-cards "schlummernden" Verwaltungssignaturen die Rolle des Zertifizierungsdiensteanbieters spielt. Geliefert werden die Chipkarten und das dazugehörige elektronische Kartenmanagementsystem vom Münchner Technologiekonzern Giesecke & Devrient in Zusammenarbeit mit der Deutschen Post Com. Diese erzeugt in ihrem Trust-center Signtrust die Zertifikate für die Signatur-Applikationen. Wünscht ein Karteninhaber explizit die Aufbringung des Zertifikates einer sicheren Signatur gem. SigG/ SigV, so ist dies anstelle der Verwaltungssignatur auch möglich. Zu diesem Zweck muss er die Dienstleistungen eines geeigneten Zertifizierungsdiensteanbieters in Anspruch nehmen.

In beiden Fällen ist immer die zusätzliche Aufbringung eines Zertifikates für die jeweilige Signatur verbunden, mit welcher z.B. Authentifizierungs- und Verschlüsselungsaufgaben durchgeführt werden können.

3.6 Die e-card als Bürgerkarte

Der Begriff "österreichische Bürgerkarte" steht nicht für einen speziellen Kartentyp, sondern vielmehr für ein Funktionskonzept, das Verwaltungsverfahren und Behördenwege auf elektronischem Wege für die Bürgerinnen und Bürger durch kryptographische Mittel sicher gestalten lässt und dadurch die elektronische Verfahrensabwicklung erst ermöglicht.

Das Bürgerkartenkonzept erfüllt die Grundanforderungen an sichere elektronische Signaturen. Damit wird die e-card als Signaturkarte in allen Bereichen der elektronischen Verwaltung allgemein einsetzbar. Voraussetzung hierfür ist, dass mittels eines einfachen und kundenfreundlichen Procedere entsprechende Zertifikate und die Personenbindung auf der e-card gespeichert werden. Damit ist in der e-card auch die Funktionalität der Bürgerkarte im Sinne des E-Government-Gesetzes integriert, welches mit dem GTeIG nun auch im Bereich der Gesundheitstelematik eine dem eHealth-Bereich angemessene gesetzliche Entsprechung gefunden hat.

Auf dieser Basis wird für die e-card der Zugang zu allen vorbereiteten Anwendungen in den Bereichen eSocial Security, eHealth, E-Government und eBusiness ermöglicht.

4 Systemkonfiguration des Infrastrukturprojektes e-card (Applikation Krankenscheinersatz)

4.1 Systemkonfiguration e-card und Subsysteme

Die Systemkonfiguration in Abbildung 2 ist in Verbindung mit dem Mengengerüst für die Basisapplikation Krankenscheinersatz (s. Projektumfang in Tabelle) zu interpretieren. Bezüglich Systemarchitektur wurden zwecks Modularität der zentralen Funktionen folgende wesentlichen Subsysteme definiert:

- Konsultationssystem (Teilprojekt 1)

Es enthält alle Funktionsmodule, welche sich mit dem für die Anspruchsprüfung erforderlichen Regelwerk der Sozialversicherung und mit dem Systembetrieb befassen. Diese zentralen Einrichtungen werden redundant und aus Verfügbarkeitsgründen (Online-System) an zwei verschiedenen Standorten errichtet.

- Kartensystem (Teilprojekt 2)

Hier werden jene Funktionsmodule zusammengefasst, welche grundsätzlich Karten- und Kartenapplikationsdaten verarbeiten. Hierzu zählen die Daten für die eigentliche Kartenproduktion, Zertifikatsdaten des Verzeichnisdienstes, kryptographische Schlüssel und Applikationsdaten der Anwendungsverwaltung (Card Application Management System). Dienstleistungen dieser Ausprägung werden i.d.R. von Trust Centern im Verbund mit Kartenherstellern überzeugend beherrscht. Aus diesem Grunde werden die entsprechenden IT-Einrichtungen beim e-card-System nicht physisch errichtet, sondern die Transaktionen des e-Kartensystems über Schnittstellen von kompetenten Partnern als Betriebsdienstleistungen zugekauft.

Weitere Teilprojekte wie Datennetzwerk, Call Center, Administrativer Client (zur Betreuung des Regelwerkes) sind nur angedeutet. Dienstleistungsorientierte Teilprojekte wie Rollout und Schulung sowie Koordination der Arztsoftware-Hersteller runden das Aufgabenspektrum des Systemintegrators SVC ab.

4.2 Mehrfachnutzung des Breitband-Netzwerkes

Abbildung 3 zeigt die gesamte Vernetzung der errichteten Infrastruktur. Der besondere Aspekt hierbei ist die Möglichkeit des Ressourcen-Sharings bei Nutzung des Gesundheits-Informations-Netzwerkes GIN. Die Applikation Krankenscheinersatz erfordert zwar aus Durchsatzgründen (Anspruchsprüfung binnen 5 Sekunden) die Performanz eines ADSL-Netzes, benötigt jedoch nicht dessen Breitbandigkeit.

Aus diesem Grunde werden auch sogenannte Mehrwertdienste des eHealth-Bereiches (z.B. Befundübertragungs- und Internet-Dienste der Ärzteschaft) über dasselbe Netz abgewickelt.

Die entsprechend sichere und geschützte Datenübermittlung mit applikationsabhängiger Prioritätssteuerung der jeweiligen Transaktionen übernehmen die IT-Einrichtungen der Peering Point-Gesellschaft, welche zu je 50 % im Aufsichts- und Verwaltungsbereich von österreichischer Ärztekammer und Hauptverband der österreichischen Sozialversicherungsträger betrieben wird.

5 Der Projektstatus

Die Darstellung der Meilensteine in Abbildung 4 liefert einen Einblick in den Fortschritt des Projektes e-card aus der Sicht Mitte Juli 2005. Zu diesem Zeitpunkt waren mehr als 2500 Ordinationen mit den IT-Komponenten zur Verarbeitung der e-card ausgestattet und mehr als 2 Mio. e-cards ausgegeben.

Die tägliche Rollout-Rate betrug 100 Ordinationen und 70.000 e-cards. Unter der Voraussetzung, dass diese Rollout-Geschwindigkeit in den Ordinationen auch in der Urlaubsperiode der Ärzte beibehalten werden kann, kommt das Projekt e-card mit seiner Basisapplikation Krankenscheinersatz noch vor Ende 2005 plangemäß zum Abschluss.

Kontakt

Dipl.-Ing. Heinz Otter
Leiter Bereich Strategische Projekte
SV-Chipkarten Betriebs- und
Errichtungsges.m.b.H.
A-1020 Wien
Schiffamtsgasse 15
Tel.: +43(1)7 14/ 36 75- 41 22
heinz.otter@chipkarte.at
www.chipkarte.at

1 Diakritischer Zeichenvorrat zur Namensdarstellung von EU-Bürgern: Behörden, welche für die Erfassung und Pflege von Personenstandsdaten verantwortlich sind, werden sich aufgrund des Rechts des Karteninhabers auf korrekte Namensschreibung, darauf einstellen müssen, die Personendaten mit den für die EU der 25 erforderlichen diakritischen Zeichen zu erfassen und zu speichern. Dies hat i.d.R. Auswirkungen auf Workstations und Datenbanken dieser Behörden. Auch der Speicherbedarf im Chip sowie der erforderliche Zeichenvorrat für die Chipkartenproduktion kann betroffen sein.

2 und nicht nur versicherten Personen

3 Elektronische Meldebestätigung

Rechtlicher Hinweis:

Ein Herunterladen des Dokuments ist ausschließlich zum persönlichen Gebrauch erlaubt. Jede Art der Weiterverbreitung oder Weiterverarbeitung ist untersagt. Freier Download (hier klicken)