Peter Gerstbach

Die österreichische Bürgerkarte

Wien, Dezember 2004

Kurzfassung

Mit dem Signaturgesetz aus dem Jahre 1999 sind sogenannte *sichere elektronische Signaturen* weitestgehend den eigenhändigen Unterschriften gleichgestellt und erfüllen damit das rechtliche Erfordernis der Schriftform. Neben der Signatur unterstützt die Bürgerkarte auch eine zweite wesentliche Anforderung: die Identifikation. Damit ist die Bürgerkarte das „amtliche Ausweisdokument“ in elektronischen Verwaltungsverfahren. Die Arbeit erklärt einführend die Grundlagen der Bürgerkarte, Anforderungen, die zu erfüllen sind, und konkrete Ausprägungen. In weiterer Folge werden die technischen Aspekte näher erläutert und die Rollen und Schnittstellen bei der Kommunikation zwischen Bürger und Verwaltung behandelt. Abschließend werden einige der im Internet bereits vorhandenen Anwendungen beschrieben.

Inhaltsverzeichnis

1 Einleitung und Problemstellung

Der fortschreitende Wandel vom Industrie- in das Informationszeitalter betrifft neben der Wirtschaft auch immer den öffentlichen Sektor. Der Staat verspricht sich durch den Einsatz von EDV kostengünstigere und schnellere Dienstleistungen, denn eine Verwaltung ohne Medienbrüche würde viele Verfahren effizienter und schneller durchführbar machen. Auf der Seite der Bürger bzw. der Unternehmen soll E-Government Behördenverfahren rund um die Uhr ermöglichen - und das einfacher sowie schneller.

Damit diese Möglichkeit vom Bürger auch angenommen wird, ist Sicherheit eine wichtige Voraussetzung. Die Bürgerkarte soll diese bieten: die Rechtssicherheit ist durch die sichere elektronische Signatur gegeben, die einer eigenhändigen Unterschrift gleichgestellt ist, Vertraulichkeit und Authentizität werden ebenfalls durch Funktionen der Bürgerkarte erfüllt. Die Bürgerkarte ist ein erweiterbares Konzept, das mit eigens dafür bestimmten Chipkarten, vorhandenen Chipkarten wie Bankomatkarten oder Dienstausweise und auch mit Geräten wie z.B. Handys funktioniert. So lange die festgelegten Voraussetzungen erfüllt werden, kann die Karte bzw. das Gerät als Bürgerkarte verwendet werden und somit die Rolle eines „elektronischen Ausweises“ übernehmen. Das Projekt wurde im November 2000 von der österreichischen Bundesregierung initiiert und hat sich seit dem stetig weiterentwickelt.

Diese Arbeit behandelt das Thema Bürgerkarte hauptsächlich von der technischen Seite. Im Kapitel 2 werden in einer allgemeinen Einführung zuerst die Grundlagen der Bürgerkarte behandelt. Es wird das Modell der beteiligten Interaktionspartner, die Anforderungen an die Bürgerkarte, deren Ausprägungen, der Lebenszyklus einer Karte und die Rolle der Bürgerkarte in der gesamten E-Government Strategie erklärt. Im Kapitel 3 wird näher auf die technischen Aspekte der Kommunikation zwischen dem Bürger und dem Staat eingegangen. Es wird der Ablauf einer E-Government-Sitzung erklärt und die Hardware- und Softwarevoraussetzungen an beiden Enden der Kommunikation besprochen, sowie die Definition der Schnittstellen (Benutzer-Schnittstelle und Security-Layer) zur Bürgerkarten-Umgebung erklärt. In einem praktischen Teil werden einige zur Zeit bereits vorhandene Anwendungen, die die Bürgerkarte einsetzen, erläutert (Kapitel 4). Den Abschluss der Arbeit bildet eine Zusammenfassung (Kapitel 5), in der auch die wesentlichen Stärken und Schwächen der Bürgerkarte deutlich gemacht werden.

2 Grundlagen der Bürgerkarte

2.1 Das Modell Bürgerkarte

Die *Bürgerkarte* ist keine physische *Karte* im eigentlichen Sinn, sondern ein Modell, das die sichere Abwicklung von E-Government und E-Commerce ermöglichen soll. Laut E-Government-Gesetz [E-G, Art. 1 §2 Z10] ist die Bürgerkarte

> *die unabhängig von der Umsetzung auf unterschiedlichen technischen Komponenten gebildete logische Einheit, die eine elektronische Signatur mit einer Personenbindung (§ 4 Abs. 2) und den zugehörigen Sicherheitsdaten und -funktionen sowie mit allenfalls vorhandenen Vollmachtsdaten verbindet.*

Das Modell der Bürgerkarte ist somit unabhängig von der technischen Umsetzung definiert und unterstützt u.a. folgende Funktionen:

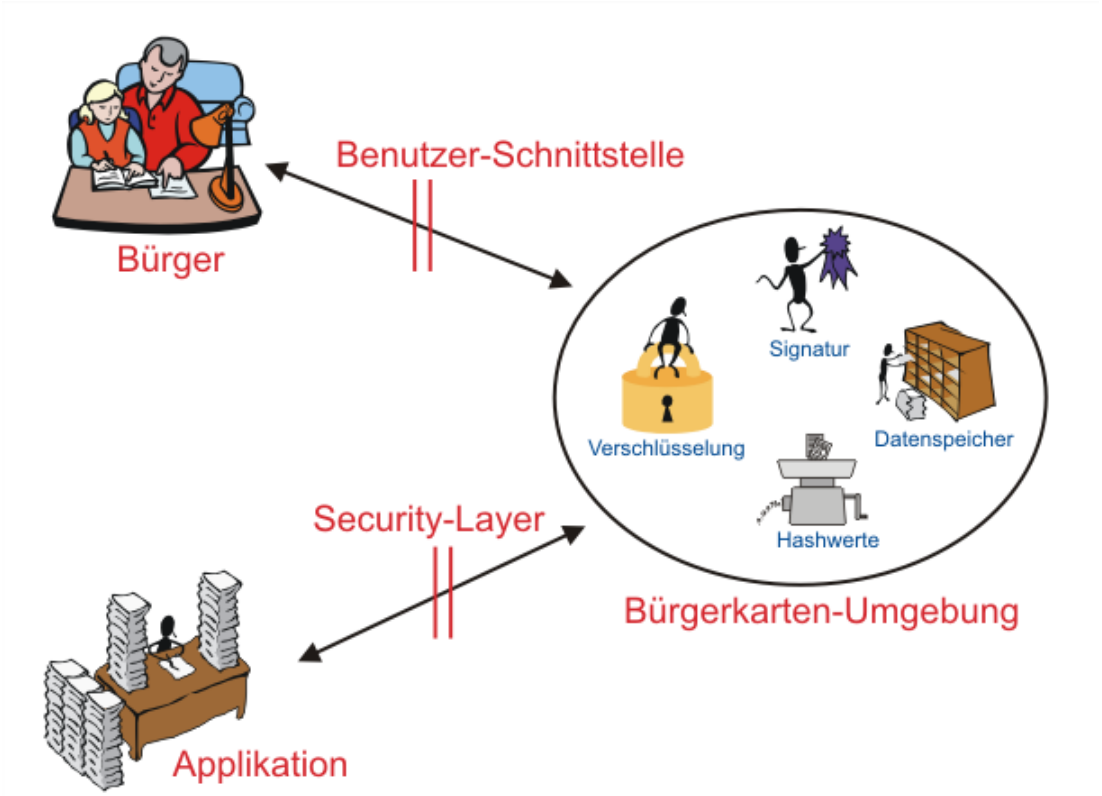
- elektronische Signatur
- Personenbindung
- Sicherheitsdaten und -funktionen
- Vollmachtsdaten

Abbildung 2.1 zeigt das Modell der Bürgerkarte mit den darin beteiligten Rollen und Schnittstellen. Die *Applikation* ist eine E-Government- oder E-Commerce-Anwendung, wie z.B. FINANZ*Online*, ein Zustelldienst oder Netbanking. Damit der Bürger auf das Service zugreifen kann, benötigt er eine *Bürgerkarten-Umgebung*. Dies ist ein Programm, das lokal am Rechner des Bürgers läuft (in diesem Fall spricht man von einer *lokalen Bürgerkarten-Umgebung*), oder ein serverbasierter Dienst (*serverbasierte Bürgerkarten-Umgebung*). Zwei Schnittstellen spezifizieren die Interaktion mit der Bürgerkarten-Umgebung: die Kommunikation zwischen Bürger und Bürgerkarten-Umgebung wird durch die Benutzer-Schnittstelle bestimmt, jene zwischen Applikation und Bürgerkarten-Umgebung regelt der Security-Layer. Die Benutzer-Schnittstelle bietet Funktionen zur Abwicklung von Befehlen an (z.B. die Anzeige der Daten zum Signieren) und ermöglicht die Konfiguration der Bürgerkarten-Umgebung. Der Security-Layer spezifiziert das Protokoll, das bei der Kommunikation verwendet wird, und die Bindung an Transportschichten wie HTTP oder TCP.

2.2 Anforderungen an die Bürgerkarte

Eine Umsetzung des Modells Bürgerkarte muss rechtlich und technisch folgende Anforderungen erfüllen [P+02]:

Abbildung 2.1: Das Modell der Bürgerkarte [HK04]



- Sichere elektronische Signatur (Abschnitt 2.2.1)
- Personenbindung (Abschnitt 2.2.2)
- Inhaltsverschlüsselung (Abschnitt 2.2.3)
- Infoboxen (Abschnitt 2.2.4)
- Security-Layer (Abschnitt 2.2.5)

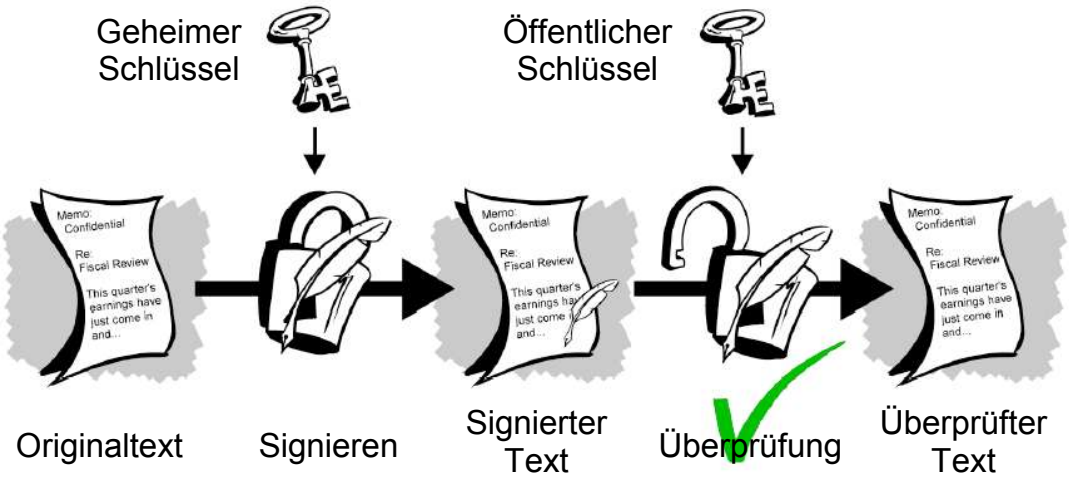
2.2.1 Sichere elektronische Signatur

Um in E-Government und E-Commerce eine sichere Kommunikation zu ermöglichen, wird die elektronische Signatur und Verschlüsselung eingesetzt. Rechtliche Grundlage dafür ist das Signaturgesetz [Sig], das im Jahr 1999 geschaffen wurde. Demnach ist eine *sichere elektronische Signatur* in fast allen Bereichen einer eigenhändigen Unterschrift gleichgestellt [Sig, §4 Z1]. Die technische Grundlage für die elektronische Signatur sind die Public-Key-Kryptographie, ein sicheres Hash-Verfahren und Zertifikate.

Public-Key-Kryptographie, auch asymmetrische Kryptographie genannt, ist ein relativ neues Gebiet der Kryptographie und wurde in den 70er Jahren entwickelt. Bei dem Verfahren werden zwei verschiedene Schlüssel zur Ver- und Ent-

schlüsselung verwendet. Der öffentliche Schlüssel (*Public Key*) wird zum Verschlüsseln und der geheime Schlüssel (*Private Key*) zum Entschlüsseln der Nachricht verwendet. Bei der *symmetrischen Verschlüsselung*, wo nur ein Schlüssel existiert, muss dieser Schlüssel sicher vom Sender zum Empfänger übertragen werden, was jedoch über das Internet nicht möglich ist. Der öffentliche Schlüssel im Public-Key Verfahren kann jedoch publiziert werden, da man mit ihm nur Daten verschlüsseln kann. Eine weitere Besonderheit der Public-Key-Kryptographie ist, dass das Verfahren auch in der umgekehrten Richtung angewendet werden kann: eine mit dem geheimen Schlüssel verschlüsselte Nachricht kann mit dem öffentlichen Schlüssel entschlüsselt werden. Dies wird bei der elektronischen Signatur angewendet: von der zu signierenden Nachricht wird ein Hash-Wert gebildet, dieser Hash-Wert wird mit dem geheimen Schlüssel verschlüsselt, was einer Signatur gleich kommt. Denn nur derjenige, der den geheimen Schlüssel kennt, kann die Nachricht signieren. Jedoch kann jeder mit Hilfe des öffentlichen Schlüssels die Authentizität und Integrität der Nachricht überprüfen [Wik04a].

Abbildung 2.2: Vorgang des Signierens (nach [NA00, Seite 20])



Für die Bürgerkarte ist demnach ein wesentliches Sicherheitsmerkmal die geschützte Speicherung des geheimen Schlüssels. In einer lokalen Bürgerkarten-Umgebung wird der geheime Schlüssel mitsamt der *Signaturerstellungseinheit* auf einer Chipkarte mit Krypto-Prozessor untergebracht. In einer serverbasierten Bürgerkarten-Umgebung wird der geheime Schlüssel beim Dienstanbieter sicher verwahrt. In beiden Fällen sorgt eine Kombination aus *Wissen und Besitz* dafür, dass nur der tatsächliche Eigentümer der Bürgerkarte Zugriff auf den geheimen Schlüssel hat. Bei der Bürgerkarten-Lösung der A-Trust ist die Chipkarte die Besitzkomponente und der PIN-Code die Wissenskomponente, bei der Lösung des österreichischen Mobiltelefonbetreibers Mobilkom Austria (A1) übernimmt das Handy (Besitz) und der Handy-PIN-Code (Wissen) diese erforderlichen Komponenten.

Hash-Wert. Da das Public-Key-Verfahren mathematisch sehr aufwändig ist und eine angehängte Signatur die Gesamtlänge der Nachricht nicht stark erhöhen

soll, wird ein sogenanntes *Hash-Verfahren* eingesetzt. Dieses ist ein nicht umkehrbarer Algorithmus, der eine umfangreiche Quellmenge auf eine wesentlich kleinere Zielmenge abbildet. Bereits kleine Veränderungen am Quelldokument führen zu völlig verschieden Hash-Werten. Das wiederholte Berechnen des Hash-Werts führt jedoch immer wieder zum selben Ergebnis [Wik04b].

Üblicherweise signiert der Sender einer Nachricht nun nur noch den viel kleineren Hash-Wert der Nachricht (dies kann bei der Bürgerkarte am Krypto-Prozessor der Chipkarte durchgeführt werden). Der Empfänger berechnet ebenfalls den Hash-Wert der Nachricht und vergleicht ihn mit der Signatur. Dadurch kann eine nachträgliche Änderung des Dokuments erkannt werden.

Zertifikate. Das dritte Element der Bürgerkarte bilden *qualifizierte Zertifikate*. Dadurch können die kryptographischen Schlüssel an die Identität des Signators gebunden werden. Eine *Authentifizierungsstelle*, die von der staatlichen Aufsichtsstelle bescheinigt wurde, prüft anhand eines amtlichen Lichtbildausweises die Identität des Bürgers und signiert dessen öffentlichen Schlüssel, dadurch entsteht das Zertifikat. Da der öffentliche Schlüssel der Authentifizierungsstelle bekannt ist und das Zertifikat damit überprüft werden kann, ist nun eine sichere Kommunikation mit jedem Bürger, der ein Zertifikat besitzt, möglich.

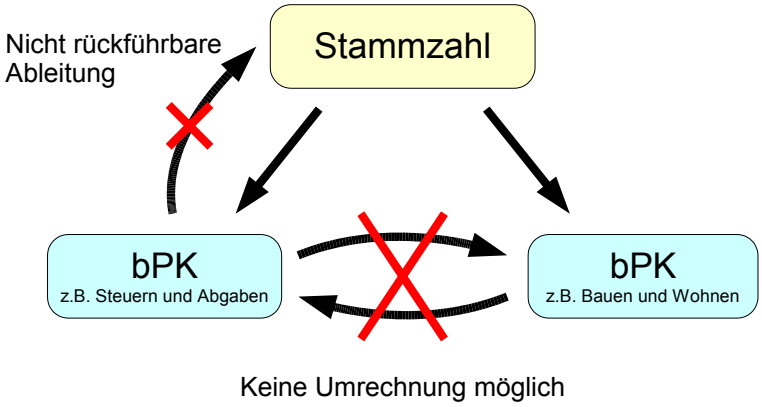
2.2.2 Personenbindung

Für die meisten Verfahren mit Behörden ist die eindeutige Identifikation des Bürgers eine Voraussetzung. Die zuvor besprochenen Zertifikate reichen jedoch alleine nicht aus, um eine Person eindeutig zu identifizieren. Denn meistens wird auf einem Zertifikat nur der Name der Person gespeichert, nicht jedoch zusätzliche Daten, die diese Person eindeutig identifizieren. Selbst zusätzliche Angaben von Geburtsdatum oder -ort würden nicht ausreichen, um in jedem Fall Eindeutigkeit herzustellen. Deswegen wird im Zentralen Melderegister (ZMR) allen in Österreich gemeldeten Menschen eine *Melderegisterzahl* (ZMR-Zahl) zugewiesen, über die eine eindeutige Identifikation möglich ist. Da die ZMR-Zahl, ähnlich wie die Sozialversicherungszahl, eine schützenswerte Information ist, wird durch den geheimen Schlüssel der Stammzahlenregisterbehörde aus der ZMR-Zahl die *Stammzahl* abgeleitet (siehe Abbildung 2.3). Die Stammzahl ist ebenfalls eindeutig für jede Person und wird auf der Bürgerkarte gespeichert.

Aus Datenschutzgründen wird bei einem elektronischen Verfahren jedoch nicht diese Stammzahl verwendet, sondern wieder eine abgeleitete Zahl, das *bereichsspezifische Personenkennzeichen* (bPK). Diese in Abhängigkeit des Anwendungsbereichs gebildet Zahl verhindert beispielsweise, dass eine behördenübergreifende Rasterfahndung durchgeführt werden kann. Die bPK für den Bereich Steuern und Abgaben unterscheidet sich z.B. von der bPK für den Bereich Bauen und Wohnen. Der verwendete Algorithmus stellt sicher, dass ein bPK nicht in ein anderes bPK umgerechnet werden kann. Ebenfalls kann aus einem bPK nicht die zugrundeliegende Stammzahl berechnet werden (siehe Abbildung 2.3) [Bun04c].

Abbildung 2.3: Von der ZMR-Zahl zur Stammzahl (nach [Bun04c])

Abbildung 2.4: Stammzahl und bPK (nach [Bun04c])



2.2.3 Inhaltsverschlüsselung

Neben der Authentizität einer Nachricht (also die Unverfälschtheit, erreicht durch digitale Signatur) ist die Vertraulichkeit ein weiteres Anliegen bei der Kommunikation zwischen Bürger und Verwaltung. Im Absatz über Public-Key-Kryptographie (Abschnitt 2.2.1 auf Seite 3) wurde bereits erläutert, wie mit dem geheimen Schlüssel eine Nachricht verschlüsselt werden kann. Der Gesetzgeber verlangt jedoch, dass Schlüssel, die zur Erzeugung von *sicheren elektronischen Signaturen* verwendet werden, nicht im Rahmen anderer kryptographischer Prozesse benutzt werden dürfen. Deswegen wird auf einer Bürgerkarte noch ein weiterer geheimer Schlüssel gespeichert, der in anderen Anwendungen, z.B. beim Signieren einer E-Mail, verwendet werden kann. Dieser zweite Schlüssel ist jedoch ebenfalls in der Personenbindung enthalten, wodurch eine eindeutige Schlüsselzuordnung möglich ist.

2.2.4 Infoboxen

In sogenannten Infoboxen können weitere Daten logisch strukturiert gespeichert werden. Solche Daten können beispielsweise Vollmachten oder andere Daten sein, die bei bestimmten Verwaltungsvorgängen vom Bürger beigelegt werden müssen. In der Bürgerkarte selbst muss so ein Speicher existieren, weiters ist es möglich, Infoboxen auch außerhalb der Bürgerkarte zu speichern. Die Speicherung auf der Bürgerkarte hat den Vorteil, dass die Daten unabhängig vom Verwendungsort immer verfügbar sind. Andererseits kann beispielsweise eine Chipkarte nur eine geringe Datenmenge speichern. Bei der externen Speicherung entfällt diese Einschränkung, dafür sind die Daten nicht mobil; Vertraulichkeit ist in beiden Fällen durch Verschlüsselung gewährleistet. Die in den vorigen Abschnitten vorgestellten Zertifikate und Personenbindungen werden ebenfalls in Infoboxen gespeichert.

2.2.5 Security-Layer

Das *Modell Bürgerkarte* ist ein offenes Konzept und bedingt die Definition einer Schnittstelle, über die Applikationen auf die Funktionalität der Bürgerkarte zugreifen können. Dadurch ist das Modell technologieunabhängig und zukunftssicher. Eine Bürgerkarten-Umgebung kann sowohl für unterschiedliche Computer-Plattformen entwickelt werden, sowie für beliebige andere Geräte, wie Handys oder PDAs. Der Abschnitt 3.2.4 auf Seite 17 beschreibt die Spezifikation des Security-Layers im Detail.

2.3 Ausprägungen der Bürgerkarte

Wie schon im Abschnitt 2.1 auf Seite 2 erwähnt, sieht das *Modell Bürgerkarte* ausdrücklich keine bestimmte Karte oder keinen bestimmten Kartentyp vor. Die Festlegung auf ein Modell und nicht auf eine bestimmte Karte bringt folgende Vorteile, die zu einer schnellen Verbreitung der Bürgerkarte führen sollen:

- Technologieunabhängigkeit: sowohl in Bezug zu dem verwendeten Gerät (*Token*) als auch in Bezug auf die Software
- Die Ausgabe der Bürgerkarten kann im Rahmen von Public-Private-Partnerships erfolgen
- Die Verwendung der Bürgerkarte wird nicht nur für die Kommunikation zwischen Bürger und Verwaltung möglich sein, sondern auch im privaten und privatwirtschaftlichen Kontext

Bisher existieren schon einige unterschiedliche Produkte auf dem Markt, die Bürgerkartenfähigkeit besitzen:

- **Bürgerkarte der A-Trust**: die Firma A-Trust bietet als akkreditierter Zertifizierungsdiensteanbieter seit Februar 2002 qualifizierte Zertifikate für sichere elektronische Signaturen an. Das Signaturkartenprodukt *a.sign premium* vereint e-Commerce Fähigkeit mit der Bürgerkarten-Funktionalität.

- **OCG Mitgliedskarte**: im Rahmen eines Pilotprojekts vergibt die Österreichische Computergesellschaft (OCG) seit Ende 2002 Mitgliedskarten mit Signatur- und Bürgerkartenfunktion an ihre Mitglieder. Die Karte ist technisch ident mit der Bürgerkarte *a.sign premium* von A-Trust. Abbildung 2.5 zeigt eine solche Karte.

- **maestro-Karte**: seit Herbst 2004 tauschen österreichische Banken die Bankomatkarten ihrer Kunden in bürgerkartenfähige Karten um. Es sind jedoch bei der Auslieferung keine Zertifikate auf den Karten vorhanden, um diese zu erstellen, muss der Kunde sich bei der Bank legitimieren. Mit der Bankomatkarte wird die Bürgerkarte erstmals einem breiten Publikum zu geringen Kosten zugänglich.

- **WU Studierendenausweis**: die Wirtschaftsuniversität vergibt seit 2000 Studierendenausweise im Chipkartenformat. Im Rahmen eines e-Voting-Projekts für die Bundespräsidentschaftswahl im April 2004 wurden die Studierendenausweise um Signatur- und Bürgerkartenfunktionialität erweitert [Kri04].

- **A1 Signatur**: der Mobilfunkbetreiber Mobilkom Austria bietet mit der *A1 Signatur* einen serverbasierten Dienst für die *Verwaltungssignatur* an. Anders als bei den kartenbasierten Lösungen wird bei der A1 Signatur nach dem Ausfüllen des Formulars ein nur einmal verwendbarer und zeitlich beschränkter SMS-Code an den Handybesitzer geschickt. Durch die korrekte Eingabe eines zusätzlichen PINs und dem SMS-Code wird die Signatur automatisch durchgeführt. Der Unterschied zwischen sicherer Signatur und Verwaltungssignatur wird in Abschnitt 2.5.1 behandelt.

- **e-Card**: die e-card ist eine Chipkarte, die den Krankenschein ablösen wird. Sie ist ebenfalls für die elektronische Signatur vorbereitet und kann dadurch auch als Bürgerkarte verwendet werden. Die e-card wird voraussichtlich im Laufe des Jahres 2005 an alle Versicherten und deren Angehörige ausgegeben.

Abbildung 2.5: Die OCG-Karte und die e-Card

Verbreitung Laut A-Trust waren Ende November 2004 ca. 16.000 Stück chipbasierte Bürgerkarten im Umlauf. In der Zählung enthalten sind die Karten, die von A-Trust selbst ausgegeben wurden und auch jene, die im Rahmen von Pilotprojekten (z.B: WU Studierendenausweis und OCG-Mitgliedskarte) ausgegeben wurde. Mit der flächendeckenden Einführung der signaturfähigen maestro-Karte

und der e-Card im Jahr 2005 wird diese Zahl vermutlich stark ansteigen. Daten über die Verbreitung der A1 Signatur liegen leider nicht vor, da eine entsprechende Anfrage an die Mobilkom Austria unbeantwortet blieb.

2.4 Lebenszyklus der Bürgerkarte

Dieses Kapitel beschreibt den Lebenszyklus einer Bürgerkarte, von der Herstellung über die Personalisierung und Verwendung bis zur Deaktivierung.

Bei einer Chip-basierten Bürgerkarte enthält die erste Phase die Herstellung und Vorbereitung des Chips und der Chipkarte. Der Chip und seine Software wird entworfen, produziert und die Karte wird für ihr Einsatzgebiet vorbereitet. Bei einer serverbasierten Bürgerkarte wird analog dazu eine Server-Infrastruktur eingesetzt, die ähnliche Funktionen und Sicherheitsanforderungen erfüllt.

Die Phase der Personalisierung ist von höchster Bedeutung, dabei werden alle Daten, die einer Person zugeordnet, sind auf die Bürgerkarte aufgebracht. Der geheime Schlüssel wird im Falle einer lokalen Bürgerkarten-Umgebung auf der Chipkarte bzw. bei einer serverbasierten Bürgerkarten-Umgebung auf dem Server gespeichert. Dadurch ist der Schlüssel vor fremdem Zugriff sicher. Der Bürger kann nun bei einem *Zertifizierungsdiensteanbieter* (ZDA) seiner Wahl ein *qualifiziertes Zertifikat* anfordern, das seinen öffentlichen Schlüssel mit den persönlichen Daten verknüpft. Die Signaturkarte wird vom ZDA nur dann an den Bürger persönlich übergeben, nachdem dieser seine Identität laut vorgelegtem, gültigem, amtlichem Lichtbildausweis bestätigt hat.

Für die Verwendung als Bürgerkarte ist die Personenbindung (siehe Abschnitt 2.2.2) für viele Applikationen erforderlich. Die Personenbindung wird in Form der eindeutigen, aus der ZMR-Zahl abgeleiteten, Stammzahl auf der Karte gespeichert. Der ZDA A-Trust ermöglicht diese Speicherung beispielsweise durch ein Online-Verfahren, das auf das Zentrale Melderegister zugreift.

Um die Sicherheit von Zertifikaten zu erhöhen, wird für diese eine begrenzte Gültigkeitsdauer festgelegt. Üblicherweise beträgt diese Gültigkeitsdauer drei Jahre. Nach Ablauf dieser Zeit muss ein neues Zertifikat beantragt werden. Um missbräuchliche Verwendung der Bürgerkarte (z.B. nach Diebstahl) zu verhindern, ist es zusätzlich möglich, das Zertifikat schon vor Ende der Gültigkeitsdauer zu sperren. Dafür speichert der Zertifizierungsdiensteanbieter im Rahmen des *Verzeichnis- und Widerrufsdienstes* zu allen ausgegebenen Zertifikaten ein Attribut, das angibt, ob das Zertifikat noch gültig ist. Jede Anwendung, die eine Signatur prüft, kann nun diese so genannten *Sperrlisten* (CRLs, *Certificate Revocation Lists*) über das Internet abrufen und somit feststellen, ob das Zertifikat zum aktuellen Zeitpunkt noch gültig ist.

2.5 Rolle im E-Gov-Konzept

Seit dem Jahr 2000 wird in Österreich mit besonderem Einsatz an der Entwicklung von E-Government gearbeitet. Im Jahr 2001 wurde das IKT-Board (Informations- und Kommunikationstechnik) eingerichtet, das u.a. die Aufgabe hat, Aktivitäten im Bereich E-Government, die mehr als ein Bundesministerium

betreffen, zu koordinieren. 2003 wurde die E-Government Plattform und das E-Cooperation Board gegründet, um IKT-Board, Länder, Gemeinden, Städte und die Wirtschaft gut in den Prozess zu integrieren.

Die im Jahr 2003 gestartete E-Government-Offensive soll die zielgerichtete und dynamische Entwicklung von E-Government weiter fördern. Eines der wesentlichen Ziele lautet:

> *Alle BürgerInnen und Unternehmen müssen sämtliche Verfahren der öffentlichen Verwaltung einfach und rasch ohne besondere Kenntnisse von Zuständigkeiten und ohne technisches Spezialwissen elektronisch ausführen können* [Bun04b].

Die E-Government-Strategie gliedert sich in zwei Teile. Teil I (*Online Verfahren*) beschreibt Rahmenbedingungen, Zielsetzungen und Umsetzung der Heranführung der Bürger an die Bundesverwaltung; Teil II (*Methoden und Verfahren in der Verwaltung*) regelt die Methoden und Verfahren, die innerhalb der Bundesverwaltung anzuwenden sind (z.B. der elektronische Akt).

Der Bürgerkarte nimmt dabei, als Schnittstelle zwischen Bürger und Verwaltung, eine wichtige Rolle ein. Der nächste Abschnitt über die Verwaltungssignatur (Abschnitt 2.5.1) beschreibt den Versuch die elektronische Signatur zu vereinfachen und damit schneller zu verbreiten. Der Abschnitt 2.5.2 behandelt die Richtlinie für einheitliche Formulare und die Amtssignatur. Gezeigt wird, wie damit der Wiedererkennungswert von behördlichen Schreiben auf die digitale Welt übertragen wird.

2.5.1 Sichere Signatur versus Verwaltungssignatur

Seit der erstmaligen Verabschiedung des Signaturgesetzes im Jahre 1999 sind einige Jahre vergangen, in denen sich Signaturen mit Chipkarte kaum durchgesetzt haben, obwohl die entsprechende Technik dafür schon lange existiert. Ein Grund kann bei den relativ hohen Einstiegshürden liegen. Es werden Chipkarte, Software und Lesegerät benötigt, die korrekt installiert und für den Bürger einfach zu bedienen sein müssen. Für den Markt entsteht durch diese Hürden eine geringe Absatzmöglichkeit für sichere elektronische Signaturen. Um die elektronische Signatur schneller zu verbreiten, wurde deswegen im E-Government-Gesetz [E-G, §25(1)] die *Verwaltungssignatur* geschaffen:

> *Im Rahmen der Bürgerkartenfunktion dürfen bis zum 31. Dezember 2007 gleichgestellt mit sicheren Signaturen auch Verwaltungssignaturen verwendet werden. Verwaltungssignaturen [... müssen nicht] allen Bedingungen der Erzeugung und Speicherung von Signaturerstellungsdaten der sicheren Signatur genügen und nicht notwendigerweise auf einem qualifizierten Zertifikat beruhen.*

Die Verwaltungssignatur verringert die Einstiegshürden ohne bei den eingesetzten Verfahren und Algorithmen Abstriche zu machen. Erleichterte organisatorische Rahmenbedingungen, wie z.B. die Verwahrung des geheimen Schlüssels,

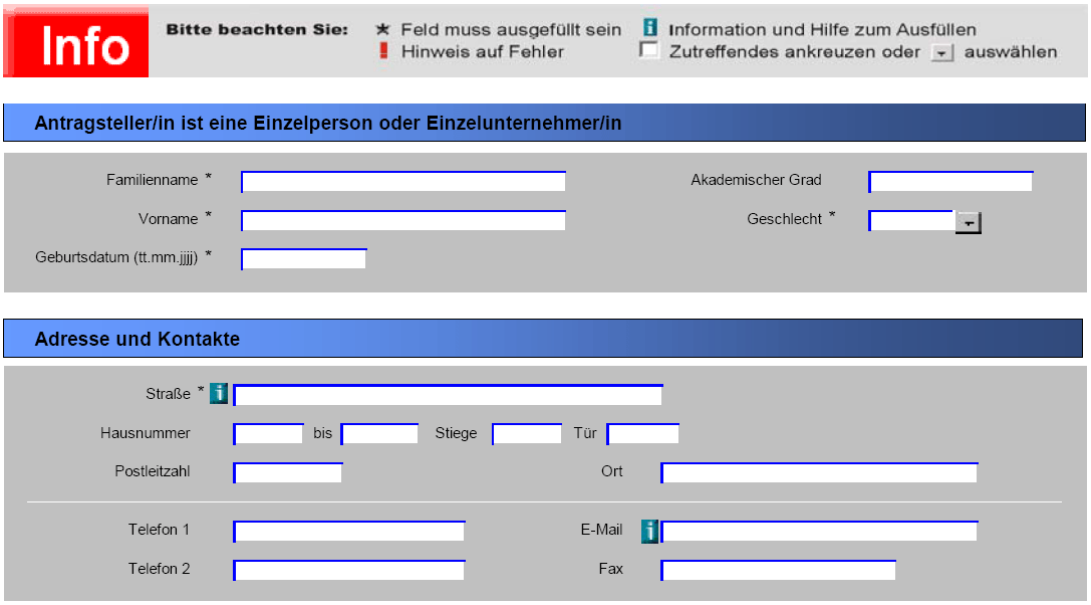
ermöglichen erst alternative Lösungen [Bun04a], wie sie z.B. von dem Handybetreiber Mobilkom Austria mit der A1-Signatur angeboten werden. Bei der Verwaltungssignatur ist jedoch auch sichergestellt, dass das Zertifikat eindeutig einer Person zugeordnet und das Auslösen der Signatur an Besitz und Wissen gebunden ist.

2.5.2 Einheitliche Formulare und Amtssignatur

Durch E-Government werden herkömmliche Verfahren elektronisch abgewickelt. Neben bisherigen Anforderungen ist man auch bestrebt, neu enstehende Anforderungen zu erfüllen. Beispielsweise werden Bescheide derzeit meistens nicht unterschrieben und oft ist die Herkunft nicht erkennbar. Beides trifft z.B. auf den Einkommensteuerbescheid zu. Einheitliche Formulare und die Amtssignatur sollen den Wiedererkennungswert von Formularen und Bescheiden erhöhen.

Einheitliche Formulare Der *Styleguide für E-Formulare* stellt die Grundlage für ein weitestgehend einheitliches Layout von E-Government-Anträgen dar. Im Styleguide wird die Gliederung, der Aufbau der Formularbausteine, Schriften, Linien, Farben und grafische Elemente definiert. Durch die Verwendung werden die technischen Möglichkeiten ausgenützt, der Wiedererkennungswert erhöht und die Verwendung für den Bürger vereinfacht. Abbildung 2.6 zeigt ein mögliches Formular, das dem Styleguide entspricht.

Abbildung 2.6: Formular nach dem Styleguide [MW04]



Amtssignatur Das E-Governmentgesetzt [E-G, §19f] regelt die *Amtssignatur*, eine Besonderheit der elektronischen Aktenführung. Die Überprüfung von digitalen Signaturen wurde bereits in Abschnitt 2.2.1 erklärt. Sie ist einfach durchzuführen, solange die Daten digital vorliegen. Bei einem Ausdruck eines digitalen

Bescheids geht diese Möglichkeit jedoch vorerst verloren. Durch den Einsatz der sogenannten Amtssignatur wird dieses Manko behoben. Abbildung 2.7 zeigt eine solche Amtssignatur. Die Bildmarke im linken oberen Eck identifiziert eine bestimmte Behörde, die Felder enthalten den Namen und die Funktion des Signators, Datum und Uhrzeit, Angaben zum Zertifikatsaussteller, eine eindeutige ID der Dokumentklasse, die Signatur und einen Hinweis auf die Rückführbarkeit in die originale elektronische Form. Diese Rückführung des ausgedruckten Bescheides in die elektronische Form kann dann beispielsweise vor Gericht durch einen Sachverständigen durchgeführt werden.

Abbildung 2.7: Amtssignatur

3 Technische Aspekte der Bürgerkarte

3.1 Ablauf einer E-Government-Sitzung

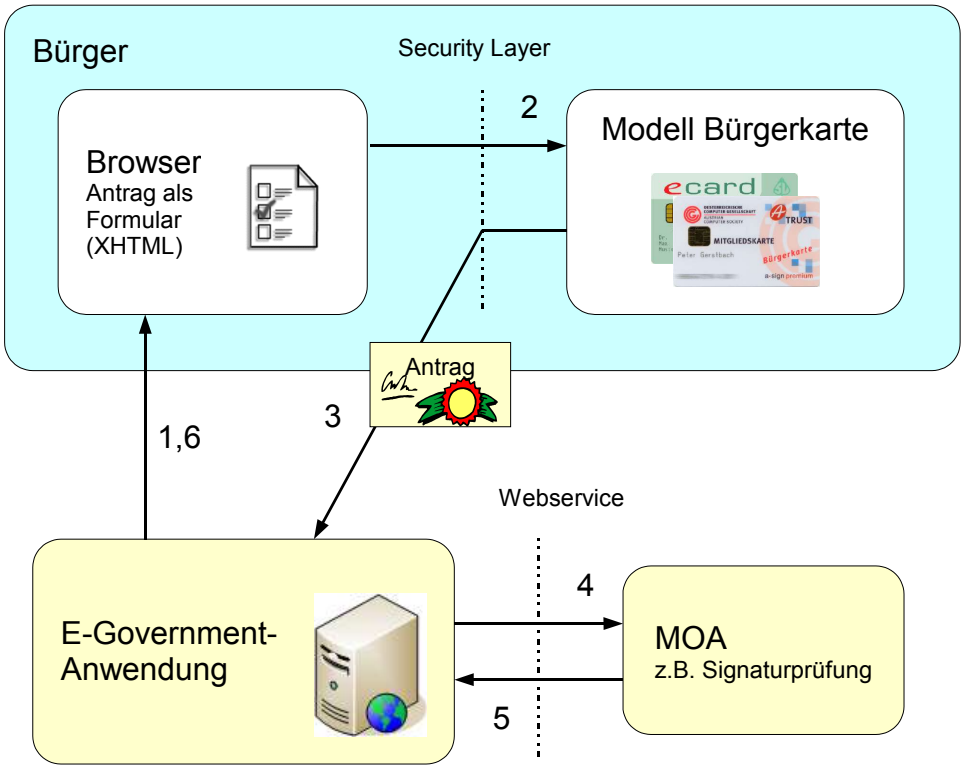
In diesem Kapitel wird anhand der Abbildung 3.1 der Ablauf einer E-Government-Sitzung beschrieben, bei der ein Antrag (z.B. der Antrag auf Kinderbetreuungsgeld) gestellt wird.

- **Formular (1)**: nachdem der Bürger die entsprechende Webseite aufgerufen hat, sendet die E-Government-Applikation das entsprechende HTML- oder XHTML-Formular an den Bürger. Im Formular sind vom Bürger alle benötigten Felder auszufüllen.
- **Security-Layer-Request (2)**: wenn der Bürger das Formular absendet, werden die Formular-Daten an die Bürgerkarten-Umgebung gesendet. Das zu verwendende Protokoll ist im Security Layer (siehe Abschnitt 3.2.4) definiert. Hat die Bürgerkarten-Umgebung die Daten empfangen, werden sie dem Bürger angezeigt und zur Signatur vorgelegt.
- **Signieren und Absenden (3)**: sobald der Antrag vom Bürger signiert wurde, wird er an die E-Government-Applikation geschickt. Das zu verwendende Protokoll ist ebenfalls im Security Layer definiert.
- **Verarbeitung (4)+(5)**: die E-Government-Applikation kann die empfangenen Daten speichern und weiterverarbeiten. Für einige Bearbeitungsschritte (z.B. Signaturprüfung oder Authentifikation des Bürgers) existieren Servermodule (*Module für Online-Applikationen*, MOA, siehe Abschnitt 3.2.5), die als Webservice angesprochen werden können.
- **Bestätigung (6)**: als Antwort auf den gesendeten Antrag erhält der Bürger ein Bestätigung seiner Angaben oder Anweisungen für weitere Schritte im Prozess.

3.2 Rollen und Schnittstellen in einer E-Government-Sitzung

In diesem Kapitel werden die definierten Rollen und Schnittstellen des *Modells Bürgerkarte* (siehe Abbildung 2.1 auf Seite 3) im Detail erläutert. Die

Abbildung 3.1: Ablauf einer E-Government Sitzung



Kommunikation zwischen dem *Bürger* und der *E-Government-Applikation* regelt die Bürgerkarten-Umgebung, ihre Schnittstelle zum Bürger ist die Benutzer-Schnittstelle, jene zur Applikation der Security-Layer. In den folgenden fünf Abschnitten wird die benötigte Infrastruktur der einzelnen Rollen erklärt und die Spezifikation der Schnittstellen beschrieben. Diese Beschreibung der Spezifikation basiert auf der Version 1.2.0 vom 14.05.2004 der österreichischen Bürgerkarte [HK04].

3.2.1 Bürger

Die wichtigste Rolle im Modell Bürgerkarte nimmt der Bürger selbst ein. Er kommuniziert über die E-Government-Applikation mit der Verwaltung und ist somit die wichtigste Zielgruppe.

Für die - beim aktuellen Stand der Technik - empfohlene lokale Bürgerkarten-Umgebung mit Chipkarte wird auf seiten des Bürgers ein Chipkartenleser benötigt. Dieser kostet im Einzelhandel aktuell ca. 20 EUR. Bei flächendeckender Einführung wird aber erwartet, dass die Kosten sinken und eventuell von der Privatwirtschaft übernommen werden, z.B. im Rahmen von e-Commerce-Projekten bei Banken. Die Geräte sind in zahlreichen Versionen am Markt verfügbar. Derzeit enthält die von der A-Trust geführt Liste an empfohlenen Kartenlesern vier Geräte von vier Herstellern. Die Geräte sind bisher aber nur unter Windows ein-

setzbar. Abbildung 3.2 zeigt den Kartenleser der Firma SCM Microsystems.

Die Verwendung von Chipkarten in Verbindung mit Kartenlesern bringt die derzeit höchstmögliche Sicherheit. Der geheime Schlüssel ist sicher auf der Chipkarte aufgebracht und kann nur zur Erzeugung von Signaturen verwendet werden, wenn der PIN bekannt ist. Das Kartenlesegerät verhindert, dass der PIN bei der Übertragung ausgespäht werden kann. Bei der Benutzung einer normalen Computer-Tastatur wäre durch ein *Keylogger*-Programm eine derartige Spionage mit geringem Aufwand möglich.

Auf Softwareseite wird die schon erwähnte Bürgerkarten-Umgebung benötigt. Diese Software wird von der Stabsstelle IKT-Strategie des Bundes kostenlos zur Verfügung gestellt. Der Abschnitt 3.2.3 behandelt die Bürgerkarten-Umgebung im Detail.

Abbildung 3.2: Kartenleser für die Bürgerkarte

3.2.2 Benutzer-Schnittstelle

Die Benutzerschnittstelle ist jene Schnittstelle, über die der Bürger mit der Bürgerkarten-Umgebung kommuniziert. Sie enthält Funktionen, um Befehle an den Security-Layer abzuwickeln, wie beispielsweise das Anzeigen eines zu signierenden Dokuments. Weiters kann über diese Schnittstelle das Verhalten der Bürgerkarten-Umgebung an die Wünsche des Benutzers angepasst werden. In den folgenden Absätzen werden zwei Anforderungen näher behandelt: der Zugriffsschutz und der Vorgang der Signaturerstellung.

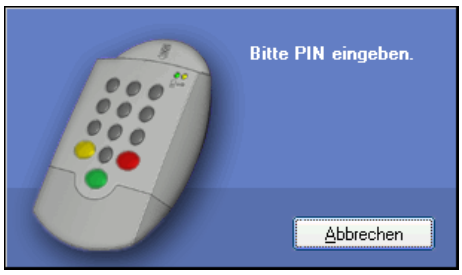
Zugriffsschutz Bei der Ausführung eines Befehls von der Bürgerkarten-Umgebung gibt es vier verschiedene Interaktionsarten. Dadurch entsteht ein Zugriffsschutz und es wird gewährleistet, dass bei bestimmten Befehlen der Benutzter informiert bzw. um Erlaubnis gefragt wird:

- **keine Interaktion**

- **Information**: die Ausführung eines Befehls muss in einfach zu verstehender Form und leicht zugänglich protokolliert werden
- **Bestätigung**: Die BKU muss vor der Ausführung die Erlaubnis des Bürgers einholen. Diese ist beispielsweise vor dem Auslesen der Personenbindung durch eine Applikation nötig. Abbildung 3.3 zeigt einen möglichen Dialog für diesen Fall.
- **Bestätigung mit Kennwort**: Zusätzlich zur normalen Bestätigung muss der Bürger das Kennwort eingeben. Die Übermittlung dieses Kennworts muss verschlüsselt durchgeführt werden. Abbildung 3.4 zeigt einen möglichen Dialog für diesen Fall.

Abbildung 3.3: Bestätigungs-Dialog

Abbildung 3.4: Bestätigungs-Dialog mit Kennwort-Eingabe



Signaturerstellung Die Signaturerstellung ist das zentrale Element einer E-Government-Sitzung. Vor der Signaturerstellung muss die BKU dem Bürger die Möglichkeit bieten, das zu signierende Dokument anzuzeigen. Ist diese Anzeige nicht möglich (beispielsweise bei einem der BKU unbekannten Dateiformat), darf es dem Bürger nicht möglich sein, eine *sichere elektronische Signatur* zu erzeugen. Weiters muss dem Benutzer auch der Zeitpunkt der Signaturerstellung angezeigt werden, da diese Uhrzeit ebenfalls in der Nachricht enthalten sein wird. Die Abbildung 3.5 auf Seite 20 zeigt die Anzeige eines zu signierendes Dokuments.

Standard-Anzeigeformat Im Abschnitt *Standard-Anzeigeformat* der Security-Layer-Spezifikation wird das Standard-Anzeigeformat zur Bürgerkarten-Umgebung definiert. Dieses Anzeigeformat muss von jeder Bürgerkarten-Umgebung angezeigt werden können. Die Basis dafür bildet der W3C-Standard[1] *XHTML*

[1] Das World Wide Web Consortium (W3C) arbeitet an der Entwicklung neuer Protokollspezifikationen und Architekturen für das World Wide Web und wird von Forschungsinstituten, IT-Unternehmen und vielen Anwendern unterstützt.

1.1 und *CSS 2* (Cascading Stylesheets 2). Ausgehend davon werden jedoch einige Einschränkungen definiert, um dynamische Elemente wie Skripts und Link-Informationen zu verhindern. Diese Einschränkungen sind notwendig, da Skripts (z.B. das im Internet häufig eingesetzte JavaScript) und Links das Erscheinungsbild verändern könnten, ohne dass die Veränderung an der Signatur erkennbar wäre.

3.2.3 Bürgerkarten-Umgebung

Die Bürgerkarten-Umgebung (BKU) ist ein Programm bzw. ein Dienst, das den Zugriff auf die Funktionen der Bürgerkarte ermöglicht. Wie bereits erklärt wurde, läuft im Falle einer *lokalen Bürgerkarten-Umgebung* ein Programm lokal am Computer des Bürgers. Das Programm kommuniziert über den Treiber mit dem Kartenleser und hat Zugriff auf die Signaturfunktionen der Smartcard. Im Falle einer *serverbasierten Bürgerkarten-Umgebung* wird die Funktionalität der Bürgerkarte von einem entfernten Service übernommen, der über das Internet angesprochen wird.

In beiden Fällen werden von der BKU zwei Schnittstellen angesprochen: für die Kommunikation mit dem Bürger implementiert die BKU die Anforderungen an die Benutzer-Schnittstelle (siehe Abschnitt 3.2.2), die Kommunikation zur E-Government-Applikation läuft über die definierten Protokolle der Schnittstellenspezifikation des *Security-Layer*s (siehe Abschnitt 3.2.4).

Derzeit existieren zwei Implementierungen von lokalen Bürgerkarten-Umgebungen. Die Firma *IT Solution* vertreibt das Produkt „trustDesk“, für dieses wurde von der IKT-Stabstelle des Bundes eine Generallizenz für alle Bürger erworben. Die Firma *BDC* bietet mit „hot:Sign“ ebenfalls eine BKU an, diese kann direkt beim Hersteller erworben werden. Beide Produkte laufen derzeit nur unter dem Betriebssystem Microsoft Windows.

Das Signaturgesetz [Sig, §18(5)] erfordert, dass die technischen Komponenten und Verfahren für die Erstellung sicherer elektronischer Signaturen nach dem Stand der Technik bescheinigt werden. Dies ist Aufgabe einer Bestätigungsstelle. Das *Zentrum für sichere Informationstechnologie - Austria* (A-SIT) ist die erste und derzeit einzige österreichische Bestätigungsstelle und hat für beide Produkte entsprechende Bescheinigungen erteilt.

3.2.4 Security-Layer

Der Security-Layer ist jene Schnittstelle, über die die Applikation mit der Bürgerkarten-Umgebung kommuniziert. Bei der Definition der Schnittstelle werden zwei Bereiche unterschieden, die im folgenden näher erläutert werden:

- Die Applikationsschnittstelle des Security-Layers
- Die Transportprotokolle des Security-Layers

Applikationsschnittstelle

Die Applikationsschnittstelle definiert die Befehle, die von einer Bürgerkarten-Umgebung zur Verfügung gestellt werden müssen, beispielsweise um eine elektro-

nische Signatur zu erstellen oder vom Datenspeicher der Bürgerkarten-Umgebung zu lesen.

Das Protokoll basiert auf einem einfachen *Anfrage/Antwort-Muster*. Die Applikation schickt eine XML[2]-kodierte Anfrage an die Bürgerkarten-Umgebung, diese sendet eine entsprechende Antwort zurück an die Applikation. Die möglichen Elemente des Protokolls sind als XML Schema spezifiziert.

Die Schnittstelle Security-Layer unterstützt zwei möglich Formate für kryptografische Verfahren. *CMS* (Cryptographic Message Syntax) ist ein Standard der Internet Engineering Task Force (IETF) und definiert eine Syntax, um beliebige Nachrichten elektronisch zu signieren, Hashwerte zu bilden und zu verschlüsseln. *XMLDSig* (XML-Signature Syntax and Processing) setzt sich ein ähnliches Ziel, um XML-Daten zu signieren. Bei XMLDSig ist es zusätzlich möglich, mehrere Datenobjekte mittels einer einzigen Signatur zu signieren oder auch einzelne Elemente aus der Signatur auszuschließen. Die Implementierung von XMLDSig ist für eine Bürgerkarten-Umgebung obligatorisch, während die CMS-Unterstützung optional ist.

Ein üblicher Anwendungsfall ist das Auslesen der Personenbindung mit darauf folgender Signierung von Formular-Daten. Die folgenden Beispiel-Listings und Abbildungen zeigen die anfallenden Kommunikationsdaten, die beim Signieren eines Test-Anbringens[3] anfallen. Bei diesem Anbringen können in einem HTML-Formular Daten wie z.B. die E-Mail-Adresse des Absenders bzw. des Empfängers eingegeben werden. Die Formular-Daten werden dann signiert und das signierte Dokument zur Kontrolle an beide E-Mail-Adressen verschickt. Listing 3.1 zeigt den XML-kodierten Befehl, der an die Bürgerkarten-Umgebung gesendet wird, um die Personenbindung auszulesen. Laut Spezifikation muss diese Aktion vom Bürger bestätigt werden (siehe auch Abbildung 3.3 in Abschnitt 3.2.2).

Listing 3.1: InfoboxReadRequest

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <sl10:InfoboxReadRequest xmlns:sl10="http://www.
     buergerkarte.at/namespaces/securitylayer/20020225#">
3   <sl10:InfoboxIdentifier>IdentityLink</
       sl10:InfoboxIdentifier>
4   <sl10:BinaryFileParameters ContentIsXMLEntity="true"/>
5 </sl10:InfoboxReadRequest>
```

Wenn der Benutzer das Auslesen erlaubt hat, wird ein weiterer Befehl an die Bürgerkarten-Umgebung gesendet, der das Signieren der Formular-Daten einleitet. Listing 3.2 zeigt diesen Befehl als XML kodiert. Aus Gründen der Übersichtlichkeit ist das XML-Dokument nur in Auszügen enthalten. Das Wurzelelement `sl11:CreateXMLSignatureRequest` leitet die Signatur nach XMLDSig ein. Das Element `sl10:XMLContent` enthält die eigentlichen Formular-Daten, u.a. die schon erwähnten E-Mail-Adressen. Innerhalb des Elements `dsig:Transform` können XSLT-Elemente (Extensible Stylesheet Transformations) angegeben werden, mit denen die XML-Daten für den Anwender formatiert werden können. Die

[2] Die Extensible Markup Language (XML) ist ein einfaches und flexibles Textformat für elektronische Publizierung und elektronischen Datenaustausch. XML ist genauso wie XHTML ein Standard des W3Cs.

[3] URL des Test-Anbringens: https://labs.cio.gv.at/egov-wip/gemeinde/anbringen-test/

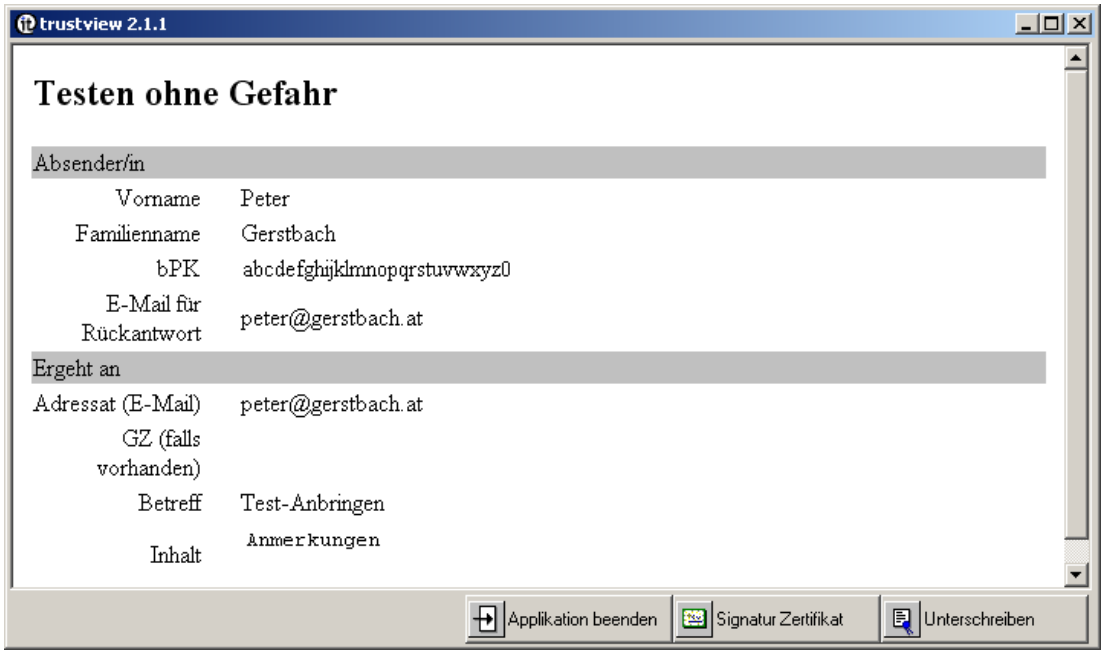
Daten für diese Transformation müssen bei der Signatur enthalten sein, da ansonsten bei der XSLT-Transformation vor dem Signieren Änderungen am Dokument vorgenommen werden könnten, die der Bürger jedoch in der Anzeige-Komponente nicht als solche erkennen könnte. Eine mögliche Anzeigekomponente mit einem zu signierenden Dokument zeigt Abbildung 3.5.

Listing 3.2: CreateXMLSignatureRequest (Auszug)

```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <sl11:CreateXMLSignatureRequest xmlns:dsig="http://www.w3.
      org/2000/09/xmldsig#" xmlns:sl10="http://www.
      buergerkarte.at/namespaces/securitylayer/20020225#"
      xmlns:sl11="http://www.buergerkarte.at/namespaces/
      securitylayer/20020831#">
3    <sl11:KeyboxIdentifier>SecureSignatureKeypair</
       sl11:KeyboxIdentifier>
4    <sl11:DataObjectInfo Structure="enveloping">
5      <sl10:DataObject>
6        <sl10:XMLContent>
7          <Eingabe writeflag="ro">
8            <Datum>06-12-2004</Datum>
9            <Uhrzeit>11:13</Uhrzeit>
10           <ID>urn:publicid:gv.at:form test-ohne-gefahr-1.0<
               /ID>
11           <Titel>Testen ohne Gefahr</Titel>
12           <inputlanguage>http://labs.cio.gv.at/egov/dict/
               egov_dict_de.xml</inputlanguage>
13           <Focus>active</Focus>
14           <Von>
15             <GivenName>Peter</GivenName>
16             <FamilyName>Gerstbach</FamilyName>
17             <bPK>abcdefghijklmnopqrstuvwxyz0</bPK>
18             <Email type="email-noempty" error="0">
                 peter@gerstbach.at</Email>
19           </Von>
20           <An>
21             <Email type="email-noempty" error="0">
                 peter@gerstbach.at</Email>
22             <ID>cio_default</ID>
23           </An>
24           <GZ/>
25           <Betreff type="no-empty" error="0">Test-Anbringen
               </Betreff>
26           <Inhalt>Anmerkungen</Inhalt>
27         </Eingabe>
28       </sl10:XMLContent>
29     </sl10:DataObject>
30     <sl10:TransformsInfo>
31       <dsig:Transforms>
32         <dsig:Transform Algorithm="http://www.w3.org/TR
             /1999/REC-xslt-19991116">
```

```
33            <xsl:stylesheet version="1.0" xmlns:xsl="http://
                 www.w3.org/1999/XSL/Transform" xmlns="http://
                 www.w3.org/1999/xhtml">
34              <!-- XSLT-Elemente... -->
35            </xsl:stylesheet>
36          </dsig:Transform>
37          <dsig:Transform Algorithm="http://www.w3.org/TR
               /2001/REC-xml-c14n-20010315"/>
38        </dsig:Transforms>
39      </sl10:TransformsInfo>
40    </sl11:DataObjectInfo>
41 </sl11:CreateXMLSignatureRequest>
```

Abbildung 3.5: Anzeige eines zu signierenden Dokuments



Transportprotokolle

Die Spezifikation der Transportprotokolle beschreibt, wie die XML-Befehle der Applikationsschnittstelle an bestimmte Transportprotokolle gebunden werden. Es werden folgende Bindungen unterstützt:

- TCP/IP
- HTTP
- SSL/TLS
- HTTPS

Von diesen Möglichkeiten wird hier nur die HTTP-Bindung erläutert, da sie direkt mit einem Web-Browser ohne weitere Komponenten (wie z.B. Applets) durchgeführt werden kann. Dieses Kapitel beschreibt die Bindung bei einer lokalen Bürgerkarten-Umgebung. Technisch gesehen ist die Bürgerkarten-Umgebung ein sehr einfacher Webserver. Ein möglicher Ablauf einer Kommunikation besteht aus folgenden Schritten:

1. Die Bürgerkarten-Umgebung wartet an der IP-Adresse `127.0.0.1` (*localhost*) am Port `3495` auf eingehende Verbindungen.

2. Eine Applikation sendet einen HTTP-Request an die Adresse `http://localhost:3495/http-security-layer-request`. Der Request enthält u.a. als Parameter den XML-Request des Security-Layer-Befehls. Listing 3.3 zeigt einen HTTP-POST-Request.

3. Die Bürgerkarten-Umgebung entnimmt den zu bearbeitenden XML-Request aus den Formular-Parametern und bearbeitet ihn. Dieser Schritt kann auch die Transformation mittels XSLT-Befehlen oder die Weiterleitung des Requests enthalten.

Listing 3.3: CreateXMLSignature HTTP-POST-Request (Auszug)

```
1 POST http://127.0.0.1:3495/http-security-layer-request HTTP
    /1.1
2 Content-Type: application/x-www-form-urlencoded
3 Content-Length: 8182
4
5 RequestType=SECURITYLAYER-REQUEST&XMLRequest=
    HIER_STEHT_DER_XML_REQUEST&DataURL=https://labs.cio.gv.
    at/egov/cgi-bin/formular_test.pl&WeitergabeParameter_=
    Wert&SonstigeFormularFelder=Wert
```

Der HTTP-Request zeigt die Adresse, an die der Request geschickt wird, und beispielhaft einige Parameter. Aus Gründen der Übersichtlichkeit wurde der XML-Request, der ja bereits in Listing 3.2 abgebildet ist, nicht als Parameter eingefügt. Im Listing ist der Parameter `DataURL` angegeben, in diesem Fall werden jene Parameter, die mit „_“ enden, an den angegebenen Server weitergeleitet.

3.2.5 Applikation

Der Kommunikationspartner des Bürgers ist die Verwaltung. An ihrer Stelle tritt eine E-Government-Applikation, im folgenden vereinfacht Applikation genannt. Die Applikation ist ein Programm, das auf einem Applikations-Server läuft und über den Security-Layer Anfragen an die Bürgerkarten-Umgebung richtet. Die Applikation nimmt dann ebenfalls die Antworten der Bürgerkarten-Umgebung entgegen und verarbeitet sie. Da für viele Verwaltungseinrichtungen bereits Backoffice-Anwendungen existieren, ist die Hauptaufgabe der Applikation zumeist diese vorhandenen Systeme anzusprechen.

Da die Spezifikation des Security-Layers offene Protokolle und Standards verwendet, kann die Applikation für viele unterschiedliche Plattformen programmiert

werden. Die beiden bekanntesten Programmierplattformen, Java von Sun Microsystems und .NET von Microsoft, bieten entsprechende Unterstützung, um solche Applikationen sicher und effizient zu entwickeln.

Einige Funktionen einer E-Government-Applikation werden in sehr vielen Installationen vorhanden sein. Beispielsweise müssen fast alle Applikationen Bescheide signieren, den Bürger anhand seiner bereichsspezifischen Personenkennung identifizieren und seine elektronische Unterschrift überprüfen. Damit diese gemeinsamen Funktionen nicht für jede Applikation einzeln programmiert werden müssen, wurden diese sogenannten *Module für Online-Applikationen* (MOA) bereits implementiert. Die öffentliche Verwaltung und auch die Privatwirtschaft kann diese Module kostenfrei nutzen. Sie können entweder direkt in die Applikation eingebunden (als Java-Bibliothek) oder als Webservice, unabhängig von der verwendeten Plattform, angesprochen werden.

4 Test existierender Bürgerkarten-Anwendungen

4.1 E-Mail

Die Verwendung zur sicheren Kommunikation mittels E-Mail ist wahrscheinlich die am häufigsten verwendete Funktion von kartenbasierten (lokalen) Bürgerkarten. Eigentlich hat dies aber mit dem Konzept der Bürgerkarte nichts zu tun, sondern ist mit jeder Signaturkarte möglich. In Abschnitt 2.2.3 wurde bereits erwähnt, dass Schlüssel, die zur Erzeugung einer *sicheren elektronischen Signatur* verwendet werden, nicht im Rahmen anderer kryptographischer Prozesse benutzt werden dürfen. Deswegen existiert auf der Karte noch ein weiteres Zertifikat, das auch in anderen Umgebungen eingesetzt werden kann, aber trotzdem den Eigentümer anhand der Personenbindung identifiziert. Dieser Schlüssel kann in anderen Anwendungen, wie bspw. einem E-Mail-Programm, verwendet werden.

Der E-Mail-Standard ist ein sehr alter Standard. Um keine Kompatibilitätsprobleme mit E-Mails einzuführen, blieb der Standard in vielen Teilen seit 1982 unverändert. Das herkömmliche System besitzt mehrere Schwächen. Die meisten Nachrichten werden im Klartext versendet und können deswegen prinzipiell auf jedem Rechner, über den die Nachricht geschickt wird, unbefugt ausgelesen oder auch verändert werden. Weiters kann die Absenderadresse einer E-Mail in der Regel beliebig eingestellt werden. Beide Schwächen können durch das Verschlüsseln bzw. Signieren von Nachrichten behoben werden.

Mit einer Chipkarten-basierten Bürgerkarte können E-Mails gemäß dem Standard *S-MIME* verschlüsselt oder signiert werden. Bereits bei der Ausstellung der Karte wird das Zertifikat mit einer E-Mail-Adresse verknüpft. Im E-Mail-Programm muss zuerst das Stammzertifikat des Kartenanbieters (A-Trust) installiert werden. Seit Mitte 2003 ist es bereits im Wurzelzertifikat von Microsoft-basierten Systemen enthalten. Danach kann das eigene Zertifikat installiert und dem E-Mail-Konto zugewiesen werden. Nun können auf Wunsch E-Mails, nach der Eingabe des PINs, signiert übertragen und somit vor Manipulationen geschützt werden.

Auf Seiten des Empfängers sind keine weiteren Konfigurationen nötig, außer der Import des Zertifikats, falls nicht bereits das Wurzelzertifikat von A-Trust enthalten ist. Anhand einer Anzeige, die je nach verwendetem E-Mail-Programm variiert, kann der Empfänger erkennen, ob die Nachricht unverändert ist. Eine Antwort-Mail kann nun auch mit dem öffentlichen Schlüssel des Bürgerkarten-Besitzers verschlüsselt werden. Der Empfänger dieser Antwort-Mail kann, nach der Eingabe seines PINs, die Nachricht wieder im Klartext lesen.

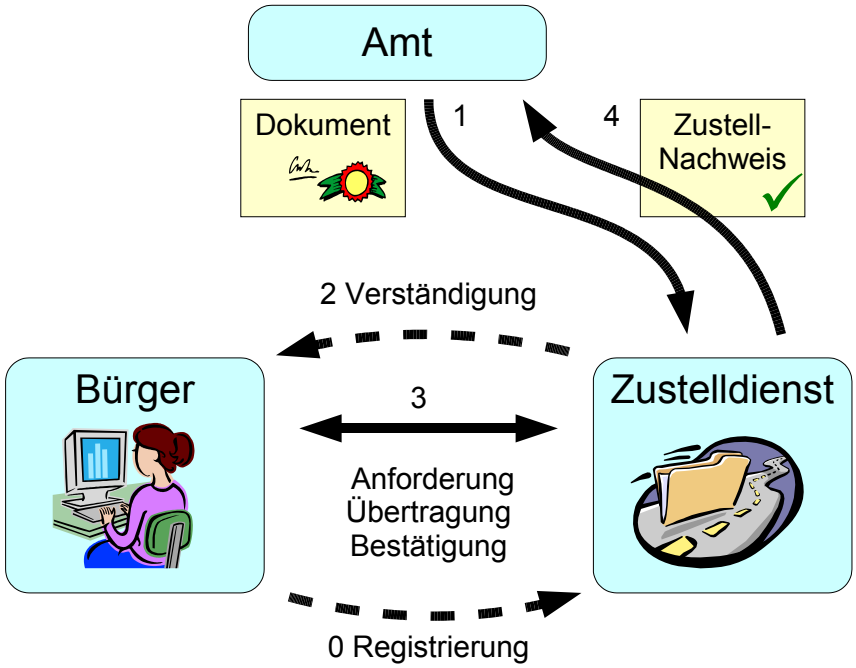
4.2 Zustellung

Die elektronische Zustellung soll allmählich die papierbasierte Kommunikation von Behörden an Bürger ersetzen. Monatlich werden beispielsweise vom Bundesrechenzentrum ca. 3 Millionen Briefsendungen ausgeschickt. Dadurch entstehen enorme Druck-, Kuvertier- und Portokosten. Eine Umstellung auf elektronische Übermittlung würde neben Kostensenkungen auch Effizienzsteigerungen und Kundenfreundlichkeit bringen und rechtliche Vorgaben für RSa- und RSb-Briefe erfüllen: die Zustellung könnte innerhalb Minuten abgeschlossen sein, statt Tage zu brauchen, es gäbe weniger Medienbrüche, Zugriff auf die Briefe wäre von überall aus möglich und der Weg des Bürgers aufs Postamt würde entfallen.

Rechtliche Grundlage für die elektronische Zustellung ist das Zustellgesetz [Zus], das im Jahr 2002 novelliert wurde. Die Anforderungen an die elektronische Zustellung ist eine qualitative Authentifizierung, aktive und passive Sicherheit, Datenschutz und ein qualitativer Zustellnachweis. Weiters sollte der Prozessablauf sowohl für die Verwaltung als auch für den Bürger einfach sein und eine Verfügbarkeit auch außerhalb der Verwaltung die Etablierung eines Marktes ermöglichen [Rei04].

Die technische Spezifikation der Zustellung ist ebenso öffentlich zugänglich wie die Spezifikationen zur Bürgerkarte. Der gesamte Prozess der Zustellung läuft in mehreren Schritten ab. Die Abbildung 4.1 illustriert die fünf, aus Sicht des Bürgers, wichtigsten Schritte.

Abbildung 4.1: Ablauf der Zustellung



- **Registrierung (0)**: Der Bürger registriert sich online mit seiner Bürgerkarte bei einem Zustelldienst seiner Wahl. Er identifziert sich, stellt Schlüssel für die Verschlüsselung zur Verfügung, gibt seine Verständigungsadresse

(z.B. per E-Mail oder SMS) an und wählt die Dokumentenformate aus, die er lesen kann. (In der Abbildung ist dieser Vorgang als Schritt **(0)** gekennzeichnet.)

- **Adressermittlung**: Alle Zustelldienste sind verpflichtet einen Verzeichnisdienst der registrierten Empfänger zu führen. Soll nun ein Dokument zugestellt werden, kann über diese Verzeichnisdienste abgefragt werden, ob der Bürger überhaupt eine elektronische Zustellung wünscht und falls ja, welche Attribute er dazu angegeben hat (Schlüssel, Dokumentenformate, etc.)
- **Übermittlung (1)**: Nun wird, falls erwünscht, das Dokument verschlüsselt und über eine Webservice-Schnittstelle an den jeweiligen Zustelldienst übermittelt.
- **Verständigung (2)**: Der Zustelldienst verständigt den Empfänger. Die Verständigung per E-Mail muss unterstützt werden - optional sind auch andere Kanäle, wie SMS, Voicemail oder FAX möglich. Wenn auf die Verständigung keine Reaktion erfolgt, wird das Schriftstück herkömmlich auf dem Papierweg zugestellt.
- **Abholung (3)**: In dem Moment, in dem sich der Bürger beim Zustelldienst mittels Bürgerkarte angemeldet hat, gelten die Schriftstücke als zugestellt. Die Schriftstücke werden aufgelistet, können angesehen bzw. heruntergeladen werden oder als normale E-Mail weitergeleitet werden. Weiters kann der Bürger die Signatur des Absenders überprüfen. Falls die Nachricht verschlüsselt wurde, kann sie der Bürger mit der Bürgerkarten-Umgebung entschlüsseln.
- **Zustellnachweis (4)**: Der Zustelldienst signiert die Login-Signatur des Bürgers und die Daten des Zustellstückes. Dies ist für den Absender der Nachricht die Bestätigung, dass das Zustellstück elektronisch zugestellt wurde.

Derzeit betreibt das Bundeskanzleramt einen Prototyp eines Zustelldienstes unter http://www.zustellung.gv.at/. Abbildung 4.2 zeigt die erste Seite nach erfolgreichem Login. Die aktuelle Version ermöglicht die Zustellstücke einzusehen, Abwesenheitsmeldungen durchzuführen und Einstellungen (Schlüssel, Dokumentenformate etc.) durchzuführen. Bis November 2004 waren auf dem System ca. 200 Benutzer registriert, also etwas über 1% aller Besitzer von Bürgerkarten. Da die Zustellung auf einer offenen Spezifikation basiert, wird es in Zukunft, vermutlich von unterschiedlichen privaten Anbietern, Zustelldienste mit erweitertem Funktionsumfang geben. Erweiterte Funktionen, wie z.B. die Verständigung oder privatwirtschaftliche Nutzbarkeit des Services, könnten eine Differenzierung unter mehreren Marktteilnehmern bringen.

4.3 Finanz Online

Die Anwendung FINANZ*Online* vom Bundesministerium für Finanzen ermöglicht seit dem Jahr 2003 elektronische Abwicklung von Steuerangelegenheiten für

Abbildung 4.2: Der „Briefkasten“ von zustellung.gv.at

Bürger, Unternehmen und Gemeinden.

Beispielsweise kann der Bürger bei FINANZ*Online* sein Steuerkonto und seine Steuerakte abfragen, die Arbeitnehmerveranlagung eingeben und die Änderung persönlicher Daten bekanntgeben. Unternehmer können ebenfalls ihre Steuerkonten und Steuerakte abfragen und u.a. die Umsatzsteuervoranmeldung und Jahreserklärungen übermitteln.

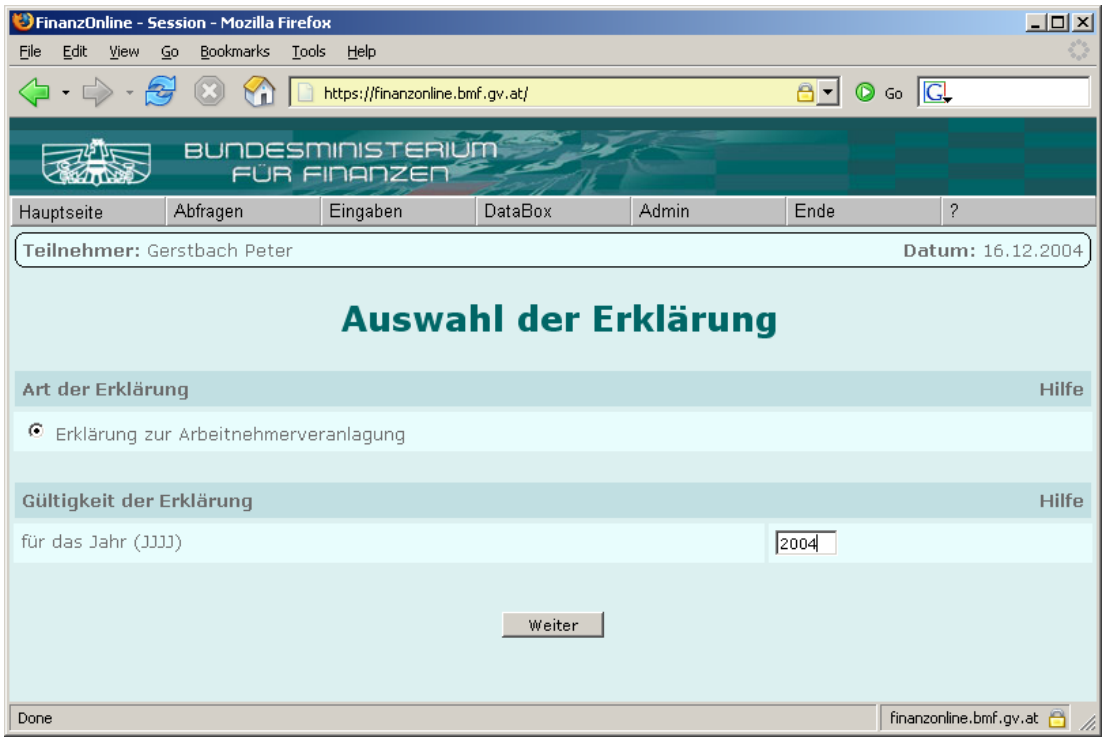
Bei der Einführung von FINANZ*Online* im Jahr 2003 war das Login nur nach einer Registrierung möglich, die Zugangsdaten wurden per Post zugeschickt. Sie bestehen aus einer 12-stelligen Teilnehmernummer, einer Benutzer-ID und einem 8-stelligen alphanumerischen PIN. Das Login war demnach langwierig und fehleranfällig. Durch die Bürgerkarte und das Auslesen der Personenbindung fällt diese Prozedur weg und ermöglicht erstmals eine einfache und sichere Verwendung. Abbildung 4.3 zeigt einen Screenshot der Anwendung.

4.4 Sozialversicherung

Die Österreichische Sozialversicherung bietet auf ihrer Homepage seit 2003 drei Services an, die Zertifikate auf Bürgerkarten zur Authentifizierung verwenden:

- Grunddaten zur Krankenversicherung
- Versicherungsdatenauszug

Abbildung 4.3: Screenshot von FINANZOnline



- Versicherungsnummernabfrage

Um die Services nutzen zu können, ist eine Erstanmeldung notwendig. Dieser Schritt ist notwendig, da die Services nicht die Personenbindung der Bürgerkarten abfragen. Wenn die Kombination aus Vorname, Nachname, Geburtsdatum, Adresse und Versicherungsnummer eindeutig zu einem vorhandenen Datensatz passen, wird die Erstanmeldung automatisiert durchgeführt, wodurch es zu keinen Verzögerungen kommen soll. Bei Fehlern in den Daten, die eine manuelle Prüfung erfordern, kann diese Freischaltung entsprechend länger dauern. Nach der Erstanmeldung ist das Zertifikat mit den Datenbeständen der Sozialversicherung abgeglichen und die Abfragen können an Arbeitstagen von 6:00 bis 22:00 Uhr durchgeführt werden.

Die Abfrage *Grunddaten zur Krankenversicherung* liefert neben der Sozialversicherungsnummer die Krankenkasse, bei der man zur Zeit versichert ist. Das Service *Versicherungsdatenauszug* generiert ein mehrseitiges PDF-Dokument, das alle seit 1972 erworbenen Zeiten und Beitragsgrundlagen und die dazugehörigen Dienstgeberdaten auflistet. Die *Versicherungsnummernabfrage* wird für alle Vertragspartner der Sozialversicherung angeboten, damit können z.B. Ärzte grundlegende Daten ihrer Patienten, wie Sozialversicherungsnummer oder Namen, überprüfen.

Bis November 2004 waren etwa 1.000 Bürgerkartenbesitzer im System registriert. Im Jahr 2003 wurden die Services ca. 5.000 mal genutzt, von Jänner bis Oktober 2004 ca. 9.000 mal, die Nutzungsfrequenz stieg also in einem Jahr um mehr als das Doppelte.

4.5 Netbanking BAWAG P.S.K.

Die BAWAG P.S.K. Gruppe unterstützt derzeit als einzige Bank in Österreich Netbanking mit Signatur-Karte. Neben der üblichen Kombination aus Teilnehmer-Nummer und PIN kann für das Login auch eine Signatur-Karte verwendet werden. Für das Login wird eine eigene Signatur-Lösung der Firma SecCommerce Informationssysteme GmbH eingesetzt. Es handelt sich also um keine echte Bürgerkarten-Anwendung, da nicht die sichere elektronische Signatur in Verbindung mit der Bürgerkarten-Umgebung eingesetzt wird, sondern das zweite Zertifikat verwendet wird, das auf der Karte vorhanden ist.

Beim Login wird ein Java-Applet geladen, welches direkt den Kartenleser anspricht und die Signatur auslöst. Neben dem Login wird die Signatur auch bei Aufträgen beispielsweise für Überweisungen eingesetzt. Es müssen somit auf Seiten des Kunden weder Verfügernummer und PIN, noch die TAN-Liste verwendet werden.

4.6 Weitere Anwendungen

Derzeit existiert noch eine Reihe weiterer Anwendungen auf Bundes- und Gemeindeebene. Das Bundesministerium für Inneres bietet elektronische Meldestellen für Kinderpornographie, Umweltkriminalität und Wiederbetätigung und den Antrag auf Ausstellung einer Strafregisterbescheinigung an. Beim Bundesministerium für soziale Sicherheit und Generationen kann der Antrag auf Kinderbetreuungsgeld ausgefüllt werden. Die Bundesbeschaffungs GmbH bietet ein System für die elektronische Ausschreibung an.

Der Österreichische Amtshelfer (help.gv.at) bietet für einige Gemeinden Verfahren zur Geburtsurkunden-Ausstellung, Gewerbeanmeldung und Kommunalsteuererklärung an. Einige Gemeinden, wie Inzersdorf-Getzersdorf oder Weikersdorf am Steinfelde, bieten weitere elektronische Verfahren an. Die vollständige Liste aller Anwendungen findet sich auf der Seite der Stabstelle IKT-Strategie des Bundes [Bun04b].

5 Zusammenfassung

Die Bürgerkarte ist das „amtliche Ausweisdokument“ in elektronischen Verwaltungsverfahren. Das Projekt wurde im Jahr 2000 gestartet und hat sich seitdem zügig weiterentwickelt. Rechtlich basiert es auf neuen Gesetzen, wie dem Signaturgesetz und dem E-Government-Gesetz. Dadurch ist eine digitale Signatur der herkömmlichen handschriftlichen Unterschrift in fast allen Anwendungsfällen gleichgestellt. Technisch lässt sich die Bürgerkarte am besten durch Chipkarten realisieren, um die Sicherheitsanforderungen zu erfüllen. Das offene und technologieunabhängige Konzept erlaubt auch Anwendungen in der Privatwirtschaft und die Verwendung von anderen Geräten, um Mobiltelefone oder USB-Geräte zur „Bürgerkarte“ zu machen.

Ende 2004 sind bereits über 16.000 chipbasierte Bürgerkarten ausgegeben, mit denen sich bereits einige E-Government-Anwendungen im öffentlichen und auch privaten Bereich nutzen lassen. Beispiele sind FinanzOnline, elektronische Zustellung, die Strafregisterbescheinung oder Services der Sozialversicherung. In Zukunft wird die Zahl der Anwendungen stark steigen, da die angebotene Infrastruktur kontinuierlich verbessert wird und Software teilweise kostenlos der Verwaltung und der Privatwirtschaft angeboten wird. Auch die Verbreitung der Bürgerkarte wird im Jahr 2005 einen weiteren Höhepunkt erlangen, wenn neue Bankomatkarten und die Sozialversicherungskarten (*e-Card*) mit Bürgerkartenfunktionalität ausgegeben werden.

Die Anforderungen an die Bürgerkarte sind die sichere elektronische Signatur und Inhaltsverschlüsselung (Einsatz von asymmetrischen Schlüsseln und Zertifikaten), die Personenbindung (dadurch wird das Zertifikat mit einer Person verknüpft), Infoboxen (um zusätzliche Dokumente, wie Vollmachten, zu speichern) und das Vorhandensein des Security-Layers.

Der Security-Layer ist das Herzstück der Technischen Spezifikation der Bürgerkarte. Er ist die Schnittstelle zwischen der Bürgerkarten-Umgebung auf Benutzerseite und der E-Government-Applikation auf Verwaltungsseite. Die Spezifikation definiert die Anforderungen an die Benutzeroberfläche und beschreibt die Kommunikation über das Internet. Sie basiert auf international etablierten Protokollen und Formaten, wie HTTP und XML.

Das Projekt Bürgerkarte ist schon weit fortgeschritten, der weiteren Verbreitung stehen jedoch noch Vorurteile und Bedenken entgegen. Auch die zur Verfügung gestellte Software muss noch weiter verbessert werden. Doch schon jetzt ermöglicht die Bürgerkarte Behördengänge von zu Hause oder vom Büro aus - rund um die Uhr. Für den Staat ergeben sich mit der durchgängig elektronischen Abwicklung effizientere Verfahren und schnellere Abwicklung, was wieder dem Bürger zu Gute kommt.

Abbildungsverzeichnis

Listings

Literaturverzeichnis

[Bun04a] Bundeskanzleramt, Republik Österreich: *Die Verwaltungssignatur*. URL: http://www.cio.gv.at/service/brochures/ (Abgerufen am 27.12.2004), Mai 2004.

[Bun04b] Bundeskanzleramt, Republik Österreich: *Homepage der Stabsstelle IKT-Strategie des Bundes*. URL: http://www.cio.gv.at/ (Abgerufen am 17.12.2004), 2004.

[Bun04c] Bundeskanzleramt, Republik Österreich: *Stammzahlen und bereichspezifische Personenkennzahl (bPK)*. URL: http://www.cio.gv.at/service/brochures/ (Abgerufen am 27.11.2004), Mai 2004.

[E-G] *Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz - E-GovG), BGBl. I Nr. 10/2004*.

[HK04] Hollosi, Arno und Gregor Karlinger: *Die österreichische Bürgerkarte*. URL: http://www.buergerkarte.at/konzept/securitylayer/spezifikation/20040514/ (Abgerufen am 30.11.2004), Mai 2004. Version 1.2.0.

[Kri04] Krimmer, Robert: *E-Voting Wahltest zur Bundespräsidentschaftswahl an der Wirtschaftsuniversität Wien 2004*. URL: http://e-voting.wu-wien.ac.at/scripts/download.php?F_ID=72 (Abgerufen am 29.11.2004), März 2004.

[MW04] Mittheisz, Johann und Harald Wiesner: *Standarddaten für E-Formulare*. URL: http://reference.e-government.gv.at/Veroeffentlichte_Entwuerfe.302.0.html (Abgerufen am 27.12.2004), Juni 2004.

[NA00] Network Associates, Inc.: *An Introduction to Cryptography*. URL: ftp://ftp.de.pgpi.com/pub/pgp/7.0/docs/english/IntroToCrypto.pdf (Abgerufen am 27.11.2004), 2000.

[P+02] Posch, Reinhard et al.: *Weißbuch Bürgerkarte*. URL: http://www.buergerkarte.at/weissbuch/20020515/WeissbuchBuergerkarte.20020515.pdf (Abgerufen am 28.11.2004), Mai 2002.

[Rei04] Reichstädter, Peter: *Elektronische Zustellung - Overview.* URL: http://labs.cio.gv.at/delivery/zustellung.ppt (Abgerufen am 10.12.2004), Mai 2004.

[Sig] *Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG), BGBl. I Nr. 190/1999 idF: BGBl. I Nr. 152/2001.*

[Wik04a] Wikipedia: *Asymmetrisches Kryptosystem.* URL: http://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem (Abgerufen am 26.11.2004), 2004.

[Wik04b] Wikipedia: *Hash-Funktion.* URL: http://de.wikipedia.org/wiki/Hash-Funktion (Abgerufen am 26.11.2004), 2004.

[Zus] *Bundesgesetz über die Zustellung behördlicher Dokumente (Zustellgesetz - ZustG), BGBl. Nr. 200/1982 idF: BGBl. I Nr. 10/2004.*