Bürgerkarte – Infrastruktur für e-Government

Reinhard Posch

Technische Universität Graz
Inffeldgasse 16a
Reinhard.Posch@a-sit.at

Schlagworte: e-Government, Smartcard, Bürgerkarte, elektronische Signatur

Abstract: Der vorliegende Beitrag stellt die Chancen einer Bürgerkarte, die ein zentrales Element für die Umsetzung von e-Government bilden kann, dar. Dabei wird vor allem auf die Notwendigkeit von geeigneten Grundsätzen und Strukturen eingegangen, die eine neue und in vielen Bereichen effizientere Verwaltung leiten müssen, um für alle betroffenen Bürger vorteilhaft zu erschienen. Wesentlich ist auch, dass Privacy Enhanced Technologies wie Chipkarten in Kombination mit der elektronischen Signaturen ein geeignetes Werkzeug zur Verbesserung des Datenschutzes sein können, da weniger Daten zentral verwaltet werden müssen.

1. Die Bürgerkarte – das wesentliche Infrastrukturelement

Die österreichische Bürgerkarte[1] ist eine Chipkarte, die die sichere elektronische Signatur ermöglicht. Bislang sind Anbringen an die Verwaltung in den meisten Fällen an die Unterschrift des Betroffenen gekoppelt. Daher muss eine Infrastruktur, die e-Government erlaubt, an diesem Punkt ansetzen und eine gleichwertige Möglichkeit auch im elektronischen Fall eines Anbringens erlauben. Mit dem Signaturgesetz[2] und der sicheren elektronischen Signatur ist die gesetzliche Basis geschaffen, die mit ganz wenigen Ausnahmen diesen elektronischen Zugang ermöglicht.

Die Bürgerkarte baut auf der **Sozialversicherungskarte** auf, die in einer ersten Stufe die Anwendung des Krankenscheinersatzes umsetzt. Diese Sozialversicherungsanwendungen und alle Daten, die auf der Karte damit verbunden sind, sind an eine Gegenkarte (Ordinationskarte) gekop-

---

[1] Informationen zur Bürgerkarte sind unter http://www.buergerkarte.at im Internet verfügbar.

[2] *Ch. Brenn*; Signaturgesetz, Erläuterte Ausgabe Bundesgesetz BGBl I 1999/190 mit den Materialien und zusätzlichen Anmerkungen. Manz Verlag, Wien 1999.

pelt, und es stellt daher diese Sozialversicherungskarte eine besonders geeignete Basis dar, davon unabhängige Anwendungen auf dieser Karte umzusetzen, da ein Quergefährdung ausgeschlossen ist.

Über die sichere elektronische Signatur hinaus kann die Bürgerkarte auch weitere Datenelemente speichern. Diese Datenelemente sind nicht an den Inhaber der Sozialversicherungskarte gebunden, da diese von der gleichen Applikation nicht gesehen werden. Diese **Datenhandtaschen** stellen keine Notwendigkeit dar, da die Informationen auch online verfügbar sein könnten. Durch die Werkzeuge der elektronischen Signatur und gegebenenfalls der Inhaltsverschlüsselung wird aber eine besonders wirksame Methode geboten, einem Übermaß an Onlinedaten entgegenzusteuern. Die tatsächlichen Inhalte und der Umfang werden letztlich durch den Karteninhaber zu bestimmen sein. Z. B. „sperrt" der Benutzer eine Datenhandtasche auf und bringt elektronische Dokumente bei. Anstelle von Dokumenten kann der Bürger auch Ort und Ordnungsbegriffe für Dokumente in derartigen Datenhandtaschen mitführen – damit können die Dokumente an beliebigen Stellen je nach Vertrauen des Bürgers abgelegt sein. Ein zentrales Ablegen von Daten des Bürgers in Register kann dadurch verringert werden. Durch Datenhandtaschen kann der Komfort aber auch das Ausmaß des Datenschutzes gesteigert werden. Bürger, die es wollen, können diese Daten aber auch auf anderen Medien oder anderen Karten mitbringen. Transparenz für den Bürger und die Möglichkeit und das Recht des Bürgers, diese Datenhandtaschen zu löschen, sind dabei eine Voraussetzung.

Für das Konzept der Bürgerkarte sind aber auch die **Rollendefinitionen** von besonderer Bedeutung. Nur so kann man in einem offenen System e-Government umsetzen ohne laufend in Gefahr zu treten, dass das Gesamtsystem durch „Angriffe" auf die Daten und durch Fälschungsversuche unmöglich wird oder zumindest deutlich an Ansehen verliert. Methoden der Attributzertifikate und andere Methoden der IT-Sicherheit müssen eingesetzt werden, um e-Government umzusetzen. Attributzertifikate sind geeignet, Rollen technisch darzustellen (z.B. Leiter der Führerscheinstelle). Die Verwaltung sollte diese Attribute rasch umsetzen. Attributzertifikate oder Zeiger zu diesen können in Datenhandtaschen im Sinne von Identifikation und Berechtigung vorhanden sein.

2. e-Government benötigt neue Strukturen

Die Systeme der Verwaltung müssen für die Bürgerkarte und für das e-Government erst fit gemacht werden. Mailsysteme und EDV-Struktur

der Ämter sind erst an die Anforderungen des Signaturgesetzes anzupassen. Der elektronische Akt muss Signaturen durchgängig integrieren können und in dessen Workflow auch Signaturen ermöglich. Neben der Integration in den elektronischen Akt ist auch das Automatisieren der Schnittstellen notwendig.

Um den Anforderungen des Datenschutzes und der Verbraucherinteressen gerecht zu werden, sind in den gesamten Kommunikationslauf Methoden der **Vertraulichkeit** (Inhaltsverschlüsselung mit geeigneter Schlüssellänge) zu ermöglichen. Erst dadurch ist auch die Anforderung an einen transparenten Aktenlauf, den der Bürger jederzeit aus seiner Warte mitverfolgen kann, möglich und kann diese die Zufriedenheit der Betroffenen wesentlich steigern.

Zur Umsetzung der Methoden, die elektronische Verwaltung ermöglichen, müssen geeignete Randbedingungen eingehalten werden:

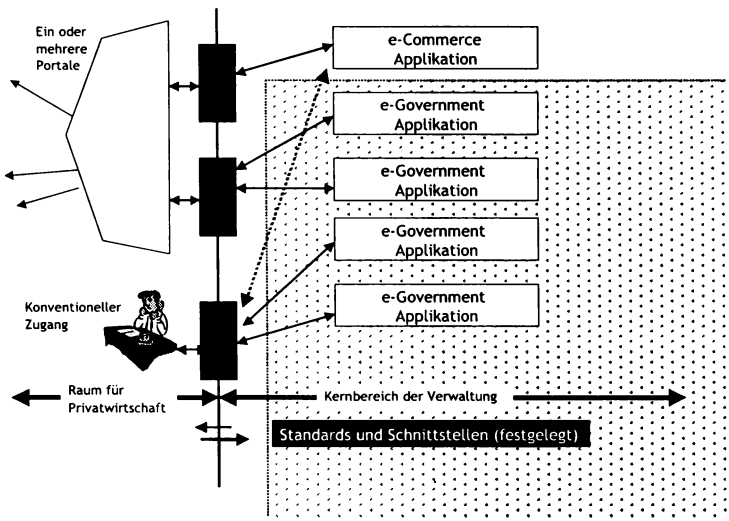
Überschaubarkeit für den Bürger: Da es sehr viele Betroffene gibt, kann man nicht davon ausgehen, dass der Bürger sich durch Schulungsmaßnahmen an das Konzept e-Government anpasst, sondern es muss dieses von sich heraus verständlich werden. Hilfestellungskonzepte können allenfalls zur „Schulung" beitragen.

Soziale Verträglichkeit: Nachteile können auch im Einzelfall für den Betroffenen nicht hingenommen werden. Schon wegen des Multiplikatoreffektes, der von benachteiligenden Situationen ausgeht, ist der Verlust an Komfort ein Kriterium das auch für jenen Personenkreis gelten muss, der sich dem Prinzip des e-Government aus seiner Warte verschließt.

Flexibles Universalkonzept: Ein wesentlicher Aspekt sind One-stop-Systeme, die beim Bürger den Eindruck erwecken, dass alle Verwaltungsaktivitäten von der ihm entgegentretenden „virtuellen Bürgerstelle" wahrgenommen werden. Dabei ist es belanglos, wie die Aufgaben im Backoffice verteilt sind. Es ist im Sinne einer positiven Konkurrenz auch wünschenswert, dass auf der Ebene der Bürger-Interfaces mittelfristig die Mechanismen der privatwirtschaftlichen Konkurrenz steuernd eingreifen.

Gewährleistung von Interoperabilität: Für den betroffenen Bürger existiert die Differenzierung zwischen den Verwaltungseinheiten nicht. Formulare, Bescheide, Urkunden etc. müssen kompatible Formate haben und bei allen Verwaltungsverfahren eingesetzt werden können. Der elektronische mit anderen Verwaltungsstellen kompatible Bescheid ist als Recht des betroffenen Bürgers zu sehen. Das Minimum dieser Kompatibilität stellt die Signatur dar, die durch die Bürgerkarte ermöglicht wird.

Sicherheit:[3] Authentizität der Kommunikationspartner, Garantien für den Schutz der Privatsphäre und Sicherheit und Schutz der Bürgerinteressen (Datenschutz, Datensicherheit) werden den Erfolg des Konzeptes e-Government wesentlich mitbestimmen. Dabei spielen die Mechanismen der Identifikation der Bürger, die auf ein Minimum zu reduzieren sind, und das Maß an Zentralismus bei der Datenhaltung, welches ebenfalls minimal sein sollte, eine wesentliche Rolle.



Es ist die zentrale Aufgabe der Politik, das Konzept e-Government glaubwürdig und effektiv an die Öffentlichkeit zu vermitteln. Politische Vorgaben müssen den Umfang, die Geschwindigkeit und die Einschränkungen prägen. Gehandelt werden muss jetzt, um mittelfristige Effekte zu erzielen. Dazu ist das Konzept der Bürgerkarte ein wesentlicher Beitrag. Wie in der obigen Skizze dargestellt, kann sich unter diesen Randbedingungen die Verwaltung auf den Kernbereich konzentrieren. Geeignete Schnittstellen können verschiedenste Zugänge ermöglichen und mittelfristig auch privatwirtschaftliche Heranführung an die Kernbereiche in offener Konkurrenz erlauben.

Diese privatwirtschaftliche offene Konkurrenz ist wesentlich, um die wirtschaftlichen Synergien mit den e-Technologien sicherzustellen.

---

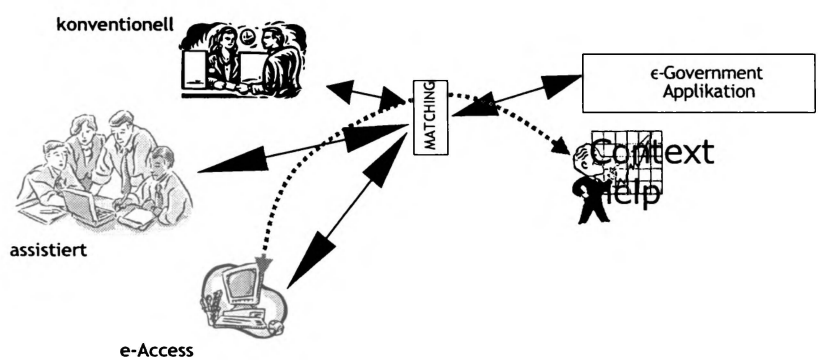
[3] *Ch. Brenn, R. Posch*; Signaturverordnung Erläuterte Ausgabe, Manz Verlag, Wien 2000.

3. Grundsätze müssen die Umsetzung leiten

Die rasante Entwicklung im Bereich der e-Technologien birgt auch viele Gefahren. Ein unüberlegtes Herangehen an diese Entwicklung und ein ausschließlich marktorientierter Zugang kann einen nachhaltigen Einsatz gefährden. Es ist daher von eminenter Bedeutung, dass die Umsetzung von e-Government auf generelle Grundsätze Rücksicht nimmt, um positiv aufgenommen zu werden und dauerhaft erfolgreich zu sein. Nur dann können die hohen Erwartungen in die Wirtschaftlichkeit und in den sparsamen Personaleinsätze durch elektronisch unterstützte Verwaltung auch umgesetzt werden.

- **Grundsatz der Freiwilligkeit:** Vor allem zu Beginn des Überganges wird es für eine beachtliche Zahl von Bürgern Emotionen oder Probleme geben, die neuen Technologien anzunehmen. Bürger, die es wollen oder die es nicht können, muss die Option des konventionellen Verwaltungszuganges offen stehen. Dabei ist es nur wichtig, dass das letzte Glied in der Anbringenskette für den Bürger konventionell aussieht. Im Kernbereich wird eine Diversifizierung nicht zu vertreten sein. Andererseits soll aber den Bürgern, die elektronisch an die Verwaltung herantreten, dies auch für die Bereiche angeboten werden, wo die Verwaltung selbst noch manuell durchgeführt wird.
- **Grundsatz des effizienten Einsatzes:** Es ist der volkswirtschaftliche, nicht der betriebswirtschaftliche Grundsatz zu beachten. Nur dann kann der große und erwartete Einsparungseffekt bei gleichzeitiger Komfortsteigerung erreicht werden.
- **Grundsätzlicher Anspruch:** Damit das gesamte System ein Erfolg sein kann, ist Interoperabilität zu erreichen. Damit muss aber der Bürger einen Anspruch auf elektronische Dokumente und Bescheide bekommen.
- **Grundsatz der IT-Sicherheit:** Datenschutz, Vertraulichkeit und Sicherheit ist in den elektronischen Vorgängen weder direkt sichtbar noch für den durchschnittlichen Teilnehmer am e-Government erfahrbar. Sicherheit und Vertraulichkeit darf sich dabei nicht auf die letzte Meile hin zum Bürger oder zum Unternehmer beschränken; Sicherheit muss auch in den internen Applikationen ein durchgehendes Prinzip sein.
- **Grundsatz der Transparenz:** Der Bürger muss das Recht haben, zu erfahren was, wann wo mit seinem Akt geschieht.

- **Grundsatz der vertikalen Durchlässigkeit:** Verwaltung findet auf mehreren Ebenen statt. Bund, Länder, Gemeinden und die Organe der Selbstverwaltung müssen Verwaltungsorganisationen schaffen, die für den Betroffenen ein kompatibles und durchlässiges e-Government ermöglichen.
- **Grundsatz der Offenheit:** Strukturen und Schnittstellen müssen allen die Teilnahme anbieten. Dies muss über die Staatsgrenzen hinaus der Fall sein, und Monopole, die weitere Entwicklung stark behindern, müssen durch offene Spezifikationen gänzlich vermieden werden. Gleichzeitig muss auch das einseitige Weiterentwikkeln und das Bilden von Vorreiterrollen in einzelnen Bereichen ermöglicht werden.
- **Grundsatz des Einsatzes privatwirtschaftliche Komponenten:** Wo immer dies strategisch zulässig ist, soll die Privatwirtschaft Möglichkeit der Konkurrenz haben. Dies ist vor allem in den weiteren zeitlichen Phasen und im Bereich der Heranführung wichtig.



Wie das obige Bild zeigt, werden die Zugänge über Portale und Marktplätze erfolgen. Auch wenn diese privatwirtschaftliche Konkurrenz einen Anreiz der Teilnahme bietet, sind die Heranführungsstrukturen der sensibelste Teil, weil er mit der großen Zahl an Benutzern in Kontakt tritt. Dies bedeutet aber, dass diese Heranführung durch Portale und Marktplätze besondere Randbedingungen erfüllen muss:

- **Information und Anbringen** müssen ohne weitere Identifikation am Portal möglich sein. Ein Anbringen benötigt in der Praxis lediglich die sichere elektronische Signatur, die bereits vollständig identifiziert.

- Eine **Interaktion** mit und ein transparentes Verfolgen der laufenden Verfahren benötigt Identifikation der Beziehung zwischen Benutzer und Verfahren. Diese sollte bewusst und transparent sein und muss von der Identifikation der Transaktion durch die elektronische Signatur unterschieden werden. Es wird dabei nicht ein Benutzer, sondern eine Beziehung zwischen einem Benutzer und gegebenenfalls einer Reihe von Verfahren identifiziert.
- Portale können bei dieser Beziehung zwischen Benutzer und Verfahren den Komfort erhöhen und die Klammer zwischen Bürger und Verwaltung bilden, doch ist die Session-Identifikation nicht geeignet, Anbringen zu authentifizieren. Der **Willensakt** muss final immer auf **elektronischer Signatur** basieren.
- Wichtig ist, dass ein Portal nur ein Minimum an Verantwortung übernimmt und auch technisch keine Manipulationsmöglichkeiten hat. Nur durch Einhalten dieser Bedingungen kann es gelingen, die Gesamtsituation für marktorientierte Konkurrenz offen zu halten.

4. Elektronische Signatur, Zertifizierung und Attribute als Basis

Die Basis der elektronischen Signatur benötigt eine Zertifizierungsinfrastruktur. Dafür wird im Signaturgesetz eine Basis gelegt, die ein weiteres zentrales Einschreiten nicht mehr nötig macht. Die Zertifizierungsdienste für die sichere elektronische Signatur auf der Bürgerkarte können aus den privatwirtschaftlichen Bereichen kommen.
Die wesentlichen Elemente der Zertifizierung sind:

- Zertifikatserstellung
- Verzeichnis- und Widerrufsdienste
- Signaturerstellungsgeräte und Schlüsselerzeugung
- Registrierung der Signatoren

Dazu käme dann noch das Erstellen, Warten und Widerrufen von Attributzertifikaten, die allerdings nach den Bedingungen der Richtlinie[4] über die elektronische Signatur nicht Zertifikate, sondern einfache elektronische Dokumente sind.[5]

---

[4] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl L 13/2000, 12.

[5] Dies ist auch dann der Fall, wenn Formate von Zertifikaten der Signatur verwendet werden.

Für den Bereich der Bürgerkarte wird durch die Ausgabe der Karte im Wege der Sozialversicherung der Zertifizierungsdienst wesentlich erleichtert, da die sicheren Signaturerstellungsgeräte bereits verteilt sein werden und damit eine wesentliche, die Kosten bestimmende Komponente bereits vorhanden sein wird.

In manchen Bereichen, wie etwa im studentischen Bereich, wird auch die Registrierung bereits durch die Ausgabe-Infrastruktur – in diesem Fall durch die Universitäten – besorgt werden können, sodass die Aufgaben der Zertifizierungsdiensteanbieter vor allem die automatisierbare Tätigkeit umspannt. Damit steht das Feld Zertifizierungsdiensteanbietern aller Größenordnungen offen.

5. Abschließende Bemerkungen

Die Bürgerkarte kann eine kritische Infrastruktur für das Umsetzen von e-Government und damit ein Aspekt der Erneuerung der Verwaltung sein. Dieses Einsetzen der e-Technologien in der Verwaltung muss wegen des monopolistischen Charakters vorsichtig geplant sein und muss wegen der Europäischen Komponente besonders auf Offenheit und Interoperabilität ausgerichtet sein. Mit Beginn der Umsetzung in Multiplikatorbereichen kann der Zugang sukzessive zu allen Bereichen erreicht werden und dadurch auch die Kompetenz der Betroffenen sowohl der Leistungserbringer wie auch der Bürger gesteigert werden. Mittelfristig wird dies zu einem Redesign der Verwaltungsabläufe führen, die die Transparenz der gesamten Verwaltung sicherstellen kann. Begleitende Öffentlichkeitsarbeit in der Einführungsphase und ständiges Monitoring des Umsetzens und des Einsatzes kann die notwendige Effizienz aber auch das geeignete Umsetzen der Datenschutz- und Verbraucheraspekte sicherstellen und muss von kompetenter politischer Arbeit begleitet sein.

Das Konzept Bürgerkarte bringt in dieses Szenario den Gedanken „IT-Sicherheit darf nicht das Privileg einiger Weniger bleiben“ ein.

Literatur

Brenn, C., Signaturgesetz, Erläuterte Ausgabe Bundesgesetz BGBl I 1999/190 mit den Materialien und zusätzlichen Anmerkungen. Manz Verlag, Wien 1999.

Brenn, C./Posch, R., Signaturverordnung Erläuterte Ausgabe, Manz Verlag, Wien 2000.

Bridwell, L.M./ Tippett, P., ICSA Labs 6th Annual Computer Virus Prevalence Survey, ICSA Labs, 2000.

Bureau of Export Administrations, Revisions to Encryption Items, US Department of Commerce, Federal Register Volume 65, Number 203, Page 62600-62610. Online resource http://www.bxa.doc.gov/Encryption, 2000.

Carnegie Mellon Software Engineering Institute, Computer Emergency Response Team Coordination Center, CERT® CC, online resource http://www.cert.org, 2001.

Dierks, T./Allen, C., The TLS Protocol Version 1.0, RFC 2246, 1999.

Internet Fraud Complaint Center, Six-Month Data Trend Report May-November 2000, National White Collar Crime Center and Federal Bureau of Investigation, 2000.

Jud, W./Högler-Pracher, R., Die Geichsetzung elektronischer Signaturen mit der eigenhändigen Unterschrift, ecolex 1999, 610.

Karlton, F. P./Kocher, P., The SSL 3.0 Protocol, Netscape Communications Corp., 1996.

Mastercard, Visa: SET Secure Electronic Transaction Specification, Book 1 – Book 3, Version 1.0, 1997.

Mitre Corporation, Common Vulnerabilities and Exposures – CVE, online resource http://www.mitre.org, 2001.

National Infrastructure Protection Center, Warning Not To Accept VeriSign Microsoft Digital Certificates dated January 29-30 2001, NIPC advisory 01-006, 2001.

NUA Internet Survey, Visa: Net Transactions Cause Credit Card Disputes, online resource http://www.nua.ie/surveys, article id 905356338, 1999.

S. Kent, S./Atkinson, R., Security Architecture for the Internet Protocol, RFC 2401, 1998.