Die Bürgerkarte: Basis und Infrastruktur für sicheres e-Government

Arno Hollosi[1] · Herbert Leitold[2] · Reinhard Posch[1, 2]

[1] Chief Information Office (CIO)
Stabsstelle IKT-Strategie des Bundes
Bundesministerium für öffentliche Leistung und Sport (BMÖLS)
Arno.Hollosi@cio.gv.at, Reinhard.Posch@cio.gv.at

[2] Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK), Technische Universität Graz
Herbert.Leitold@iaik.at, Reinhard.Posch@iaik.at

Zusammenfassung

Die österreichische Bürgerkarte stellt hinsichtlich der Umsetzung elektronischer Signaturen eines der engagiertesten Projekte des europäischen Raums dar, zumal eine flächendeckende Ausgabe signaturfähiger Chipkarten an alle österreichischen Bürger bereits im Sommer 2002 beginnen soll. In diesem Beitrag wird das Projekt Bürgerkarte vorgestellt. Dazu werden die Kernelemente der Bürgerkarte umrissen – diese sind die sichere elektronische Signatur welche die Anforderung der eigenhändigen Unterschrift und der Schriftlichkeit erfüllt, weitere Schlüsselpaare zur Authentifizierung oder Inhaltsverschlüsselung wie beispielsweise als Element sicherer Kommunikation im Internet, Berechtigungsnachweise, sowie individuelle Infoboxen als Datenspeicher.
Es wird das Konzept der Security-Kapsel zur technologieneutralen Einbindung der Chipkarte in unterschiedliche Umgebungen erläutert, die einerseits sicherheitsrelevante Elemente wie die vertrauenswürdige Anzeige integriert, zugleich auch die Kartenschnittstelle zu einer auf XML basierenden Anwendungsschnittstelle abstrahiert. Dabei ist insbesondere der Ansatz offener, technologieneutraler Schnittstellen hervorzuheben. Diese Sicherheitsschicht wird als Bindeglied zwischen der Applikation und der Karte einerseits den Anforderungen unterschiedlicher Anwendungen gerecht, wie denen des e-Government in einem *public private partnership*, wie sie andererseits auch unterschiedliche Ausprägungen der Bürgerkarte zulässt. Am Beispiel einfacher Applikationsszenarien werden wesentliche Elemente der Kommunikation des Bürgers mit der öffentlichen Verwaltung exemplarisch dargestellt.

1 Einleitung

Die österreichische Bundesregierung hat in der Regierungsklausur vom 20. November 2000 einstimmig den Einsatz von Chipkartentechnologie zur Vereinfachung der Amtsgeschäfte des Bürgers vereinbart. Diese Entscheidung stellt einen der wesentlichsten Impulse zur elektronischen öffentlichen Verwaltung dar – das e-Government. Die durch den Hauptverband der österreichischen Sozialversicherungen ausgeschriebene Sozialversicherungskarte wird in offener Weise und durch die Ergänzung mit elektronischen Signaturen als Schlüsselkarte – wie auch andere Karten die diesem Konzept folgen – zu einer Bürgerkarte. Diese elektronischen Signaturen werden die Anforderung der eigenhändigen Unterschrift entsprechend dem Signa-

turgesetz [SigG99], respektive gemäß Artikel 5.1 der EU Signaturdirektive [EURi99] erfüllen.

Es ist mit der Bürgerkarte eine infrastrukturelle Basis der Authentifizierung des Bürgers in der Kommunikation mit der Behörde geschaffen. In einer holistischen Betrachtungsweise der Geschäftsabläufe öffentlicher Verwaltung bedarf es jedoch weiterer Elemente, die sich sowohl über die Anwenderkomponente die direkt mit der Chipkarte kommuniziert, über den Bedarf an wohldefinierten Schnittstellen, über die Vielzahl an verwaltungsseitig zu bedeckenden Applikationen, als auch über die datenschutzrechtlichen Aspekte in der Einführung von Verfahrenskennungen definieren.

In diesem Beitrag werden diese Aspekte der Geschäftsabläufe elektronischer Verwaltung im Kontext der Bürgerkarte diskutiert. Dazu wird in Abschnitt 2 der legislative Rahmen im Sinne der EU Richtlinie [EURi99] zur elektronischen Signatur und des österreichischen Signaturgesetzes (SigG) [SigG99] sowie der Signaturverordnung [SigV00] skizziert. Dies wird in Abschnitt 3 um den technisch-infrastrukturellen Rahmen im Sinne der wesentlichen Kernelemente der Bürgerkarte erweitert. Es sind dies vor allem die technische Struktur der Karte, die Trennung der Funktionen und die Aufteilung der Ressourcen. In Abschnitt 4 wird das Konzept der Security-Kapsel diskutiert. Diese gewährleistet in technologieneutraler Weise die Ankopplung unterschiedlicher Applikationen an die Bürgerkarte über offene Schnittstellen. Abschließend werden in Abschnitt 5 in exemplarischer Weise Verfahrensszenarien erläutert. Dabei werden vor allem auch Verfahrenskennungen diskutiert, über die aus einer nicht rückführbaren Ableitung des eindeutigen Personen-Ordnungsbegriffes Anforderungen des Datenschutzes gewahrt bleiben.

2 Rechtlicher Rahmen

Die EU Richtlinie zur elektronischen Signatur [EURi99] bildet einen gemeinschaftlichen Rahmen zur rechtlichen Anerkennung elektronischer Signaturen sowie für Zertifizierungsdienste. Dabei definiert die Richtlinie für elektronische Signaturen, die bestimmten technischen Anforderungen genügen, in Artikel §5.1, dass diese:

a) die rechtlichen Anforderungen an eine Unterschrift in bezug auf in elektronischer Form vorliegende Daten in gleicher Weise erfüllen wie handschriftliche Unterschriften in bezug auf Daten, die auf Papier vorliegen, und

b) in Gerichtsverfahren als Beweismittel zugelassen sind.

Die technischen Rahmenbedingungen derartiger elektronischer Signaturen sind vor allem in den Anhängen der Richtlinie definiert. Vorraussetzung für die oben zitierte Äquivalenz zur handschriftlichen Unterschrift ist, dass die elektronische Signatur von einer sogenannten ‚sicheren Signaturerstellungseinheit' (Anhang III der Richtlinie) erstellt wurde und auf einem sogenannten ‚qualifizierten Zertifikat' (Anhang I und II der Richtlinie) beruht[1].

Die Anforderungen der Signaturdirektive sind in der Europäischen Union zur Zeit nahezu vollständig durch nationale Signaturgesetze umgesetzt. Im deutschen Sprachraum sind dies

[1] Das österreichische Signaturgesetz [SigG99] bezeichnet elektronische Signaturen, die von einer sicheren Signaturerstellungseinheit erzeugt werden und die auf einem qualifizierten Zertifikat beruhen als *sichere elektronische Signatur*. In diesem Beitrag wird deshalb in weiterer Folge der Begriff ‚sichere Signatur' verwendet. Der Begriff ist mit dem der *qualifizierten elektronischen Signatur* des deutschen SigG [SigG01] vergleichbar.

das deutsche Signaturgesetz [SigG01] und die deutsche Signaturverordnung [SigV01], sowie das österreichische Signaturgesetz [SigG99] und die österreichische Signaturverordnung.

In Anlehnung an zuvor obig zitierten Artikel §5.1 der EU Richtlinie definiert das österreichische Signaturgesetz für sichere Signaturen in [SigG99] §4 besondere Rechtswirkungen, wie folgt:

(1) *Eine sichere elektronische Signatur erfüllt das rechtliche Erfordernis einer eigenhändigen Unterschrift, insbesondere der Schriftlichkeit im Sinne des § 886 ABGB, sofern durch Gesetz oder Parteienvereinbarung nicht anderes bestimmt ist.* [2]

Anforderungen an die Schriftform sind insbesondere in den Bereichen der öffentlichen Verwaltung, wie beispielsweise im Zuge des Anbringens des Bürgers an die Behörde, gegeben. Die sichere elektronische Signatur entfaltet im öffentlichen Sektor somit ein immenses Potential in zweierlei Hinsicht: Zum einen bietet sich durch das Vermeiden von Medienbrüchen, wie sie schon im Übergang von Papierformularen zum meist bereits elektronisch unterstützten Backoffice entstehen, ein offensichtliches Rationalisierungspotential. Zum anderen ist eine Serviceverbesserung gegenüber dem Bürger alleine schon dadurch möglich, dass mit sicheren elektronischen Signaturen die Identität im Zuge der Ausstellung des qualifizierten Zertifikates a priori festgestellt ist, eine verfahrensimmanente Notwenigkeit der Feststellung der Identität somit auf diese zurückgreifen kann und somit das persönliche Erscheinen im Amt nicht zwingend erforderlich ist.

In Erweiterung der grundlegenden rechtlichen Rahmenbedingungen des [SigG99] gibt die Signaturverordnung [SigV00] auch technische Maßgaben, wobei jene, die im Kontext dieses Aufsatzes von Bedeutung sind, nachfolgend kurz skizziert werden.

Hinsichtlich der Verfahren werden die Schlüssellängen für sichere Signaturen beim Verfahren Rivest, Shamir Adleman (RSA) [RSAL98] oder Digital Signature Algorithm (DSA) [NIST00] mit mindestens 1023 Bit festgelegt – für DSA-Varianten, die auf elliptischen Kurven basieren, mit mindestens 160 Bit.

Die Signaturverordnung definiert des weiteren, dass technische Komponenten und Verfahren zu sicheren elektronischen Signaturen zu prüfen sind. Anwendbar sind hier beispielsweise die Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC) [EUni92] oder anerkannte Schutzprofile nach den Gemeinsamen Kriterien [ISO98]. Derartige zu prüfende Komponenten sind offensichtlich die sichere Signaturerstellungseinheit, wie es am Beispiel Bürgerkarte im folgenden Abschnitt diskutiert wird. Es unterliegen aber auch andere Komponenten, wie die der vertrauenswürdige Anzeige, Anforderungen der Prüfung, worauf in diesem Beitrag im Zuge der Security-Kapsel noch eingegangen wird.

3 Kernelemente der Bürgerkarte

Der Name Bürgerkarte ist ein Arbeitstitel für das Chipkartenprojekt der österreichischen Verwaltung. Es stellt dies eine Schlüsseltechnologie auf der Seite der Bürger und der Verwaltung bei der Nutzung von e-Government dar. In einem möglichst offenen und daher für die

[2] Für wenige bestimmte Rechtsgeschäfte, wie aus dem Familien- und Erbrecht oder für Bürgschaftserklärungen, entfaltet die sichere elektronische Signatur nach §4(2) [SigG99] nicht die Rechtswirkung der Schriftlichkeit. Auf diese Sonderfälle wird hier der Vollständigkeit halber zwar hingewiesen, in weiterer Folge werden diese im Beitrag jedoch nicht weiter behandelt.

weiteren Entwicklungen des hoch dynamischen Bereiches der e-Technologien geeigneten System ermöglicht die Bürgerkarte die notwendige Identifikation der Betroffenen. Transaktionen, die bislang nur durch persönliches Erscheinen oder mit Mitteln der Papiertechnologie (unterfertigte Formulare) möglich waren, können damit online durchgeführt werden.

Die initial als häufigst anzunehmende Ausprägung der Bürgerkarte basiert auf der Sozialversicherungskarte des Hauptverbandes – Projekttitel ELSY [ELSY99]. Dieses flächendeckende Chipkartenprojekt wird um die sichere elektronische Signatur entsprechend Signaturgesetz [SigG99] erweitert. Elliptische Kurven finden Anwendung, die bei einer Schlüssellänge von 160 Bit die Anforderungen der Signaturverordnung [SigV00] erfüllen, aber auch im europäischen Kontext als zukünftig für sichere Signaturen anerkannt zu erwarten sind [ALGO01].

Sowohl im Kontext dieses Beitrags, als auch im Verständnis einer Bürgerkarte als ein Konzept, das die Erledigung der Amtsgeschäfte des Bürgers online ermöglichen soll, ist die Bürgerkarte jedoch von der Sozialversicherungskarte entkoppelt anzusehen. Vielmehr ist eine Vielzahl an verschiedenen Ausprägungen denkbar und definiert, die sich durch unterschiedliche Anforderungen sowohl an den Chip, gegebenenfalls auch an die Oberfläche auszeichnen. Ein Überblick wird in der folgenden Tabelle 1 gegeben, in der nur einige Elemente der Oberfläche und des Chips zur Veranschaulichung dargestellt sind, wie mit den Ausprägungen Sozialversicherungskarte ELSY, Studentenkarte, Basiskarte und Personalausweis nur ein Ausschnitt möglicher Bürgerkarten gegeben wird. Für einen detaillierten Überblick wird auf das „Weißbuch Bürgerkarte“ verwiesen [PoLe01]

Tab. 1: Ausprägungen des Konzeptes Bürgerkarte

	SV-Karte ELSY	Studenten-karte	Basiskarte	Personal-ausweis
Oberfläche: SV-Nummer	erforderlich			
Oberfläche: Bild		optional/ sinnvoll		erforderlich
Oberfläche: Sicherheit, z.B. Lasergravur				erforderlich
Oberfläche: Ablaufdaten		erforderlich		erforderlich
Chip: SV-Record	erforderlich			
Chip: Signatur	optional/ sinnvoll	erforderlich	erforderlich	erforderlich
Chip: Berechtigungen		optional/ sinnvoll		
Chip: Daten		optional/ sinnvoll		optional/ sinnvoll

Die Bürgerkarte umfasst in obgenannter Ausprägung in Kombination mit der Sozialversicherungskarte drei wesentliche Bereiche, wie folgt:

1. Die Anwendung Krankenscheinersatz der Sozialversicherung: Diese verwendet symmetrische Kryptographie und bildet über die Sicherung über eine Gegenkarte (Ordinations-

karte) ein geschlossenes System, auf das in diesem Beitrag nicht weiter eingegangen wird.

2. Die sichere elektronische Signatur gemäß [SigG99] [SigV00] sowie weitere Schlüsselpaare für kryptographische Authentifizierung und Inhaltsverschlüsselung, um über die Infrastruktur Bürgerkarte auch in Breitenanwendungen wie im e-commerce oder im Internet sicherheitssteigernden Nutzen zu erreichen.
3. Die Bürgerkarte macht die restlichen Bereiche, die auf der Karte verfügbar sind, nutzbar. Aus der Sicht der elektronischen Signatur und der Zertifizierung sind dies fest vorgegebene Datenblöcke auf der Karte, die nicht mit der elektronischen Signatur in Interaktion treten, respektive keine weiteren Funktionen auf der Karte auslösen. Je nach Anwendung können auch Zugangsberechtigungen (Schlüssel) für diese Datenelemente in der Personalisierung eingerichtet werde.

Zur Veranschaulichung obig beschriebenen Szenarios wird in nachfolgender Abbildung 1 die Dateistruktur illustriert. Linker Hand sind die Bereiche der kryptographischen Schlüssel der sicheren elektronischen Signatur dargestellt, wie auch der weiteren Schlüssel wie der zur Inhaltsverschlüsselung. Die mittig dargestellte Applikation Krankenscheinersatz ist nur über eine Gegenkarte zugänglich, im Kontext gegenständlichen Aufsatzes ist diese nicht von vorrangigem Interesse. Die Infoboxen sind rechter Hand dargestellt.

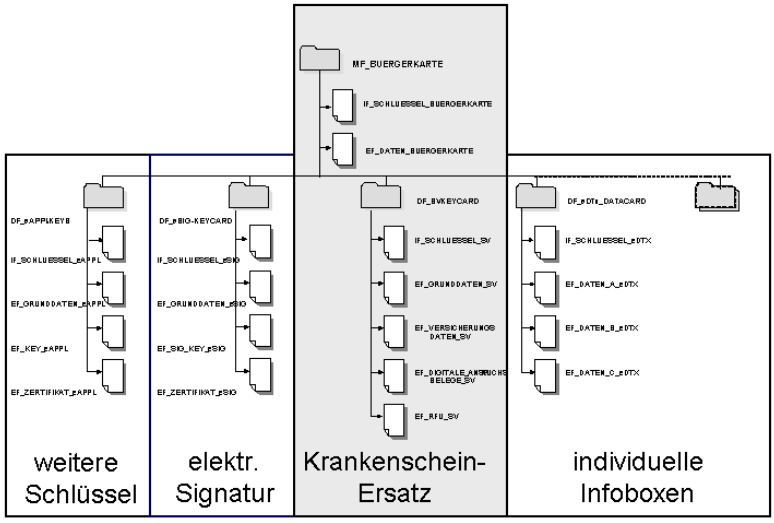

Abb. 1: Struktur der Bürgerkarte in Kombination mit der SV-Karte

Im e-Government ist vor allem die sichere Signatur als Authentifizierung des Bürgers von Bedeutung. Bereits im vorigen Abschnitt 2 wurde skizziert, dass die Rechtslage die dafür erforderliche Sicherheitsfunktionalität nicht einzig auf die sichere Signaturerstellungseinheit – die Signaturkarte – beschränkt. Es sind weitere Komponenten zu bedenken, wie die vertrauenswürdige Anzeige, wie auch unterschiedliche Applikationen zu erwarten sind. Dies wird anhand der Security-Kapsel im folgenden Abschnitt diskutiert.

4 Security-Kapsel

Die Security-Kapsel stellt eine abgeschlossene Einheit der Bürgerkartenfunktionen dar und kapselt in sich alle relevanten Funktionen für die Signatur (z.B. vertrauenswürdige Anzeige). Applikationen greifen nur über die Schnittstelle der Kapsel, den Security-Layer [HKP01], auf die Bürgerkarte zu. Für die Applikationen ist die zugrundeliegende Technologie transparent, welches größtmögliche Flexibilität und ein Maximum an Vorwärtskompatibilität gewährleistet.

Zusätzlich trennt das Konzept der Security-Kapsel klar die rechtliche Verantwortung nach Signaturgesetz. Dadurch, dass sich alle für eine sichere elektronische Signatur zu prüfenden und vom Zertifizierungsdiensteanbieter (ZDA) zu verantwortenden Komponenten (wie z.B. die PIN-Eingabe) innerhalb der Security-Kapsel befinden, sind aufrufende Applikationen von jedweden rechtlichen Anforderungen befreit und können ohne Abstimmung mit den ZDAs bzw. ohne Kenntnis der rechtlichen Details entwickelt und betrieben werden.

Weiters bietet die Security-Kapsel eine logische Sicht auf die Funktionen und Daten der Bürgerkarte. Die reale Implementierung, ob auf der Chipkarte, oder als Softwarekomponente innerhalb der Kapsel ist nach außen nicht sichtbar. Durch diese Abstrahierung kann die Security-Kapsel eine kohärente Sicht unterschiedlichster Hardware-Token bzw. unterschiedlich ausgeprägter Chipkarten nach außen bieten, Applikationen sind gegenüber diesen Details ignorant. Damit wird die Security-Kapsel zum integrierenden Element der Bürgerkartenfunktionen.

Durch Kapselung und Ansprache über eine TCP/IP Schnittstelle kann die Security-Kapsel an einer beliebigen Arbeitsstation oder auch in einer externen Einheit, wie einem Mobiltelefon oder einem Personal Digital Assistent (PDA) implementiert sein. Der Übergang zu einer Karte, wie über den Cryptographic Token Interface Standard [PKCS00], ist eine zweite, nach außen transparente Schnittstelle der Security-Kapsel.

Die Schnittstelle zur aufrufenden Anwendung, welche die Bürgerkartenfunktionen abstrahiert, wird Security-Layer genannt. Aus Gründen des einfachen Parsens mit Standardwerkzeugen erfolgt die Kodierung der Protokoll-Elemente in Extensible Markup Language (XML). Das Protokoll besteht aus einfachen Anfrage-/Antwort-Mustern. Anfragen werden von der Applikation in XML kodiert und über eine definierte TCP/IP-Verbindung an die Security-Kapsel übermittelt. Die Applikation erhält auf dem selbem Weg eine XML-kodierte Antwort. Für die Applikation stellt die Security-Kapsel eine Black Box dar, der einzig mögliche Zugang erfolgt über den Security-Layer. Das Szenario der wesentlichen Schnittstellen ist in folgender Abbildung 2 dargestellt.

Ein Beispiel für die Abstraktion der Bürgerkartenfunktion durch die Security-Kapsel ist das Signieren eines Dokuments mittels Cryptographic Message Syntax (CMS) [Hous99] oder XML-DSIG [ERSo01]. Die Applikation übermittelt lediglich das zu signierende Dokument und gibt die Art der Signatur (CMS oder XML-DSIG) vor. Die Security-Kapsel übernimmt die restlichen Funktionen und liefert das fertig signierte Dokument im gewünschten Format zurück. Damit ist die Applikation von den sicherheits- und rechtskritischen Aufgaben entkoppelt, was insbesondere in der Vielzahl der e-Government Anwendungen vorteilhaft ist. Die Security-Kapsel bietet auch die Signaturprüfung an und entlastet so Applikationen von Details der elektronischen Signatur im gesamten Lebenszyklus eines Dokuments.

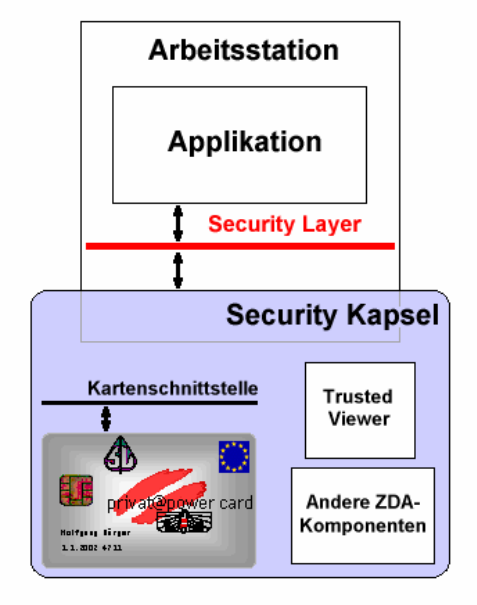

Abb. 2: Schnittstellen der Security-Kapsel

Da im Kontext des e-Government Kommunikation vor allem über das WorldWideWeb stattfindet, bietet die Security-Kapsel noch spezielle Protokollbindungen des Security-Layer, wie zum Beispiel die Hyper Text Transfer Protocol (HTTP)-Bindung. Diese Bindung erlaubt es, völlig ohne aktive Komponenten im Webbrowser auszukommen. Abbildung 3 zeigt den generellen Ablauf. Der Webbrowser übermittelt die Anfrage per HTTP-POST-Request an die Security-Kapsel (1), welche die Antwort entweder an den Webbrowser selbst, oder an eine in der Anfrage angegebene Universal Resouce Location (URL) sendet (2). Im letzteren Fall leitet die Security-Kapsel den Webbrowser per HTTP-Redirect (3) auf eine andere URL um.

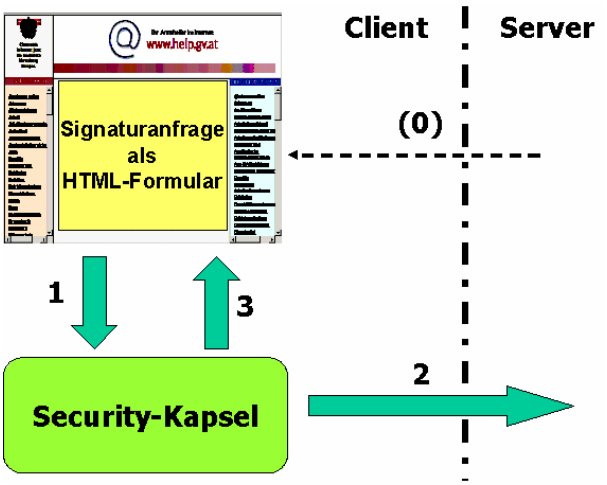

Abb. 3: HTTP-Bindung der Security-Kapsel (keine aktive Komponenten im Browser)

5 Anwendungsszenarien und Verfahrensablauf

In den betrachteten Anwendungsszenarien treten die Bürger über festgelegte Schnittstellen, insbesondere unter Einbeziehung der Security-Kapsel, typischerweise über Portale an die verschiedenen Anwendungen der Verwaltung heran, wobei sich der Hoheitsbereich der Verwaltung auf dessen unmittelbaren Kernbereich reduziert, dabei somit hinreichend Raum für privatwirtschaftliche Umsetzung und Lösungen lässt. Dieses Szenario ist in folgender Abbildung 4 skizziert,

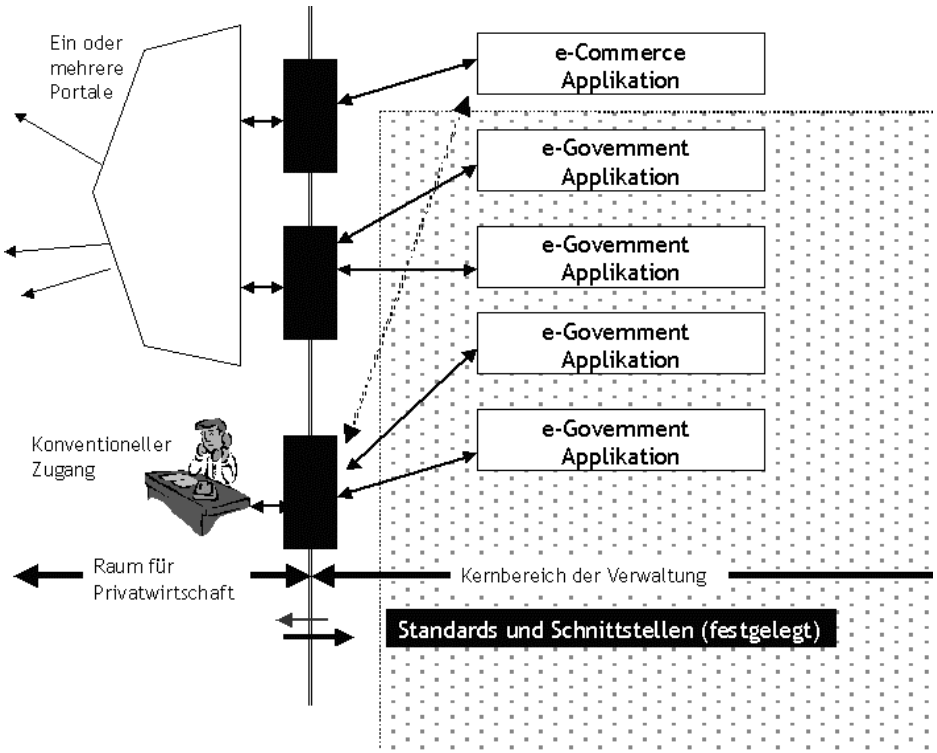

Abb. 4: e-Government im Wechselspiel Privatwirtschaft und Verwaltung

Die Offenheit bei der Heranführung ist Schlüssel der erfolgreichen Umsetzung von e-Government. Interaktion von Bürgerkarte, e-Government und das mögliche Zusammenspiel mit Portalen und Marktplätzen ist ein wesentliches Element der Gesamtstruktur. Mit der Technologie der elektronischen Signatur ist dabei ein beachtlicher Schritt in Richtung Komfort möglich und gleichzeitig kann der Datenschutz von Betroffenen dadurch erhöht werden. Dabei wird zwischen den verschiedenen Bereichen der Umsetzung klar unterschieden, um auch Unabhängigkeit und damit Weiterentwicklung sicherzustellen.

Wesentlicher Aspekt der Heranführung der Bürger an die Verwaltungsapplikation ist, dass die Authentifizierung der Bürger gegenüber der Verwaltung Ende-zu-Ende über die sichere elektronische Signatur im Rahmen der Verfahren erfolgt. Zusätzliche Elemente der Authentifizierung wie Single-Sign-On oder an den Portalen sind dabei nicht zwingend und somit im allgemeinen nicht erforderlich. Personalisierung der Portale selbst, wie beispielsweise für kontextabhängige Hilfefunktionen, kann jedoch für die Bürger wertsteigerndes Element sein. Im auch privatwirtschaftlichen Betrieb der Portale ist dies jedoch vom Verfahren und somit von der öffentlichen Verwaltung entkoppelt zu betrachten, zumal das Portal nicht in rechtliche Verantwortung eintreten wird.

Es ist ein wesentliches Ziel, Sicherheit und Datenschutz in den Verfahren zu garantieren, ohne dabei den Komfort zu vernachlässigen. Im Sinne des Datenschutzes sind Personen-Ordnungsbegriffe zum Ablegen und Wiederfinden in elektronischen Verfahren in der Verwaltung so zu gestalten, dass es nicht möglich ist, von Ordnungsbegriffen in einer Verfahrensgruppe auf Ordnungsbegriffe der gleichen Person in anderen Verfahrensgruppen zu schließen. Demgegenüber können während des Abwickelns eines Verfahrens die entsprechenden Zugänge dann sichergestellt werden, wenn die betroffene Person dies veranlasst.

Als Ausgangspunkt für die verfahrensabhängige Kennung dienen eindeutige, lebenskonstante, personenbezogene Ordnungsbegriffe, wie die Zahl des Zentralen Melderegisters (ZMR) für natürliche Personen oder das Zentrale Vereinsregister (ZVR) für Vereine als Beispiel einer juridischen Person. Dieser Ordnungsbegriff wird in weiterer Folge als Basisbegriff bezeichnet. Aus dem Basisbegriff lässt sich ein verfahrensbezogener und personenbezogener Ordnungsbegriff über Hashverfahren ermitteln, sodass sich der Zusammenhang zwischen unterschiedlichen Verfahren nicht ohne Kenntnis des Basisbegriffs herstellen lässt [Posc01]. Dies ist in folgender Abbildung 5 dargestellt.

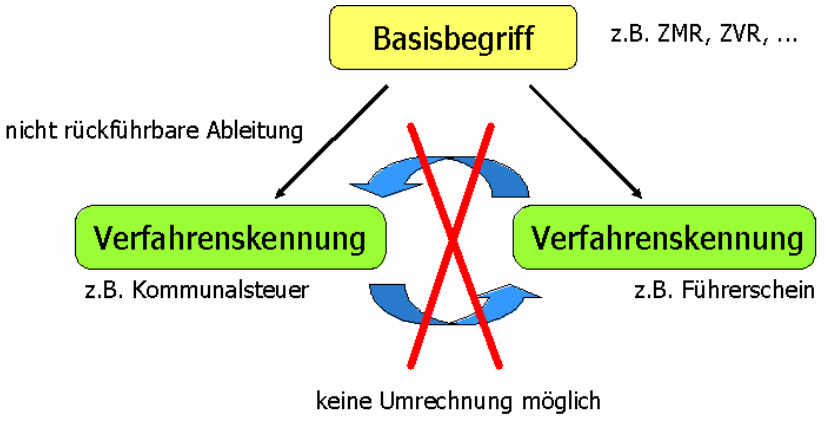

Abb. 5: Ableitung der nicht rückführbaren Verfahrenskennung

Das Verwaltungsreformgesetz 2001 [VRfG01] gibt dafür den rechtlichen Rahmen als dementsprechende Erweiterung des Verwaltungsverfahrensgesetzes vor (§4a des [VRfG01]):

> *Zum Zweck der eindeutigen Identifikation von Verfahrensbeteiligten im elektronischen Verkehr mit der Behörde darf diese die ZMR-Zahl (§ 16 Abs. 4 des Meldegesetzes 1991, BGBl. Nr. 9/1992) als Ausgangsbasis für eine verwaltungsbereichsspezifisch unterschiedliche, abgeleitete und verschlüsselte Personenkennzeichnung verwenden. [...] Die ZMR-Zahl darf von der Behörde anlässlich der elektronischen Identifikation nicht aufgezeichnet werden.*

Der Basisbegriff für die Verfahrenskennung wird in gesicherter Weise auf die Bürgerkarte aufgebracht und mit dieser in einen zwingenden Zusammenhang gebracht, sodass die Verwendung der gleichen Kennung durch Personen, die diese Karte nicht besitzen und aktiviert haben, technisch ausgeschlossen wird. Die Aktivierung der Chipkarte erfolgt im Rahmen der Registrierung der elektronischen Signatur bei einem Zertifizierungsdiensteanbieter. Dabei wird durch die Behörde die Zusammengehörigkeit der Schlüssel der Karte und des Basisbegriffes für die Verfahrenskennung bestätigt.

Um eine eineindeutige Beziehung zwischen Karte und Person herzustellen wird ein „Personenbindung“ genanntes Tuppel aus den öffentlichen Schlüsseln der Karte und dem Basisbegriff gebildet. Dies wird von der zuständigen Behörde signiert. Damit kann innerhalb eines Verfahrens die Person durch Beigabe der Personenbindung anhand ihrer elektronischen Unterschrift auf dem anzubringenden Dokument eindeutig von der Behörde identifiziert werden.

Abbildung 6 zeigt ein entsprechendes Szenario. In den Dokumentdaten wird die Verfahrenskennung der Person eingetragen und die Personenbindung beigegeben. Beim Eingang prüft die Behörde, ob Unterzeichner und Antragsteller dieselbe Person sind. Die Pfeile im Bild stellen den Prüfkreislauf dar. Wenn Übereinstimmung vorhanden ist, dann kann die Personenbindung verworfen werden, im Akt selbst wird nur das Dokument mit der Verfahrenskennung gespeichert.

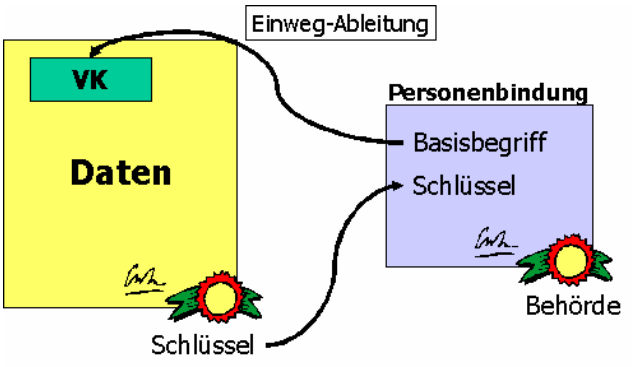

Abb. 6: Prüfung der Identität mit Verfahrenskennung und Personenbindung

Auf ähnliche Weise können (Vertretungs-)Vollmachten oder Attributzertifikate in das System eingefügt werden, ohne in elektronischen Akten dauerhaft gespeichert werden zu müssen.

Der Ablauf im Kontext eines elektronischen Antrages im e-Government stellt sich somit wie nachfolgend skizziert dar:

1. Die Person wendet sich an ein Portal und wird von dort mit den notwendigen Formularen bzw. mit Hilfestellung versorgt, um den Antrag auszufüllen. Dabei können auch notwendige Beilagen, wie z.B. die Zahlungsbestätigung für die Verfahrensgebühren dem Antrag beigelegt werden. Die Person signiert den Antrag und schickt ihn an die entsprechende Verfahrensapplikation der Behörde (das Portal kann auch im Sinne eines One-Stop-Shops diese Weiterleitung übernehmen). Der Antrag wird von der Einlaufapplikation des Amtes automatisch geprüft (Syntax, Struktur, Signatur, Vollmachten) und stellt eine Empfangsbestätigung aus. Zu diesem Zeitpunkt hat das Amt den Antrag rechtskräftig entgegengenommen und ein möglicher Fristenlauf beginnt.
2. Der Antrag wird in der Backoffice-Applikation des Verfahrens abgearbeitet. Dies wird in der Regel auch manuelle Schritte enthalten, bzw. kann auch organisationsübergreifend sein. Während dieser Zeit kann die Person mittels der Geschäftszahl (Zahl des Aktes), welche in der Empfangsbestätigung angeführt ist, bei der Einlaufstelle Auskunft über den Verfahrensstand erlangen. Sobald das Verfahren abgeschlossen ist, wird ein entsprechender Bescheid vom Amt ausgestellt und elektronisch signiert.
3. Dieser Bescheid wird an die gewünschte Adresse zugestellt. Im Falle einer elektronischen Zustellung findet eine Hinterlegung bei einem Zustellserver statt (eine weitere mögliche Portalfunktion). Im Sinne des Datenschutzes wird dieser Bescheid entspre-

chend verschlüsselt, um den Zustellserver auch von privatwirtschaftlichen Einrichtungen betreiben lassen zu können. Der Zustellserver übernimmt die Benachrichtigung der Person (z.B. per Email, SMS, ...) und sendet dem Amt bei erfolgter Zustellung (Person holt Bescheid ab) eine Abholbestätigung. Die Person kann die Echtheit des Bescheides (die Signatur) mittels der Security-Kapsel prüfen.

In allen Schritten dieses Verfahrens kommen vornehmlich XML-kodierte Daten, Dokumente und Schnittstellen zum Einsatz. Wo immer sinnvoll, wird ein standardisiertes Format verwendet. Hauptaugenmerk liegt dabei auf der Automatisierbarkeit, sowie Interoperabilität zwischen den verschiedenen Anwendungen und Applikationen. Neben der Strukturierbarkeit und dem Vorhandensein einer großen Auswahl an Standardtools, bietet XML den Vorteil mittels Stylesheets jederzeit in gängigen Webbrowsern für Anwender gut leserlich angezeigt werden zu können – für die Akzeptanz des e-Governments eine wesentliche Bedingung.

Conclusio

In diesem Beitrag wurde die österreichische Bürgerkarte als eine Sicherheitsinfrastruktur diskutiert, die über die bevorstehende Ausgabe an alle österreichischen Bürger insbesondere im Bereich des e-Government immense Potentiale zu entfalten in der Lage ist. Dies ist einerseits über ein Rationalisierungspotential offenbar, da über elektronische Geschäftsabläufe kostspielige Medienbrüche vermeidbar werden, gleichzeitig die Durchlaufzeiten wie etwa durch die Möglichkeit der parallelen Bearbeitung elektronischer Akte reduziert werden. Andererseits ist gegenüber dem Bürger eine Steigerung der Servicequalität schon über die Möglichkeit des Anbringens in elektronischer Form zu erzielen.

Es wurde erarbeitet, dass die Bürgerkarte, wenngleich über die Sozialversicherungskarte ELSY initial konkretisiert, nicht als eine einzige technische Realisierung anzusehen ist. Vielmehr ist sie ein Konzept der sicheren elektronischen Signatur in der öffentlichen Verwaltung, das in einer Vielzahl von Ausprägungen denkbar ist. Diesen unterschiedlichen bürgerseitigen Realisierungen stehen nicht weniger verschiedenartige verwaltungsseitige Anwendungen gegenüber. Mit der Security-Kapsel hat der Beitrag ein Konzept vorgestellt, das in technologieneutraler Art über offene Schnittstellen ein Bindeglied darstellt. In Kombination mit der Bürgerkarte selbst konzentriert die Secuirty-Kapsel die sicherheitsrelevanten Komponenten, zugleich wird damit erreicht, dass neue Ausprägungen der Bürgerkarte relativ einfach in bestehende Lösungen des e-Government einzuphasen sind.

Der Beitrag hat abschließend skizziert, wie die Konzepte elektronischer Verwaltung in einem public-private-partnership gegenwärtig umgesetzt werden. Es wurde dabei skizziert, wie über abgeleitete Verfahrenskennungen die Datenschutzaspekte dergestalt implementiert sind, dass der Bürger die Vorteile der eindeutigen Verfahrensidentifikation nutzen kann, wie über Abfrage des Verfahrensstandes, gleichzeitig aber eine automatisierte Verknüpfung unterschiedlicher Verfahren technisch ausgeschlossen bleibt.

Literatur

[ALGO01] EESSI Algorithmengruppe, Algorithms and Parameters for Secure Electronic Signatures, version 2.0, Oktober 2001.

[ELSY99] Allgemeines Sozialversicherungsgesetz, BGBl.Nr. 189/1955 zuletzt geändert durch BGBl. I Nr. 194/1999.

[ERSo01] Donald Eastlake, Joseph Reagle und David Solo: XML-Signature Syntax and Processing, W3C Candidate Recommendation, April 2001.

[EUni92] Europäische Union, Kriterien für die Bewertung von Systemen der Informationstechnik (ITSEC), hrsgg. v.d. Europäischen Union, 1992.

[EURi99] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen.

[HKP01] Arno Hollosi, Gregor Karlinger, Reinhard Posch: Security-Layer zur Bürgerkarte, November 2001.

[Hous99] Hously, R.: Cryptographic Message Syntax (CMS). IETF Request For Comment RFC 2630, Juni 1999.

[ISO98] International Standards Organisation, Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik - Common Criteria (CC) version 2.1, ISO15408, 1998.

[NIST00] National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication FIPS PUB 186-2, 01/2000.

[PKCS00] RSA Laboratories, PKCS #11 - Cryptographic Token Interface Standard, v.2.11, 2000.

[PoLe01] Reinhard Posch und Herbert Leitold: Weissbuch Bürgerkarte, Erstversion im Auftrag des Bundesministeriums für öffentliche Leistung und Sport, Juni 2001.

[Posc01] Reinhard Posch: Personenkennung – Kontrollierbare Identifikation, unveröffentlichter Entwurf – Fachbeirat Bürgerkarte, April 2001.

[RSAL98] RSA Laboratories, PKCS #1 v2.0: RSA Cryptography Standard, October 1998.

[SigG99] Österreich: Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG), BGBl. I Nr. 190/1999, BGBl. I Nr. 137/2000, BGBl. I Nr. 32/2001.

[SigG01] Deutschland: Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001, BGBl. I, S. 876; veröffentlicht am 21. Mai 2001.

[SigV00] Österreich: Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung - SigV), StF: BGBl. II Nr. 30/2000.

[SigV01] Deutschland: Verordnung zur elektronischen Signatur vom 16. Mai 2001, BGBl. I S. 3074, in Kraft seit 22. Mai 2001.

[VRfG01] Verwaltungsreform Gesetz, 2001.