Die Bürgerkarte - der digitale Personalausweis wird Realität in Europa

Robert Nitschke

IT Consultant
NOVOSEC AG
Sulzbacher Str. 29-39
65824 Schwalbach am Taunus
robert.nitschke@novosec.com

Abstract: Bürger können ebenso wie Unternehmen mit Hilfe der elektronischen Signatur ihren Geschäftsverkehr nicht nur sicherer gestalten, sondern auch deutlich vereinfachen. Signaturgesetze schaffen dabei die notwendigen Rahmenbedingungen. Während die Ausgabe von Signaturkarten in Deutschland derzeit noch verstärkt von der Industrie übernommen wird und der Staat sich eher zurückhält, sind andere europäische Länder in diesem Punkt viel aktiver. Mehrere Staaten wie beispielsweise Estland oder Finnland geben bereits elektronische Identitätskarten, sogenannte Bürgerkarten, an ihre Bevölkerung aus. Mit deren Hilfe werden nicht nur die Amtsgeschäfte der Bürger vereinfacht, auch nicht-staatliche Firmen können – analog zu dem herkömmlichen Personalausweis in der realen Welt – einen staatlichen Identitätsnachweis für ihre Geschäfte über das Internet verwenden. Dieser Ansatz „Ein Staat - eine Signaturkarte“ bietet die besten Voraussetzungen für eine flächendeckende Nutzung von elektronischen Signaturen. Sollte Deutschland seine abwartende Haltung bzgl. der Ausgabe von Bürgerkarten beibehalten, wird der Vorsprung des europäischen Auslandes gegenüber Deutschland größer.

Einleitung

Elektronische Signaturen bieten für Transaktionen im Internet überzeugende Vorteile; z. B. gewährleisten sie die Authentizität der Nachrichten. Behörden, Kreditinstitute, Unternehmen und auch Bürger können mit der elektronischen Signatur ihren Geschäftsverkehr nicht nur sicherer gestalten, sondern auch deutlich vereinfachen. Der Einsatz digitaler Zertifikate erlaubt auch die Überprüfung der Identität des Kommunikationspartners. Die Rechtswirksamkeit der elektronischen Signatur kann entweder durch vertragliche Regelungen innerhalb einer (globalen) Public Key Infrastruktur (PKI) oder durch Gesetze unter bestimmten Voraussetzungen erreicht werden.

Elektronische Signaturen

Eine elektronische Signatur muss folgende Eigenschaften erfüllen (vgl. [BSW95]):

- **Abschlusseigenschaft**: Sollte nach dem Signieren das Dokument verändert werden, passt die Signatur nicht mehr zu dem neuen Dokument. Die Signatur wird somit ungültig.
- **Echtheitseigenschaft**: Nur der Signierer kann die Unterschrift erstellen.
- **Nicht-Abstreitbarkeit**: Der Signierer kann später nicht behaupten, die Unterschrift nicht geleistet zu haben ("Non-repudiation"). Diese Eigenschaft ist eine sehr wichtige Voraussetzung für Verträge.
- **Verifikationseigenschaft**: Die Unterschrift kann von jedem überprüft werden.

Zur Erstellung der elektronischen Signatur werden asymmetrische kryptographische Verfahren verwendet. Als Basis dafür dienen Funktionen, die zwar auf der einen Seite effizient zu berechnen sind, deren Umkehrfunktionen auf der anderen Seite aber nur mit extrem hohem Aufwand zu berechnen sind. Ein Beispiel hierfür ist die diskrete Exponentialfunktion (vgl. [Sc96], [MOV96]):

> Bei gegebenen Zahlen P, d und x ist die Berechnung von $y = x^d \bmod P$ relativ leicht möglich (y ist der Rest bei der Division von x^d durch den *Modul* P, P ist eine Primzahl), die Berechnung von d bei Kenntnis von x , y und P ist jedoch im Allgemeinen sehr schwierig.

Bei den asymmetrischen Verfahren werden zwei unterschiedliche Schlüssel (privat, öffentlich) verwendet. Der private Schlüssel ist geheim zu halten und sollte demnach nur im Besitz einer einzelnen Person sein; der andere, öffentliche Schlüssel kann für alle anderen Teilnehmer in einem System frei zugänglich sein. Jeder Teilnehmer kann eine signierte Nachricht mit dem öffentlichen Schlüssel des Signierenden überprüfen (= verifizieren).

Weil das Signieren einer umfangreichen Nachricht sehr rechenintensiv sein kann, wird aus der zu signierenden Nachricht ein sogenannter Hash-Wert erzeugt. Dieser repräsentiert die ursprüngliche Nachricht wie z.B. ein Fingerabdruck einen bestimmten Menschen repräsentiert. Wendet man jetzt einen bekannten, asymmetrischen Algorithmus (RSA, DSA, Elliptic Curves, etc.) mit Hilfe des privaten Schlüssels des Senders auf den Hash-Wert an, erhält man einen signierten Hash-Wert. Die ursprüngliche Nachricht wird meistens zusammen mit diesem signierten Hash-Wert als Signatur an den Empfänger geschickt.

Zum Verifizieren der Signatur bildet der Empfänger ebenfalls den Hash-Wert der Nachricht und wendet den öffentlichen Schlüssel des Senders auf den (signierten) Hash-Wert an. Stimmen beide Ergebnisse überein, weiß der Empfänger, dass der Sender diese Nachricht erstellte und dass diese nicht (z.B. auf dem Transportweg) verfälscht wurde.

Digitale Zertifikate

Eine elektronische Signatur allein reicht allerdings nicht aus, die **Identität** des Signierenden zu überprüfen bzw. zu garantieren. Bei herkömmlichen Verträgen müssen sich die Unterzeichner ggf. mittels eines Personalausweises ausweisen. Diese Identität wird in elektronischen Medien mit digitalen Zertifikaten sichergestellt.

Zertifikate werden verwendet, um im Zusammenhang mit dem Versand von Dokumenten oder Transaktionen im Internet den Urheber bzw. Versender zweifelsfrei zu identifizieren. Mit Hilfe von Zertifikaten kann also überprüft werden, dass der Sender signierter Daten wirklich die Person ist, für die er sich ausgibt. Das Zertifikat selbst wird in der Regel von einer vertrauenswürdigen Instanz ausgegeben.

Ein Zertifikat ist als digitales Pendant zu einem Ausweis eine Datenstruktur, die sowohl den öffentlichen Schlüssel als auch die zur eindeutigen Identifikation (z.B. Name, Geburtsort und –datum) nötigen Informationen einer Person bzw. Entität beinhaltet. Diese Informationen hängen jeweils vom einzelnen Zertifikatstyp ab. Im Kontext von Web-Anwendungen wird oftmals zwischen Client- und Serverzertifikaten unterschieden. Clientzertifikate werden benutzt, um sich als Person oder System zu authentifizieren, wohingegen Serverzertifikate dazu dienen, eine Prüfung der Authentizität des Servers zu ermöglichen.

Einen ausführlicheren Überblick über elektronische Signaturen und Zertifikaten findet man bei [FGNR02a].

Signaturgesetze erzeugen rechtlichen Rahmen

Die meisten europäischen Länder haben in den letzten Jahren Gesetze bzgl. der elektronischen Signatur verabschiedet und erfüllen damit Anforderungen der EU-Richtlinie 1999/93/EC. So ist beispielsweise im Mai 2001 in Deutschland das "Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Formschriften" im Bundesgesetzblatt verkündet worden [D01]. Damit ist die Erwartung verbunden, dass die Nutzung der elektronischen Signatur in Deutschland an Bedeutung gewinnen wird. Eine weitere Maßnahme zur Popularisierung der elektronischen Signatur ist der Beschluss des Bundeskabinetts vom 16.01.2002 zur Ausstattung der Behörden mit der benötigten Hard- und Software. Elektronische Signaturen, genau genommen nur die qualifizierten elektronischen Signaturen [FGNR02a], sind jetzt in Deutschland rechtlich weitestgehend mit handschriftlichen Unterschriften gleichgestellt. Mit ihnen können – sofern gewisse Voraussetzungen wie z.B. eine hochwertige Registrierung erfüllt sind - Geschäftsabschlüsse via Internet sicherer und schneller abgewickelt werden.

Qualität der Registrierung

Eine entscheidende Frage lautet, wer die Identifikation der Kommunikationspartner vornimmt und wie die personenbezogenen Daten hinterlegt werden. Simple Anmeldeprozesse über das Internet können nur schwer bezüglich Falschangaben verifiziert werden.

Das Anbieten von Identifikationsdienstleistungen erfordert eine qualitativ hochwertige Kundenregistrierung sowie eine Reputation als vertrauenswürdige Instanz am Markt. Gerade Banken besitzen langjährige, enge Beziehungen zu ihren Kunden, die sich auf Grund der gesetzlichen Vorschriften entsprechend legitimiert haben. Daher weisen Banken auch ein hohes Potenzial auf, die Identifikation als Dienstleistung für Geschäftstransaktionen anzubieten.

Für die Übernahme des Identitätsnachweises bei einer initialen Registrierung könnten ggf. Gebühren erhoben werden. Das Modell ist vergleichbar mit dem PostIdent-Verfahren, auf das derzeit bei Kundenregistrierungen, die eine Überprüfung eines gültigen Ausweises benötigen, häufig zurückgegriffen wird.

Emission von Signaturkarten

Zur Nutzung der elektronischen Signatur werden verstärkt Signaturkarten ausgegeben. Als potentielle Emittenten können folgende Einrichtungen/Branchen agieren:

- Staat (mit seinen Behörden)
- Banken/Kreditkartenunternehmen
- Mobilfunknetzbetreiber
- Sonstige kartenausgebende Stellen (z.B. Mitarbeiterausweis, Kundenkarten)

Aufgrund der hohen Kosten für die benötigte Infrastruktur und Kundenregistrierung sind allerdings nur wenige finanzstarke Unternehmen in der Lage, Signaturkarten flächendeckend zu emittieren.

Bislang gibt es in Deutschland noch keinen Beschluss, Signaturkarten als Bürgerausweise analog zu dem bestehenden Personalausweis auszugeben. Signaturkarten werden in Deutschland derzeit noch stärker von den Banken als von den Behörden (z.B. Pilotprojekte in Bremerhaven, Passau und Ulm) emittiert.

Ganz anders sieht es da im Europäischen Ausland aus, wo Signaturkarten in erster Linie von den staatlichen Behörden flächendeckend an die Bürger ausgegeben werden. Diese Bürgerkarten lassen sich dann auch für die Dienstleistungen nicht-staatlicher Firmen nutzen.

Die staatliche Ausgabe von Signaturkarten schafft somit auch Firmen eine verbesserte Möglichkeit, ihre Geschäftsprozesse ins Internet zu übertragen.

Europäisches Ausland

Mehrere europäische Länder geben bereits heute Bürgerkarten aus bzw. haben die Emission angekündigt. Besonders weit sind dabei folgende Länder:

- Belgien
- Estland
- Finnland
- Italien
- Österreich
- Schweiz

Belgien

Am 2. April 2003 konnten die ersten Stadtverwaltungen mit der Ausgabe der elektronischen ID card beginnen. Die Bürgerkarte in Belgien soll den Bürgern Zugriff auf Dienstleistungen des Staates gewähren und die Kommunikation zwischen Bürger und Verwaltung fördern. Zukünftig sollen alle 589 Stadtverwaltungen Belgiens die ID card ausgeben [EI03]. Diese Karte ist fünf Jahre gültig und kostet derzeit € 10.

Estland

Am 28.01.2002 startete Estland mit der Ausgabe von Bürgerkarten („National ID cards“) [EE03a], [EE03b].

Abbildung 1: Bürgerkarte in Estland

Diese werden von dem „Estonian Citizenship and Migration Board“ ausgegeben. Die Karte entspricht den Anforderungen des Estischen Signaturgesetzes und ist für alle Bürger sowie ausländische Personen mit einem permanenten Aufenthalt in Estland Pflicht, sofern sie älter als 15 Jahre sind. Die Bürgerkarte kann über die Bankfilialen der Hansapank sowie der Ühispank beantragt werden.

Finnland

Seit Anfang 2000 werden in Finnland (über die Polizeiämter) elektronische ID cards ausgegeben [FIN03]. Diese Bürgerkarte ist auch ein offizielles Reisedokument für finnische Bürger bzw. Ausländer, die sich permanent in Finnland aufhalten, in 19 europäische Staaten.

Abbildung 2: Bürgerkarte in Finnland

Die Karte ist für drei Jahre gültig und kostet € 29,00. Sie enthält drei Zertifikate: eines zur Authentifizierung des Karteninhabers, ein weiteres zur Erstellung von nicht-abstreitbaren Signaturen und eines der ausstellenden Zertifizierungsstelle.

Derzeit kann man die Karte für den Zugriff auf Online-Banking und Versicherungsdienstleistungen, sowie für weitere Dienstleistungen, die von den regionalen Verwaltungen sowie der öffentlichen Administration angeboten werden, verwenden.

Im Juni 2004 soll die Bürgerkarte in Finnland - ähnlich wie in Österreich - mit der Sozialversicherungskarte kombiniert werden [EI03].

Italien

Im März 2001 wurde die erste italienische elektronische Bürgerkarte als vollwertiger Ersatz des bestehenden Personalausweises ausgegeben [I03].

Abbildung 3: Bürgerkarte in Italien

Zunächst werden die Karten in den 83 größten Städten Italiens emittiert.

Es wird erwartet, dass nach ca. fünf Jahren etwa 50 Millionen Italiener eine Bürgerkarte besitzen und u.a. für ihre Amtsgeschäfte verwenden.

Österreich

Die österreichische Regierung beschloss am 20. November 2000 den Einsatz von Chipkartentechnologien zur Vereinfachung der Amtsgeschäfte des Bürgers [A03]. Die Bürgerkarte ist dabei die vom Hauptverband der Sozialversicherungen ausgegebene Sozialversicherungskarte, die um die Möglichkeit, elektronische Signaturen zu erstellen, erweitert wird. Durch die Synergie zwischen Sozialversicherungskarte und Bürgerkarte ergeben sich vor allem in Bezug auf das Kartenmanagement erhebliche Einsparungspotenziale. Die österreichische Bürgerkarte ist derzeit freiwillig.

Es wird überlegt, auch einen neuen Personalausweis auf der Technologie der Bürgerkarte umzusetzen. Somit wären sowohl die Funktionen der Bürgerkarte für elektronische Transaktionen als auch die Funktionen eines konventionellen Ausweises auf einer Karte gebündelt.

Schweiz

Die Schweizer Regierung hat beschlossen, den elektronischen Personalausweis einzuführen [CH03]. Das Eidgenössische Justiz- und Polizeidepartement (EJPD) erarbeitet bis Ende 2003 ein Konzept und einen Gesetzesentwurf zur Einführung einer elektronischen Identitätskarte. Diese Bürgerkarte soll mithelfen, eine Reihe von vertraulichen und verbindlichen Online-Anwendungen im Bereich eGovernment und eCommerce in der Schweiz voranzutreiben.

Der elektronische Personalausweis soll dabei sowohl als konventionelle als auch als elektronische Identitätskarte eingesetzt werden können und rechtsverbindliches Signieren ermöglichen. Die Karte wird eine reine Identitätskarte sein. Weitere Informationen, wie zum Beispiel Gesundheitsdaten, sollen nicht auf der Karte gespeichert werden.

Marktpenetration

Des Öfteren wird gerade in Deutschland die Frage gestellt, ob sich die Ausgabe von Bürgerkarten lohnt und wie ggf. ein Return on Investment erzielt werden kann. Der Aufbau der entsprechenden Infrastruktur kostet schließlich Geld und kann in der Regel nicht durch den Verkauf der Signaturkarten an die Bürger refinanziert werden. Bürger werden nur dann freiwillig Bürgerkarten erwerben, wenn die Vorteile überwiegen und die Kosten überschaubar sind.

Anwendungen

Ein wichtiger Punkt, der auch bei einer flächendeckenden Ausgabe von Signaturkarten nicht außer Acht gelassen werden darf, sind die Anwendungen. Bereits heute werden in Deutschland bei mehreren Anwendungen elektronische Signaturen eingesetzt. In den kommenden Monaten und Jahren wird sich die Anzahl dieser Anwendungen deutlich erhöhen.

So werden im Rahmen der Initiative "BundOnline2005" in Deutschland die ersten Modellprojekte umgesetzt (ELSTER - die elektronische Steuererklärung, e-Vergabe, etc.); bis 2005 sollen nahezu 400 Dienstleistungen des Bundes online verfügbar sein. Zeitaufwändige Behördengänge könnten dadurch bald der Vergangenheit angehören. Mitarbeiter der Behörden können dabei anhand des E-Government-Handbuchs des BSI (siehe [FGNR02b]) entscheiden, ob für die jeweilige Dienstleistung elektronische Signaturen benötigt werden bzw. geeignet sind.

Andere Staaten sind ebenfalls bestrebt, staatliche Dienstleistungen zukünftig auch elektronisch anzubieten. Im Vergleich zu den anderen europäischen Staaten ist die Schweiz im Bereich der Nutzung der neuen Technologien für Anwendungen des Staates weit fortgeschritten: Viele Dienstleistungen auf Gemeinde-, Kantons- und Bundesebene sind mittlerweile per Internet abruf- und auch nutzbar. Darüber hinaus war es bei der letzten Volkszählung erstmals möglich, das ganze Verfahren "per Mausklick" abzuwickeln. Nach offiziellen Angaben haben vier Prozent der schweizerischen Bevölkerung davon Gebrauch gemacht.

Gesetzliche Bestimmungen

Es bleibt festzuhalten, dass eine Bürgerkarte auch analog zum herkömmlichen Ausweis verwendet werden kann. Sollte ein Staat wie beispielsweise Estland beschließen, den herkömmlichen Personalausweis bzw. Reisepass durch die Bürgerkarte komplett zu ersetzen, dann werden die Bürger dazu verpflichtet, anstelle des bisherigen Passes bzw. Ausweises zukünftig die Bürgerkarte zu bezahlen (auch wenn diese wie bei den herkömmlichen Ausweisen Eigentum des Staates bleibt). In diesem Fall muss allerdings sichergestellt werden, dass die Gültigkeit der Bürgerkarte in etwa der der Ausweise entspricht. Sollten Zertifikate nur ein Jahr gültig sein und müsste der Bürger dann Jahr für Jahr neue Karten kaufen bzw. neue Zertifikate beantragen und ggf. sogar selbst auf seine Karte einspielen, wird eine Zustimmung der Bevölkerung nur schwer zu erreichen sein.

Businessmodelle sind neben der Zertifikatsdauer auch verstärkt vom Volumen abhängig und müssten je Europäischem Staat einzeln berechnet werden. Es ist aber interessant, dass gerade Länder mit kleineren Bevölkerungszahlen vermehrt auf die Bürgerkarte als Identifikationsmedium setzen.

Fazit

Der Einsatz elektronischer Signaturen kann und wird den alltäglichen Geschäftsverkehr vereinfachen. Amtsgeschäfte lassen sich zukünftig einfach und bequem von zuhause aus erledigen. Auch wenn man in Deutschland diesen Eindruck nicht unmittelbar vermittelt bekommt: Die Bürgerkarte wird immer stärker in Europa eingesetzt. Länder wie Estland, Finnland und auch die Schweiz sind mit ihrem Ansatz „Ein Staat - eine Signaturkarte“ derzeit in diesem zukunftsweisenden Geschäftsfeld Deutschland einen guten Schritt voraus.

Nicht nur im Bereich eGovernment gibt es eine Vielzahl von Nutzungsmöglichkeiten von Bürgerkarten mit Chipkartentechnologie. Es ist daher davon auszugehen, dass die Bürgerkarte auch in Deutschland kommen wird, ansonsten würde sich der Vorsprung der genannten europäischen Länder gegenüber Deutschland nur weiter vergrößern.

Literaturverzeichnis

[A03] http://www.buergerkarte.at/

[BSW95] A. Beutelspacher, J. Schwenk, K. Wolfenstetter: Moderne Verfahren der Kryptographie, Vieweg, 1995, S. 16

[CH03] http://www.admin.ch/

[D01] Gesetz über die Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften; 16.05.2001; Bundesgesetzblatt Jahrgang 2001 Teil I Nr. 22, ausgegeben zu Bonn am 21.05.2001

[EE03a] http://www.pass.ee/

[EE03b] http://www.riso.ee/en/

[EI03] http://www.electronic-identity.org/

[FGNR02a] M. Fischlin, A. Giessler, R. Nitschke, H. Ritter: E-Government-Handbuch: Verschlüsselung und Signatur, http://www.bsi.bund.de/fachthem/egov/, 2002

[FGNR02b] M. Fischlin, A. Giessler, R. Nitschke, H. Ritter: E-Government-Handbuch: Authentisierung im E-Government, http://www.bsi.bund.de/fachthem/egov/, 2002

[FIN03] http://www.fineid.fi/

[I03] M. Gentili, Italian Electronic Identity Card – principle and architecture, Proceedings of the 27th VLDB Conference, Roma, Italy, 2001

[MOV96] A. Menenzes, P. van Oorschot, and S. Vanstone: Handbook of Applied Cryptography, CRC Press, 1996, S. 116

[Sc96] B. Schneier; Applied Cryptography, John Wiley & Sons, Inc., second edition, 1996, S. 496-498