Die Bürgerkarte – Ein Ass im Ärmel?

Funktionen, Voraussetzungen und Einsatzmöglichkeiten

Bei den kommenden ÖH-Wahlen im Mai 2009 sollen die Studierenden an österreichischen Hochschulen ihre Vertreter auch elektronisch via *E-Voting* – also über das Internet (`www.oeh-wahl.gv.at`) – wählen können. Darüber hinaus können seit 2001 in Österreich immer mehr Amtswege auch online erledigt werden. Notwendige Voraussetzung dafür ist die sogenannte Bürgerkarte – ein Teilbereich der österreichischen E-Government[1)]-Strategie.

E-Government in Österreich

„Der Startschuss für E-Government im Rahmen einer kooperativen Zusammenarbeit in Österreich ist im Jahr 1998 gefallen. Die Task-Force ‚E-Austria' mit den führenden Experten Österreichs empfahl 2001 ein ‚IKT[2)]-Board' einzurichten, welches die rechtlichen und technischen Voraussetzungen schaffen sowie die Planung und Entwicklung von E-Government-Lösungen zwischen Bund, Ländern und Gemeinden koordinieren sollte."[3)]

Die österreichischen E-Government-Aktivitäten sind im Laufe der Zeit durch politische Initiativen der Europäischen Union beeinflusst worden. Dazu zählten z.B. *eEurope 2002*[4)] sowie *eEurope2005: Eine Informationsgesellschaft für alle*[5)]. In Österreich ist im Jahr 2003 die *E-Government-Offensive 2003* mit dem Ziel gestartet worden, Österreich in Bezug auf E-Government in das europäische Spitzenfeld zu bringen und eine Position unter den besten fünf EU-Staaten zu sichern.

Darüber hinaus gab es seitens der österreichischen Bundesregierung das Bestreben, **Verwaltungsabläufe bürgerfreundlicher zu gestalten** bzw. die Effizienz des Verwaltungsapparates zu steigern. Ein weiterer Schritt war daher die Gründung der *Plattform Digitales Österreich* (PDÖ) im Jahr 2005. Diese Plattform nimmt seither für die österreichische Bundesregierung eine Koordinierungs- bzw. Strategieentwicklungsfunktion im Hinblick auf E-Government ein. Abbildung 1 zeigt, aus welchen Bausteinen – rechtlich, technisch und organisatorisch – sich die österreichische E-Government-Strategie zusammensetzt, darunter auch der Strategiebaustein *Bürgerkarte*.

Was ist die Bürgerkarte?

Bei der Bürgerkarte handelt es sich nicht um eine Karte im eigentlichen Sinne, d.h. sie ist weder ein Blatt Papier, noch ein Stück Plastik, sondern genau genommen eine Bürgerkarten**funktion**. Um elektronische Behördendienste (siehe *Einsatzmöglichkeiten der Bürgerkarte* im Kasten auf Seite 23) über das Internet in Anspruch nehmen zu können, benötigt man eine Art **elektronischen Ausweis**, durch den die Identität des/der Benutzers/Benutzerin festgestellt werden kann. Die Bürgerkartenfunktion stellt zu diesem Zweck ein **Signatur-Zertifikat** zur Verfügung, welches die Identifizierung und Authentifizierung des Benutzers ermöglicht (siehe *Elektronische Signaturen – Ein kleiner Einblick in Technik & Recht* auf Seite 25).

Abb. 1: Teilbereiche der österreichischen E-Government-Strategie
(Quelle: *Behörden im Netz – Das österreichische E-Government ABC*, 2008, Seite 12)

Damit man die Bürgerkartenfunktion verwenden kann, benötigt man ein **Speichermedium** – eine Karte –, auf deren Chip das Signatur-Zertifikat gespeichert ist. Dafür kann man z. B. die e-card der Sozialversicherung oder auch die Bankomatkarte (Maestro) verwenden[6].

Weiters benötigt man:

- einen **Computer mit Internetzugang**
- die auf diesem Computer installierte, aktuelle **Bürgerkartensoftware** oder Online-Bürgerkartenumgebung (BKU) (`www.buergerkarte.at/de/voraussetzungen/software.html`) sowie
- ein **Kartenlesegerät** (`www.buergerkarte.at/de/voraussetzungen/kartenleser.html`)

© sxu.hu; Wikipedia

Was kann die Bürgerkarte?

Die Bürgerkarte verfügt über mehrere Features. Eine ihrer wichtigsten Funktionen ist die sogenannte **digitale Signatur**, mit deren Hilfe es möglich ist, Dokumente elektronisch zu unterschreiben. Gerade dieser Anwendungsfall unterstützt das Konzept des E-Governments, Amtswege bürgerfreundlich und zugleich effizient auf elektronischem Wege erledigen zu können.

Zusätzlich zur digitalen Signatur kann man auch den privaten elektronischen Schriftverkehr **verschlüsseln**. In diesem Fall wäre ausschließlich der Empfänger einer Nachricht in der Lage, diese auch wieder zu entschlüsseln. Um Nachrichten oder Dokumente selber verschlüsseln zu können, muss man im Besitz eines privaten Schlüssels samt Zertifikat sein, welcher in das Signatur- oder E-Mail-Programm importiert werden muss.
Anmerkung: Wer die Bürgerkartenfunktion auf der e-card gespeichert hat, kann damit gegenwärtig keine E-Mails verschlüsseln, da die gängigen E-Mail-Programme die von der e-card verwendeten Verschlüsselungsverfahren („elliptische Kurven") noch nicht unterstützen.[7]

Eine weitere Funktion ist die Möglichkeit, stellvertretend für andere Personen Rechtsgeschäfte im Rahmen einer **elektronischen Vollmacht**[8] zu erledigen. An dieser Stelle sei noch darauf hingewiesen, dass man mit einer sogenannten eps-Onlineüberweisung (*e-payment standard*)[9] auch **elektronisch bezahlen** kann.

Wie aktiviert man die Bürgerkarte?

Im Wesentlichen gibt es zwei Möglichkeiten: Entweder aktiviert man die Bürgerkarte online, oder man lässt die Aktivierung bei einer Registrierungsstelle durchführen. Abhängig davon, welche Chipkarte man für die Verwendung als Bürgerkarte einsetzen möchte, werden im Folgenden die gängigsten Aktivierungsmöglichkeiten der Bürgerkarte auf der e-card bzw. der Bankomatkarte (Maestro) näher beschrieben.

Informationen zur Aktivierung alternativer Chipkarten erhalten Sie unter `www.buergerkarte.at/de/aktivieren/anbieter.html` bzw. beim jeweiligen Kartenanbieter.

Onlineaktivierung der e-card

Für die Onlineaktivierung müssen Sie die Bürgerkartensoftware installiert und das Kartenlesegerät inklusive installierter Treiber mit eingesteckter e-card an den Computer angeschlossen haben.

Mit vorhandenen Zugangsdaten zu FinanzOnline

1. Rufen Sie die Webseite `https://finanzonline.bmf.gv.at/` auf.
2. Loggen Sie sich mit Ihrer Zugangskennung ein.
3. Klicken Sie auf den Button *e-card jetzt aktivieren*.
4. Folgen Sie den Anweisungen auf dem Bildschirm.

1) Unter E-Government versteht man im weiteren Sinn die Vereinfachung und Durchführung von Prozessen zur Information, Kommunikation und Transaktion innerhalb und zwischen staatlichen, kommunalen und sonstigen behördlichen Institutionen sowie zwischen diesen Institutionen und Bürgern bzw. Unternehmen durch den Einsatz von Informations- und Kommunikationstechniken (vgl. `http://de.wikipedia.org/wiki/E-Government`).

2) IKT = Information, Kommunikation, Transaktion

3) siehe Broschüre *Behörden im Netz – Das österreichische E-Government ABC*, Seite 20 (`www.digitales.oesterreich.gv.at/DocView.axd?CobId=27782`)

4) `http://europa.eu/scadplus/leg/de/lvb/l24226a.htm`

5) `http://europa.eu/scadplus/leg/de/lvb/l24226.htm`

6) Weitere Karten, die möglich sind, siehe `www.buergerkarte.at/de/aktivieren/anbieter.html`

7) `www.a-sit.at/de/dokumente_publikationen/flyer/email_sign.php#Mails`

8) siehe `https://vollmachten.stammzahlenregister.gv.at/mandates/`

9) `https://www.bmf.gv.at/EGovernment/EZahlungsverkehrder_2565/_start.htm`

Ohne Zugangsdaten zu FinanzOnline

1. Rufen Sie die Webseite `https://www.a-trust.at/e-card/` auf.
2. Lesen Sie die Informationen genau durch. Beachten Sie, dass für die Registrierung die e-card in das angeschlossene Kartenlesegerät eingesteckt sein muss!
3. Klicken Sie auf den Button *Weiter zur Online-Aktivierung*.
4. Folgen Sie den Anweisungen auf dem Bildschirm.
5. Wählen Sie abschließend den Punkt *RSa Brief bestellen* aus (der Aktivierungscode wird Ihnen via RSa-Brief in wenigen Tagen zugestellt).
6. Nach dem Erhalt des RSa-Briefes rufen Sie nochmals die Seite `https://www.a-trust.at/e-card/` auf.
7. Schließen Sie die Onlineaktivierung durch Eingabe des Aktivierungscodes ab.

Bitte beachten Sie, dass bei der Freischaltung der Bürgerkarte über FinanzOnline in den Browsereinstellungen Cookies erlaubt sein müssen.

Persönliche Aktivierung der e-card

Registrierungsstelle in Ihrer Nähe

1. Rufen Sie die Webseite `https://www.a-trust.at/e-card/rafinder.aspx` auf.
2. Suchen Sie eine Registrierungsstelle in Ihrer Nähe.
3. Beachten Sie auf der Seite die Hinweise bezüglich einer Terminvereinbarung.
4. Suchen Sie die Registrierungsstelle persönlich auf und nehmen Sie Ihre e-card sowie einen amtlichen Lichtbildausweis mit.

Nur für Studierende

Aktion studi.gv.at

Bis Juni 2009 bietet studi.gv.at allen Studierenden die Möglichkeit, die Bürgerkartenfunktion auf der e-card kostenlos zu aktivieren: Die ersten 10.000 Studierenden, die an dieser Aktion teilnehmen, erhalten ein kostenloses Kartenlesegerät (Klasse 1)[1)].

1. Rufen Sie die Webseite `http://studi.gv.at/termine` auf.
2. Suchen Sie sich einen passenden Termin (weiter unten auf der Seite) oder kontaktieren Sie einen Tutor.
3. Nehmen Sie zum Termin Ihre e-card (diese muss noch mindestens sechs Monate gültig sein) sowie einen amtlichen Lichtbildausweis mit.

studi.gv.at
help4students

1) Bitte beachten Sie hierzu den Abschnitt *Der Kartenleser macht´s* auf Seite 31.

Persönliche Aktivierung der Bankomatkarte

Achtung: Informieren Sie sich auf der Webseite Ihrer Bank über mögliche Kosten!

1. Rufen Sie die Webseite `www.a-trust.at/registrierung/product_search.asp` auf.
2. Folgen Sie den Anweisungen auf dem Bildschirm.
3. Suchen Sie eine Registrierungsstelle in Ihrer Nähe.
4. Beachten Sie die Hinweise zur Terminvereinbarung.
5. Sofern Ihre Personenbindung noch nicht bei der Registrierung aktiviert wurde, können Sie das online unter `www.a-trust.at/zmrservice` nachholen.
6. Folgen Sie den Anweisungen auf dem Bildschirm.

Wo kann ich die Bürgerkarte praktisch einsetzen?

Natürlich stellt sich nun die berechtigte Frage, worin die Vorteile in der Freischaltung einer Bürgerkarte liegen, bzw. welche Services damit in Anspruch genommen werden können. Einsatzmöglichkeiten der Bürgerkarte sind:

- Onlineerledigung von Amtswegen
- Elektronische Zustellung von Bescheiden
- Ausstellung elektronischer Rechnungen
- Rechtsgültige elektronische Unterschrift in der Privatwirtschaft
- Identität für elektronische Geschäfte
- E-Banking
- Verschlüsselung von E-Mails und Dateien
- Bürgerkarte als Ausweis

Ausführliche Informationen dazu finden Sie unter `http://help.gv.at` (*Startseite Bürger/innen – Leben in Österreich – E-Government*) bzw. im nebenstehenden Kasten.

Achtung: Viele Anwendungen lassen sich nur mit installierter Bürgerkartensoftware, angeschlossenem Kartenlesegerät inklusive installierter Treiber und eingesteckter Chipkarte sowie entsprechenden Browsereinstellungen (Cookies, Java, Stammzertifikate) ausführen, anderenfalls erscheint eine Fehlermeldung im Browser (*Sichere Verbindung fehlgeschlagen*).

Sicherheit – was ist zu beachten?

Der Zugriff auf Funktionen der Bürgerkarte ist durch die sogenannte **Karten-PIN** (4-stellig) geschützt. Damit kann ein Auslesen der persönlichen Daten von der Karte verhindert werden. Für die Anwendung der digitalen Signatur benötigt man die sogenannte **Signatur-PIN** (6-stellig).

EINSATZMÖGLICHKEITEN DER BÜRGERKARTE

Ausführliche Informationen unter **http://help.gv.at**
(*Startseite (Bürger/innen) » Leben in Österreich » E-Government*)

Onlineerledigung von Amtswegen

Arbeitnehmerveranlagung, Einkommenssteuererklärung	https://finanzonline.bmf.gv.at
Antrag auf Studienbeihilfe	www.stipendium.at (unter *Studienförderung – Formulare*)
Meldebestätigung	https://meldung.cio.gv.at/egovMB/
Strafregisterbescheinigung („*Leumundszeugnis*“)	https://apps.egiz.gv.at/strafregister/
Sozialversicherungsdatenauszug (Versicherungszeiten)	www.sozialversicherung.gv.at (unter *Online Services*)
Grunddaten zur Krankenversicherung (Sozialversicherungsträger, Mitversicherung)	www.sozialversicherung.gv.at (unter *Online Services*)
Beitragskonto der Sozialversicherung	www.sozialversicherung.gv.at (unter *Online Services*)
Leistungsinformation – LIVE online (persönliches Leistungsblatt)	www.sozialversicherung.gv.at (unter *Online Services*)
Antrag auf Kinderbetreuungsgeld	www.sozialversicherung.gv.at (unter *Service – Für Versicherte – Formulare*)
Abfrage Pensionskonto	www.sozialversicherung.gv.at (unter *Online Services*)
Diebstahlanzeige (nur Tatort Wien)	http://help.gv.at (Suchfunktion verwenden)
Meldung von Kinderpornographie	http://help.gv.at (Suchfunktion verwenden)
Meldung von NS-Wiederbetätigung	http://help.gv.at (Suchfunktion verwenden)
Meldung von Umweltkriminalität	http://help.gv.at (Suchfunktion verwenden)

Elektronische Zustellung von Bescheiden

Bescheide elektronisch erhalten (eingeschriebene RSa-Briefe)	www.zustellung.gv.at https://www.meinbrief.at

E-Banking

Beachten Sie bitte hierzu die Website ihrer Bank. Informieren Sie sich dort auch über eventuelle Kosten.

Identitätsnachweis (Bürgerkarte als Ausweis)

E-Voting (z.B. ÖH-Wahl)	www.oeh-wahl.gv.at

Verschlüsselung von Dateien

Dokumente ver-/entschlüsseln	http://demo.a-sit.at

Rechtsgültige elektronische Unterschrift in der Privatwirtschaft

Verträge elektronisch signieren	Tools unter www.buergerkarte.at/de/pdf-signieren/

Achtung: Viele Anwendungen lassen sich nur mit installierter Bürgerkartensoftware, angeschlossenem Kartenlesegerät inklusive installierter Treiber und eingesteckter Chipkarte sowie entsprechenden Browsereinstellungen (Cookies, Java, Stammzertifikate) ausführen

Bei der **Verwendung der PINs** sollten Sie unbedingt daran denken, dass

- die Länge der PIN von der Art der Anwendung bzw. vom notwendigen Schutz abhängt. Deshalb sollten Sie bei der Auswahl der PINs auch **keine trivialen Kombinationen** (wie z.B. Geburtsdatum) verwenden.
- die PINs immer **unbeobachtet eingegeben** werden sollten.
- die PINs immer **geheim gehalten** werden sollten.
- die **gemeinsame Aufbewahrung** der PINs mit der Karte **vermieden** werden sollte.

Diese Vorgangsweise ist notwendig, da es sich bei der Verwendung der PINs um eine **rechtlich verbindliche Unterschrift** handelt, d.h. die Verwendung der qualifizierten Signatur in Kombination mit der Signatur-PIN ist einer eigenhändigen Unterschrift gleichgestellt (laut Signaturgesetz sind allerdings einige Ausnahmen wie z. B. beim Testament vorgesehen)!

Fazit

Die Verwendung der Bürgerkarte im Rahmen von E-Government hat für den/die Benutzer/-in gegenüber dem klassischen Behördenweg einige Vorteile, z. B. können:

- Behördenwege zeit- und ortsunabhängig online erledigt werden.
- Wegzeiten sowie Zeitverlust durch Warten etc. vermieden werden.
- Benutzer/-innen von E-Government-Services sich im Vorfeld eines Behördenweges Aufwand bei der Informationssuche (Zuständigkeiten, Öffnungszeiten, Standort, Verkehrsverbindung etc.) ersparen.
- Dokumente direkt in elektronischer Form an andere Behörden weitergeleitet werden (z. B. Meldezettel zur Beantragung eines Visums an Botschaften).

Wie bereits beschrieben, ist für die Verwendung der Bürgerkarte ein Kartenlesegerät erforderlich. Bitte beachten Sie in diesem Zusammenhang die **Hinweise zur sicheren Verwendung von Kartenlesegeräten** im Artikel *Endlich sicher mit der Chipkarte?* auf Seite 28.

Wolfgang Walzer

SB-Terminals an der Universität Wien mit Kartenlesegeräten ausgestattet

Die an der Universität Wien installierten SB-Terminals werden für die kommende ÖH-Wahl im Mai 2009 mit Chipkartenlesegeräten ausgestattet, damit die Studierenden alternativ zur Papierwahl an der elektronischen Wahl teilnehmen können. Die SB-Terminals sind an folgenden Standorten verfügbar:

Standort	Anzahl
UZA II Althanstraße 14 Im Bereich der Portierloge	**2**
UZA II Althanstraße 14 Vor Hörsaal 6	**2**
Gebäudekomplex Gymnasiumstraße/Franz-Klein-Gasse Im Neubau im Bereich der Eingangshalle	**2**
Universitätscampus / Hörsaalzentrum Im Erdgeschoss im Bereich der EDV-Räume	**2**
Universitätssportzentrum (USZ) Auf der Schmelz 6 Im Bereich der Eingangshalle	**1**
Universitätssportzentrum (USZ) Auf der Schmelz 6a Im 3. Stock im Bereich der Bibliotheksgarderobe	**1**
Hauptgebäude Dr.-Karl-Lueger-Ring 1, Rechter Seiteneingang Hof IV, Stiege 6, Tiefparterre, gegenüber Referat Studentpoint	**5**
BWZ, Bauteil II Brünner Straße 72 Im Eingangsbereich	**2**

Informationen

Informationen zur Bürgerkarte finden Sie unter `www.buergerkarte.at`, insbesondere zu folgenden Themen:

- **FAQs**, z.B. *Was tun bei Verlust der Karte?* `www.buergerkarte.at/de/hilfe/faq.html`
- **Spezifikationen und technische Dokumentationen** `www.buergerkarte.at/de/spezifikation/`
- **Datenschutz und Sicherheit** `www.buergerkarte.at/de/datenschutz-sicherheit/`

Informationen zum Thema E-Government erhalten Sie im Internet unter:

- Plattform Digitales Österreich `www.digitales.oesterreich.gv.at`

Bitte machen Sie Ihr Zeichen

Elektronische Signaturen – ein kleiner Einblick in Technik & Recht

Der elektronischen Signatur kommt im Rahmen des Bürgerkartenkonzepts eine wesentliche Bedeutung zu, ermöglicht sie doch die **Identifizierung** und **Authentifizierung** des Bürgers, der/die mit der Behörde, Bank etc. elektronisch in Kontakt tritt. Der folgende Beitrag skizziert das Funktionsprinzip der digitalen Signatur und gibt einen kurzen Überblick über die aktuellen rechtlichen Rahmenbedingungen.

Die elektronische Signatur

Das österreichische Signaturgesetz definiert eine elektronische Signatur als *elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung, also der Feststellung der Identität des Signators, dienen.*

Die hier vorliegende Begriffsbestimmung wurde technologieneutral gestaltet und erlaubt verschiedenste technische Realisierungen. In der Praxis werden elektronische Signaturen jedoch zumeist als sogenannte **digitale Signaturen unter Verwendung von asymmetrischen Kryptoalgorithmen und Zertifikaten** verwirklicht.

Funktionsprinzip

Das Funktionsprinzip der digitalen Signatur soll im Folgenden anhand eines Beispiels veranschaulicht werden (siehe Abb. 1). Wir nehmen hierfür an, dass Absenderin A Empfänger B ein Dokument übermittelt und mittels digitaler Signatur den Nachweis erbringen möchte, dass

1. das Dokument tatsächlich von ihr stammt
   = **Authentizität des Kommunikationspartners**

2. der Inhalt des Dokuments nicht verändert wurde
   = **Integrität der Daten**.

Absenderin A ...

... erstellt ein Dokument und signiert dieses digital: Mit Hilfe eines mathematischen Verfahrens (*Hash-Verfahren*) wird aus den Zeichen des Dokuments eine Prüfsumme (der sogenannte *Hash-Wert*) ermittelt – quasi ein „elektronischer Fingerabdruck". Diese Prüfsumme wird nun mit dem privaten Schlüssel der Absenderin A verschlüsselt. Der private Schlüssel ist dabei ausschließlich der Signaturschlüsselinhaberin, also Absenderin A, zugänglich. Das Ergebnis dieser Verschlüsselung ist die digitale Signatur.

weiter auf Seite 27

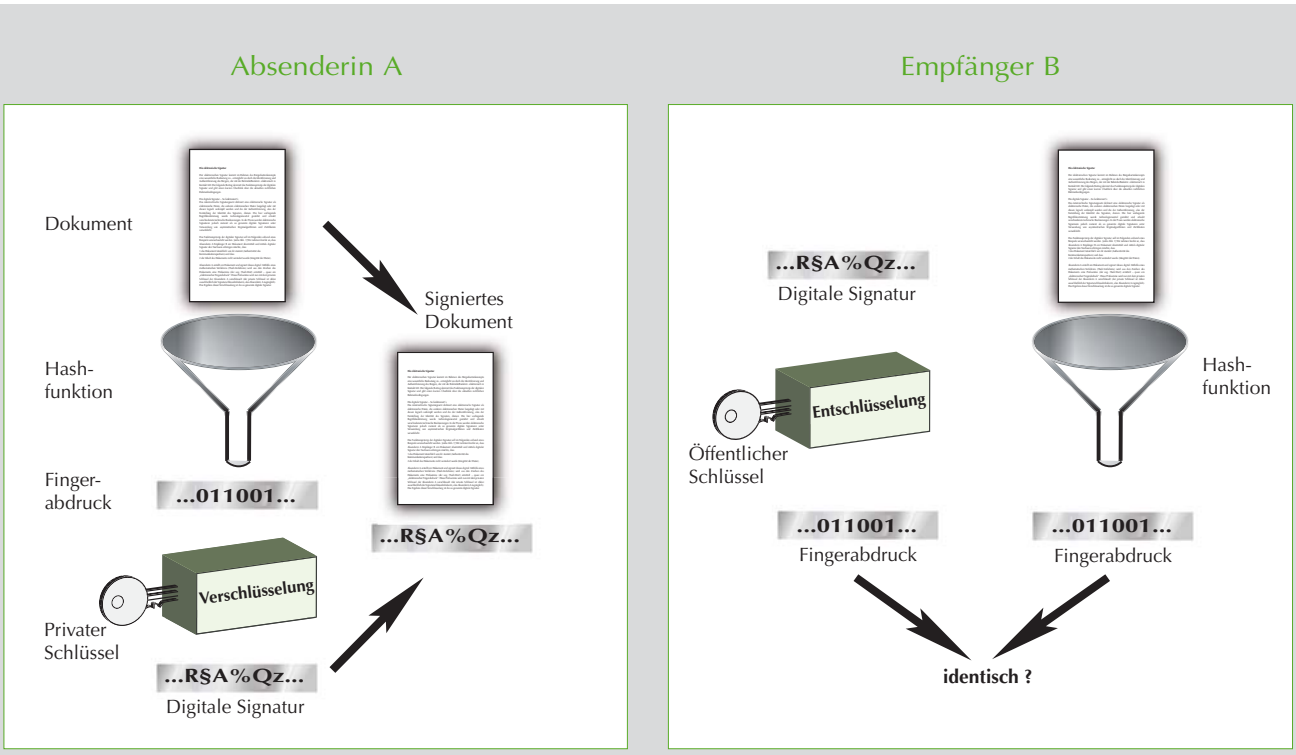

Abb. 1: Funktionsprinzip der digitalen Signatur

ELEKTRONISCHE SIGNATUREN – ARTENVIELFALT

Im Rahmen der EU hat man sich im Jahr 1999 auf gemeinschaftliche Rahmenbedingungen für elektronische Signaturen geeinigt. Die Umsetzung der EU-Signaturrichtlinie erfolgte in Österreich mit 1.1.2000 durch das Signaturgesetz (SigG). Dieses gibt den rechtlichen Rahmen für die Erstellung und Verwendung von elektronischen Signaturen vor. Allerdings gab es am SigG diverse Kritikpunkte, die jedoch mit der umfangreichen Novellierung 2007 weitgehend entschärft wurden. Das aktuelle SigG kennt verschiedene Ausprägungen von elektronischen Signaturen. Diese Ausprägungen unterscheiden sich zum Teil wesentlich hinsichtlich ihrer Sicherheitsanforderungen sowie ihrer Bedeutung im Rechtsverkehr.

a) Die (einfache) elektronische Signatur
beruht auf einem (einfachen) Zertifikat. Als solches gilt laut SigG eine elektronische Bescheinigung, mit der Signaturprüfdaten einer bestimmten Person zugeordnet werden und deren Identität bestätigt wird. Im Gegensatz zu einem qualifizierten Zertifikat sind die Anforderungen an den ZDA (Zertifizierungsdiensteanbieter) hier nicht besonders hoch – es besteht somit eine geringere Sicherheit, dass die Zertifikatsvergabe ordnungsgemäß ablief und die Angaben im Zertifikat korrekt sind. Dennoch können einfache elektronische Signaturen vor Gericht nicht als Beweismittel ausgeschlossen werden.

b) Die qualifizierte elektronische Signatur (vormals auch als „sichere“ Signatur bezeichnet)
ist nach dem österreichischen Signaturgesetz eine elektronische Signatur,

- die ausschließlich dem Signator zugeordnet ist,
- die Identifizierung des Signators ermöglicht (und somit eine Registrierung des Signators bei der Zertifikatsausstellung erfordert),
- mit Mitteln erstellt wird, die der Signator unter seiner alleinigen Kontrolle halten kann (womit zum Ausdruck gebracht wird, dass auch ausreichende Schutzmaßnahmen erforderlich sind) und
- die mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass jede nachträgliche Veränderung der Daten festgestellt werden kann (d.h. den Einsatz eines geeigneten Hash-Verfahrens notwendig macht).

Zudem muss die qualifizierte Signatur auf einem qualifizierten Zertifikat beruhen und unter Verwendung von technischen Komponenten und Verfahren erstellt werden, die den Sicherheitsanforderungen des SigG und der auf seiner Grundlage ergangenen Verordnungen entsprechen. Auf Basis dieser Definition ergeben sich für die qualifizierte Signatur hohe Qualitätsanforderungen an die zur Signaturerstellung verwendeten Hard- und Software-Signaturprodukte.

Die qualifizierte elektronische Signatur erfüllt als einzige das rechtliche Erfordernis einer eigenhändigen Unterschrift.[1)] Damit kann das zivilrechtliche Formerfordernis der Schriftform auch durch Beisetzung einer qualifizierten Signatur zu einem elektronischen Dokument erfüllt werden. Praktisch (nicht Juristendeutsch) heißt das: Mit einer Bürgerkarte mit qualifizierter elektronischer Signatur können z.B. auch privatrechtliche Verträge elektronisch unterschrieben werden.

c) Die fortgeschrittene elektronische Signatur
In die Novellierung des SigG 2007 wurde zudem der EU-konforme Begriff der „fortgeschrittenen elektronischen Signatur“ aufgenommen. Von der qualifizierten elektronischen Signatur unterscheidet sich diese Signatur einzig dadurch, dass die Signatur nicht notwendigerweise auf einem qualifizierten Zertifikat beruht und nicht notwendigerweise mit einer sicheren Signaturerstellungseinheit erstellt werden muss. Die fortgeschrittene Signatur ist besonders im Wirtschaftsbereich verbreitet (z.B. zum Schutz von Geschäftsdokumenten vor Veränderung und zur Identifikation des Erstellers eines Geschäftsdokumentes).

d) Die Verwaltungssignatur
Das E-Government-Gesetz kennt neben den im SigG definierten elektronischen Signaturen zwei Sonderformen: die Amtssignatur (auf Seite der Behörde) sowie die Verwaltungssignatur (auf Seite des Bürgers). Die Verwaltungssignatur war eine Übergangslösung. Bis Ende 2007 wurde die Bürgerkartenfunktion auf die e-card mit einem Verwaltungssignatur-Zertifikat aufgebracht. Verwaltungssignaturen mussten nicht alle Bedingungen der Erzeugung und Speicherung von Signaturerstellungsdaten der qualifizierten Signatur erfüllen und nicht notwendigerweise auf einem qualifizierten Zertifikat beruhen. Bereits ausgestellte Verwaltungssignaturen dürfen nun bis zum Ablauf des Zertifikats, längstens jedoch bis zum 31. Dezember 2012 im Rahmen der Bürgerkartenfunktion gleichgestellt mit qualifizierten Signaturen verwendet werden. Bürgerkarten-Neuausstellungen *müssen* jedoch auf einem qualifizierten Zertifikat beruhen.

1) Hier wurden einige Ausnahmen definiert: siehe § 4 Besondere Rechtswirkungen

Empfänger B ...

... wird das Dokument im Klartext plus der erstellten digitalen Signatur übermittelt. Die digitale Signatur kann nun verifiziert werden, indem die verschlüsselte Prüfsumme mit dem öffentlichen Schlüssel, der allen Kommunikationspartnern zur Verfügung steht, entschlüsselt wird und mit der (nach dem gleichen Verfahren gebildeten) Prüfsumme des Klartextdokuments verglichen wird.

Schon die kleinste Veränderung an dem Dokument – wie das Einfügen eines einzelnen Buchstabens oder das Ersetzen eines Beistriches durch einen Punkt – wäre dann anhand der abweichenden Prüfsumme (dem „Fingerabdruck") erkennbar. Wenn die beiden Werte übereinstimmen, weiß Empfänger B, dass der Inhalt des Dokuments nicht verfälscht wurde und dass das Dokument der-/demjenigen zugerechnet werden kann, die/der Zugriff auf den privaten Schlüssel hat.

Zertifikate

Empfänger B kann daraus aber noch nicht ableiten, dass es sich bei der signierenden Person tatsächlich um die z.B. im Absenderfeld angegebene Frau Muster handelt. Um der digitalen Signatur vertrauen zu können, muss eine korrekte Zuordnung des öffentlichen Schlüssels zu einer Person sichergestellt werden. Diese Zuordnung erfolgt mittels sogenannter Zertifikate. Durch ein Zertifikat können Anwender/-innen den öffentlichen Schlüssel einer Identität zuordnen.

Die Ausstellung und Administration von Zertifikaten sollte dabei von einer vertrauenswürdigen Instanz übernommen werden, damit die Anwender/-innen sich auf die in den Zertifikaten enthaltenen Informationen verlassen können. In der Regel obliegt dies den sogenannten Zertifizierungsdiensteanbietern (im Folgenden kurz ZDA genannt).

Die Aufgaben der ZDA werden im Signaturgesetz geregelt. Im Wesentlichen sind dies:

- **Identifizierung** einer Person (beispielsweise mittels Vorlage eines Ausweises)
- Bestätigung der eindeutigen Zuordnung eines öffentlichen Schlüssels zu dieser Person durch ein **Zertifikat**
- **Erzeugung des privaten Schlüssels** sowie
- Bereitstellung eines öffentlich zugänglichen **Verzeichnisdienstes**, über den die Empfänger digital signierter Dokumente die Zertifikate nachprüfen können.

Schlüsselpaar

Wie bereits erwähnt, kommen bei asymmetrischen Algorithmen zwei Schlüssel zum Einsatz. Diese bilden ein Schlüsselpaar und stehen zueinander in einem mathematischen Verhältnis. Aufgrund dieser mathematischen Verknüpfung kann der **öffentliche Schlüssel** zur eindeutigen Identifizierung des zugehörigen privaten Schlüssels verwendet werden. Der **private Schlüssel** darf aber nach dem jeweiligen Stand der Technik nicht aus dem öffentlichen Schlüssel errechenbar sein. Um dies zu gewährleisten, bedient man sich komplexer mathematischer Verfahren (RSA, DSA, ECC, ...)

Hinweis: Zurzeit wird die Verschlüsselungsmethode, die die e-card verwendet (elliptische Kurven) von den gängigen E-Mail-Klienten nicht unterstützt. Wenn die Bürgerkartenfunktion auf der e-card gespeichert ist, können damit gegenwärtig keine E-Mails verschlüsselt werden.

Aber auch andere Aspekte sind für die Sicherheit des Verfahrens entscheidend, wie etwa die sichere Verwahrung und Geheimhaltung des privaten Schlüssels. So gilt es sicherzustellen, dass tatsächlich nur der Inhaber Zugriff auf den privaten Schlüssel hat. Dies kann mittels verschiedenster technischer Lösungen realisiert werden, wobei der Sicherheitslevel je nach Lösung variiert.

Als derzeit sicherstes Medium für die Aufbewahrung des privaten Schlüssels gelten Chipkarten. Das sind im Wesentlichen spezielle Plastikkarten, auf die ein Chip aufgebracht wurde. Der private Schlüssel wird dabei auf den Kartenchip gespeichert und ist in der Regel mit einem Passwort bzw. einer PIN geschützt (z.B. die Bürgerkartenfunktion auf der e-card).

Ebenso wichtig wie die technischen Maßnahmen zur Sicherung des privaten Schlüssels ist freilich auch der verantwortungsvolle und umsichtige Umgang der Benutzer/-innen mit ihrem Passwort bzw. PIN (siehe hierzu Artikel *Endlich sicher mit der Chipkarte?* auf Seite 28).

Die Signaturen auf der Bürgerkarte

Wird die Bürgerkarte z. B. auf der e-card oder auf der Bankomatkarte aktiviert, so werden immer zwei Zertifikate aufgebracht. d.h. es stehen auch zwei Signaturen zur Verfügung:

- eine **qualifizierte Signatur** (mit qualifiziertem Zertifikat), die mit dem **6-stelligen Signatur-PIN** ausgelöst wird (z. B. für Antragstellungen im elektronischen Amtsverkehr, als elektronische Unterschrift etc.; siehe Artikel *Die Bürgerkarte – Ein Ass im Ärmel?* auf Seite 20)
- sowie eine **einfache Signatur** (mit einfachem Zertifikat), die mit dem **4-stelligen Geheimhaltungs- oder auch Karten-PIN** (Termini synonym) ausgelöst wird (z. B. für Anwendungen, die keine eigenhändige Unterschrift erfordern oder zur Verschlüsselung).

Michaela Bociurko

Endlich sicher mit der Chipkarte?

Die Unterschrift auf dem Papier kann man aber auch fälschen …

Die Chipkarte oder Smart Card als Träger des privaten Schlüssels für den Einsatz bei elektronischen Signaturen (siehe *Bitte machen Sie Ihr Zeichen* auf Seite 25) hat einerseits große Hoffnungen geweckt: Der Computer als Kommunikationsmedium wird sicher, Identitäten werden zweifelsfrei festgestellt und vertrauliche Nachrichten kann nur der Empfänger einsehen. Andererseits stellt sich die Frage, ob diese Technologie den Erwartungen auch gerecht werden kann: Wie trägt die Chipkarte dazu bei, die Kommunikation zwischen Sender und Empfänger über das Internet zu sichern, welche Bedrohungen gilt es dabei abzuwehren und wie kann man diesen begegnen?

Kommunikation unter der Lupe

Nehmen wir einen klassischen Amtsweg als Beispiel und betrachten zunächst modellhaft den Kommunikationsfluss eines **persönlichen Gesprächs**:

Der Bürger, die Informationsquelle, spricht einen Antrag aus und sendet damit eine Nachricht. Diese wird durch einen Kanal transportiert, in diesem Fall die Luft, in der sich die Schallwellen ausbreiten. Die Amtsperson hört – empfängt – die Nachricht, die damit an ihrem Ziel angelangt ist (Abb. 1).

Abb. 1: Modell zwischenmenschlicher Kommunikation am Beispiel des klassischen Amtsweges

Mitunter wird dieser Kommunikationsfluss gestört, wenn beispielsweise ein rücksichtloser Handynutzer in sein Mobiltelefon brüllt, als müsste er ohne technische Hilfe seiner Tante Mizzi etwas quer durch Wien zurufen. Der Mensch hat gelernt, solche Nebengeräusche bei der Kommunikation durch eine Feedback-Schleife zu korrigieren: Die Empfängerin fragt im Zweifel nach und wiederholt die wesentlichen Angaben, um sicherzugehen, dass sie alles richtig verstanden hat. Damit wird die Gefahr einer verfälschten Nachricht gemindert. Da der Rückkanal genau wie der Vorwärtskanal aufgebaut ist, gehen wir nicht weiter darauf ein.

Was ändert sich an diesem Modell, wenn das Internet ins Spiel kommt? Die Kommunikation erfolgt nicht mehr direkt (Face-to-Face), sondern über technische Hilfsmittel bestehend aus Hardware und Software wie Computer, Datenleitungen, Webanwendungen und Datenbanken. Man könnte also meinen, der elektronische Antrag sei lediglich die Fortsetzung des Parteienverkehrs mit digitalen Mitteln. Doch es hat sich eine neue Gefahrenzone eingeschlichen: Der Kanal hat sich verändert. Anstelle von Schallwellen ist das Internet getreten – von Sender und Empfänger schwer kontrollierbar, da der eigenen Kontrolle entrückt, dennoch will man sich darauf verlassen können. Dieser Kanal muss also irgendwie gesichert werden (Abb. 2).

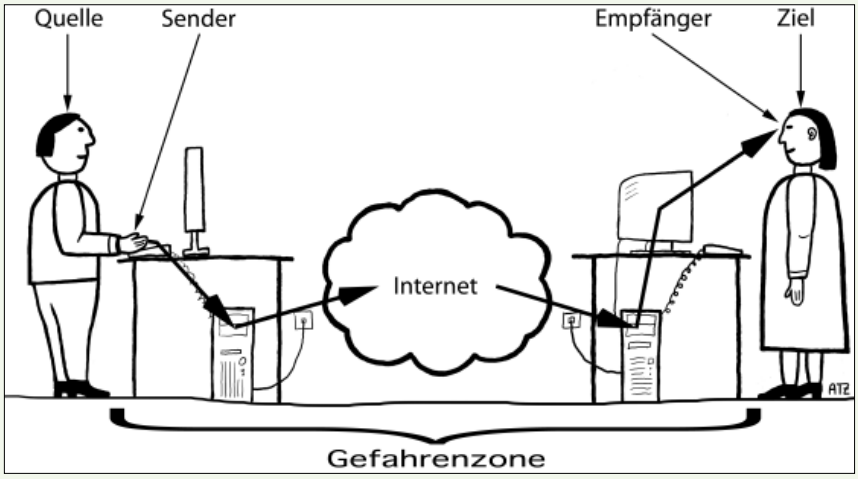

Abb. 2: Modell computervermittelter Kommunikation: Auf der Graphik ist das Internet mitten im Kommunikationskanal als Wolke dargestellt. Dieses Bild ist unter Netzwerkern üblich, da es zum Ausdruck bringt, dass keinerlei Annahmen über seine Struktur oder Eigenschaften, über die Betreiber der Knoten und deren Zuverlässigkeit getroffen werden: Es wird als Transportweg ohne Garantien behandelt.

Sicher, aber wovor?

Wir haben bereits die Möglichkeit von Kommunikationsstörungen gestreift, dabei aber nicht in Betracht gezogen, dass jemand vorsätzlich und böswillig in den Kommunikationsprozess eingreifen könnte, um

- zu verhindern, dass eine Nachricht ihr Ziel erreicht (*Verletzung der Verfügbarkeit*).
- eine Nachricht zu verändern (*Verletzung der Integrität*).
- eine eigene Nachricht als die von jemand anderen auszugeben (*Verletzung der Authentizität*).
- eine vertrauliche Nachricht zu belauschen (*Verletzung der Vertraulichkeit*).

Bei der computervermittelten Kommunikation wiegen diese Bedrohungen um einiges schwerer als bei der zwischenmenschlichen Kommunikation. Will man jemanden daran hindern, persönlich einen Antrag bei einem Amt einzubringen, braucht es gewisse Gewalt und zieht zudem einiges Aufsehen auf die eigene Person. Unseres Wissens hat auch noch niemand – schon gar nicht erfolgreich – versucht, durch ständiges, lautes Wiederholen seines Namens eine Amtsperson dazu zu bringen, ein Dokument versehentlich auf einen anderen Namen auszustellen. Störungen bei der Face-to-Face-Kommunikation erkennen die Beteiligten meistens sofort, so dass es nur schwer möglich ist, eine Nachricht unbemerkt zu verfälschen.

Eine *Denial-of-Service*-Attacke[1] im Internet lässt sich dagegen relativ einfach mit gemieteten Botnets preiswert, anonym und über längere Zeit, an mehreren Orten gleichzeitig durchführen.

Im normalen Leben beweisen wir unsere Identität mit einem Lichtbildausweis oder mit unserer eigenhändigen Unterschrift. Beide Verfahren sind keineswegs kugelsicher, aber die Wahrscheinlichkeit, bei Missbrauch gefasst zu werden, ist groß. Man kann auch kaum ständig zum selben Amt gehen und jedes Mal einen auf einen anderen Namen lautenden Ausweis vorlegen. Das würde irgendwann auffallen. Massenhaft verschiedene Unterschriften zu fälschen ist im realen Leben ebenfalls höchst aufwendig. Ein Computer dagegen wird selten misstrauisch, solange er stur sein vorgegebenes Programm abarbeitet.

Auch mit der Gefahr, dass jemand eine Unterhaltung belauscht, wissen wir umzugehen. Jeder kennt die gelben Diskretionszonenstreifen zwei Meter vor dem Schalter und kann einschätzen, wie wirksam oder unwirksam diese Maßnahme ist. Bei Computer, Internet etc. weiß man nicht so genau, was diese tun oder wie man sie daran hindern könnte. Bei der elektronischen Übertragung kann sich jede Komponente in dem langen Stille-Post-Spiel zwischen Sender und Empfänger unbemerkt und effektiv als Fälscherwerkstatt betätigen.

Gefahr aus dem Internet

Betrachten wir zunächst das Internet als Gefahrenzone. Damit die Nachricht auf ihrer Reise von einem Computer zum andern nicht abgehört oder verändert werden kann, setzt man Verfahren wie Verschlüsseln und Signieren ein. Dabei kann man an zumindest zwei Ebenen ansetzen, wobei im Prinzip dieselben Schutzmechanismen verwendet werden:

- Man kann die Verbindung selbst sichern, indem jedes einzelne Datenpaket signiert und verschlüsselt wird. Das ist vor allem bei interaktiven Anwendungen sinnvoll, wenn etwa Webformulare auszufüllen sind.

- Man kann die Nachricht signieren und verschlüsseln, bevor sie übertragen wird. Das ist besonders dann angebracht, wenn eine Nachricht auch nach der Übertragung aufbewahrt bzw. weitervermittelt wird, z.B. E-Mail oder Dokumente.

Im Internetalltag hat sich dafür die Technik der Secure Sockets Layer (SSL) bzw. Transport Layer Security (TLS)[2]

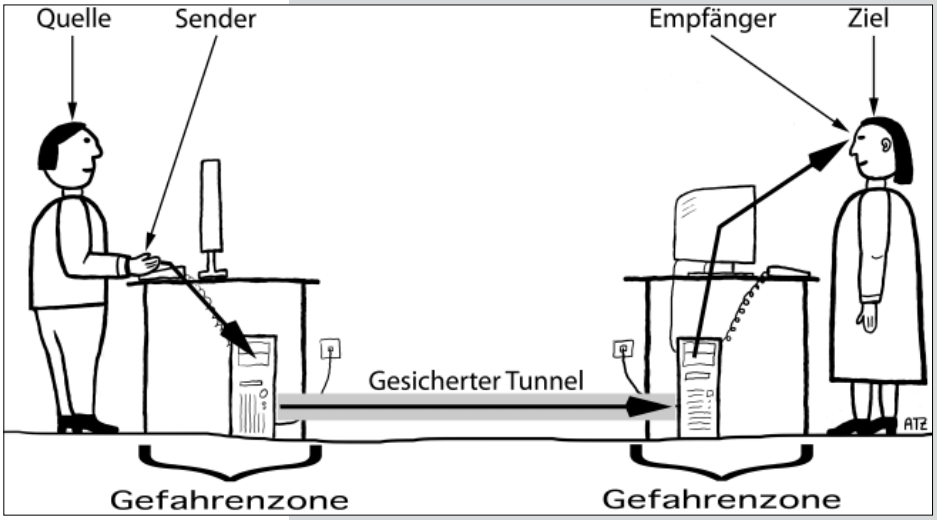

Abb. 3: Modell einer sicheren Verbindung mit SSL/TLS.

als allgegenwärtiger Standard zur Sicherung interaktiver Anwendungen durchgesetzt, z. B. bei webbasierten Anwendungen des Zentralen Informatikdienstes, Online-Shops, Telebanking usw. Da die Verbindung insgesamt gesichert wird, entsteht unabhängig von der Netzstruktur ein direkter Kanal zwischen zwei Computern. Zum Identitätsnachweis nennt der/die User/-in – vor Abhören geschützt – dem Server ein vorher vereinbartes Passwort (siehe Abb. 3).

Leider lassen sich Computernutzer/-innen erstaunlich leicht dazu überreden, ihr Passwort Betrügern zuzusenden oder auf deren Webseiten bekannt zu geben, da sie in eine Phishing-Falle[3] geraten sind.

1) Bei DoS-Attacken wird ein Server gezielt mit so vielen Anfragen bombardiert, dass das System die Aufgaben nicht mehr bewältigen kann und im schlimmsten Fall zusammenbricht.

2) siehe *Was ist TLS/SSL?* in comment 06/2, Seite 43 (`http://comment.univie.ac.at/06-2/43/`)

3) siehe *Phishing – Bitte nicht anbeißen!* in `comment 06/2`, Seite 37 (`http://comment.univie.ac.at/06-2/37/`)

Das kommt mir kryptisch vor

Kryptografische Verfahren[4] wie z. B. die digitale Signatur (siehe *Bitte machen Sie Ihr Zeichen* auf Seite 25) sind, wenn sie sachkundig umgesetzt werden, auf mittlere Sicht außerordentlich sicher. Diese defensive Formulierung weist bereits auf Schwachstellen hin:

- Detailfehler machen häufig die ganze Kryptografie hinfällig. So hat erst im Oktober 2008 bei Debian-Linux ein kaputter Zufallszahlengenerator dazu geführt, dass die vermeintlich unerratbaren Schlüssel stets aus einer kleinen, leicht durchprobierbaren Menge ausgewählt wurden. Unter Ausnutzung dieser Sicherheitslücke[5] konnte der private Schlüssel eines großen US-Einzelhandelsunternehmens errechnet und damit ein erfolgreicher Man-in-the-Middle-Angriff[6] auf eine HTTPS-Verbindung ausgeführt werden.[7]

- Fortschritte der Hardware, vor allem aber der Kryptoanalyse, bewirken, dass Algorithmen gewissermaßen altern. Dagegen helfen auch längere Schlüssel nur sehr begrenzt. Für kein heute als unangreifbar geltendes Verfahren gibt es einen mathematischen Sicherheitsbeweis.[8]

Zeitgenössische Kryptographie ist also für den Schutz von Passwörtern beim Einloggen in die Webanwendung und zum Unterschreiben der Steuererklärung hervorragend geeignet: Die Steuererklärung für das Vorjahr wird in einem Jahrzehnt niemand mehr fälschen wollen und Ihre Passwörter haben Sie bis dahin hoffentlich auch schon geändert.

Skepsis ist aber angebracht, ob Kryptographie auch für langfristig sensible Angelegenheiten ausreichenden Schutz bietet. Es ist damit zu rechnen, dass eine heute abgefangene verschlüsselte Nachricht in ein paar Jahrzehnten leicht gelesen werden kann. Interaktive Anwendungen können naturgemäß nicht rückwirkend gefälscht werden, wenn die Sicherungsalgorithmen geknackt sind, Nachrichten und ihre digitale Unterschrift lassen sich dann aber perfekt fälschen. Die Vorstellung hat etwas Gruseliges, dass jemand z. B. im Jahr 2030 eine mit heuer datierte, rechtsgültig vom Bundespräsidenten unterschriebene Urkunde herstellen könnte, laut der er die Hofburg und Schloss Schönbrunn um je einen Euro erworben hat. Die Frage ist weniger, ob so etwas möglich wird, als vielmehr wann.

Kurzfristig liegt es näher, nicht die Kryptographie anzugreifen, sondern den Schlüssel und den Mechanismus, der die Verschlüsselung bzw. Signatur durchführt. Im Kommunikationsmodell wird es deutlich, dort sind die Computer an den Enden des Kanals immer noch als Gefahrenzone ausgewiesen.

Sicherheit der Endgeräte

Was nutzt es, wenn das Internet dank Kryptographie völlig sicher Daten transportiert, von denen man aber gar nichts weiß? Die Frage mag überraschen – aber wer kann schon behaupten, nie gegen die unerklärlichen Eigenmächtigkeiten eines Computerprogramms gekämpft zu haben? Dahinter steckt noch gar keine böse Absicht. Wenn jedoch aus Unachtsamkeit durch Internetdownloads, E-Mail-Verkehr oder Datenübertragung von USB-Sticks und Netzwerk-Shares etc. Schadsoftware auf Computer nichtsahnender Anwender/-innen gelangt, wird für einen Angreifer prinzipiell alles möglich:

- Tastatureingaben abfangen
- Programme ausführen
- den Bildschirminhalt einsehen oder verändern
- beliebige Dateien von der Festplatte auslesen oder verändern
- Programme oder das Betriebssystem manipulieren
- angeschlossene Geräte wie Mikrophon oder Webcam mitbenutzen
- vorhandene Netzwerkanschlüsse missbrauchen

Mit solchem virtuellen Ungeziefer wird der gesamte kryptografische Schutz ausgehebelt: Man könnte jede beliebige Kommunikation des PC-Eigentümers fälschen, abhören oder auch vollständig generieren, noch bevor sie in den sicheren Tunnel gelangt.

Ist das nicht etwas weit hergeholt? Leider nein. Infizierte PCs haben sich in den vergangenen zehn Jahren zum Hauptproblem der Computersicherheit schlechthin gemausert. Tag für Tag entdeckt der ZID infizierte Rechner im Universitätsnetz, und niemand weiß, wie viele unerkannt bleiben.

Die typische Malware ist Massenware, hergestellt von einer eigenen (Schatten-) Industrie. Das Glück im Unglück: Irgendjemandem unter den Millionen Betroffenen fällt eine derart verbreitete Malware meistens auf, der sie dann den Herstellern von Antivirenprogrammen übermittelt, die ihre Virensignaturen entsprechend erweitern. So kann man sich wenigstens vor älterer Malware schützen.

Gefährlich, wenn auch selten, sind jene Tierchen, die extra für eine Einzelperson oder eine verhältnismäßig kleine Gruppe gezüchtet wurden: Die Virenscanner erkennen sie nicht. Individuelle Angriffe dieser Art erfordern einen gewissen Aufwand – es muss also jemand ein Interesse daran haben, genau diesen Rechner zu infiltrieren, wobei das Interesse auch mittelbar sein kann, etwa um einen anderen Rechner im selben Netz sozusagen „von innen“ anzugreifen.

Der Rolle der Chipkarte

Passwort und Verschlüsselung bzw. Signatur stoßen an ihre Grenzen, wenn der/die Anwender/-in das Passwort ausplaudert oder wenn der Rechner von Malware übernommen wird. Kann die Chipkarte auch in diesen Fällen für Sicherheit sorgen?

Zunächst zu ihrer Funktionsweise: Eine Chipkarte ist ein kleiner Computer mit Prozessor, Speicher, Betriebssystem und Software. Auf ihr ist der geheime Schlüssel der Anwenderin/des Anwenders gespeichert und wird auch nie nach außen übertragen. Stattdessen kann die Karte selbst digitale Unterschriften erzeugen und regelt dabei die Zugriffsberechtigung: Solange ihr nicht der richtige PIN gegeben wird, verweigert sie die Arbeit. Mehr noch: nach mehrfacher Fehleingabe sperrt sie sich völlig.

Was der Chipkarte jedoch fehlt, sind Tastatur und Bildschirm sowie die Verbindung zum Internet. Deswegen muss sie in einen Kartenleser, ein Gerät mit Steckvorrichtung und Anschlusskabel (meist USB), eingesteckt werden, der die Verbindung mit dem Computer bzw. mit einer auf dem Computer gespeicherten Software herstellt. Diese Anwendung – bei der Bürgerkarte ist das die Bürgerkartenumgebung (BKU), sonst der Webbrowser bzw. ein Plugin oder Applet darin – stellt eine Nachricht am Bildschirm dar, ersucht um Freigabe durch den User und sendet dann einen Fingerabdruck des Dokuments zwecks Signatur zur Chipkarte. Die Anwendung sendet die Signatur dann gemeinsam mit dem Dokument zum Amt. Die Karte sichert nicht die Verbindung als solche, sondern kann lediglich Nachrichten bzw. Dokumente unterschreiben, und aus der Sicht des Antrags für einen sicheren Kanal zum Amtscomputer sorgen (Abb. 5).

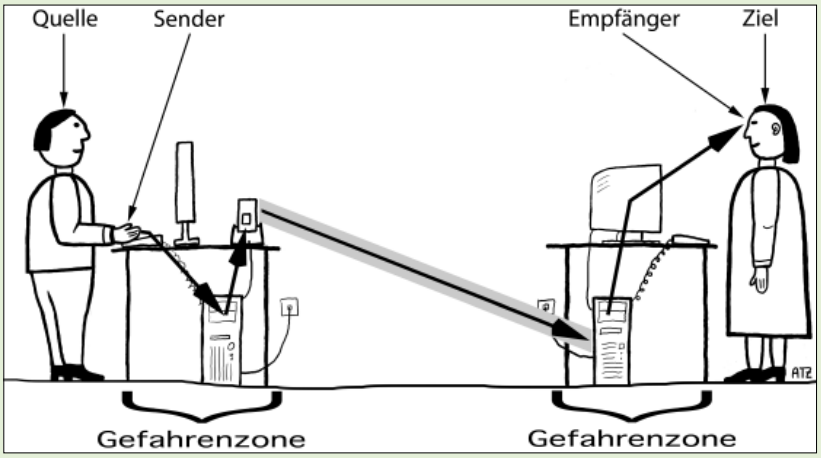

Abb. 5: Mittels Chipkarte gesicherte Kommunikation zwischen Sender und Empfänger

Der Kartenleser macht's

Rekapitulieren wir, was eine Malware im Computer anrichten kann: Sie kann Tastatureingaben belauschen oder simulieren, Bildschirminhalte manipulieren, angeschlossene Geräte sowie das Netzwerk nutzen. Das reicht, um den Schutz der Chipkarte auszuhebeln: So kann die Eingabe der PIN belauscht werden, beliebige Dokumente unter Vorweisen der erlauschten PIN durch die Chipkarte signiert werden, das Ergebnis an Ämter, Banken etc. gesendet werden. So schnell kann es gehen, und schon hat der Antragsteller, der vielleicht nur einen Meldezettel unterschreiben wollte, auch noch sein Ferienhaus der mexikanischen Drogenmafia überschrieben.

Bringt also die Chipkarte keinerlei Sicherheitsgewinn gegenüber der kartenlosen TLS/SSL-Sicherung, wenn man dem eigenen Rechner nicht trauen kann? Diese Schlussfolgerung ist verfrüht. Denn nicht die Chipkarte ist unsicher, sondern die Eingabe der PIN über den Computer.

Um diese Sicherheitslücke zu schließen, gibt es Kartenlesegeräte der Klasse 2[9]. Sie verfügen über eine eigene Tastatur zur Eingabe der PIN oder sind in die PC-Tastatur integriert, jedenfalls können sie den PIN ohne Umweg über den PC direkt zur Karte senden, ein Belauschen durch Malware ist also ausgeschlossen. Diese Geräte sind zwar wesentlich teurer als die einfachen Kartenleser, sicherheitstechnisch sind sie den einfachen Geräten jedoch in jedem Fall vorzuziehen.

Eines ist noch ganz besonders wichtig: Sofern sie einen Kartenleser der Klasse 2 besitzen, geben Sie die Karten-PIN auch stets auf der Tastatur des Kartenlesers ein und achten Sie darauf, dass Sie dabei nicht beobachtet werden. Warum wir so darauf herumreiten? Dass der Kartenleser eine Tastatur hat, verhindert nicht, dass der PIN auch über den PC eingegeben werden kann. Wenn Sie nur ein einziges Mal den PIN über den PC eingegeben haben und die Malware hat es mitbekommen, kann diese die Karte wie beim Klasse 1-Gerät unbegrenzt missbrauchen.

4) siehe *Grundbegriffe der Kryptographie* in comment 00/3, Seite 20 (`http://comment.univie.ac.at/00-3/20/`)

5) siehe `www.debian.org/security/2008/dsa-1571/`

6) Man-in-the-Middle-Angriff: Methode, bei denen sich ein Angreifer in Rechnernetzen in eine Kommunikationsverbindung einklinkt und damit vollständige Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern hat.

7) *Können wir TLS/SSL noch vertrauen?* Vortrag von Alexander Talos-Zens, 38. ACOnet TBPG-Treffen zugleich 18. ArgeSecur-Treffen, Wien. 7. Oktober 2008

8) siehe Ferguson; Schneier (2003) *Practical Cryptography*, Seite 344

9) Die Einteilung der Kartenlesegeräte in Klassen entspringt der Spezifikation des Home-Banking Computer Interface (HBCI) des deutschen Zentralen Kreditausschusses (ZKA). Je höher die Klasse, umso sicherer ist das Gerät.

„Kein Achilles ohne Ferse“,

sagt der Volksmund, und der Kartenleser Klasse 2 ist da keine Ausnahme: Am anfangs beschriebenen Kommunikationsmodell hat sich ja durch die PIN-Eingabe über die Tastatur des Kartenlesers nichts geändert. Noch immer wird die Information, die zu signieren ist, vom Computer zur Chipkarte geschickt. Das wirft eine beängstigende Frage auf: Wer garantiert mir, dass, was am Bildschirm zu sehen ist, auch das ist, was die Chipkarte nach (sicherer) Eingabe des PIN signiert?

Leider niemand. Die Bürgerkartenumgebung steht auf verlorenem Posten: Software ist wie ein Theaterstück, das erst dadurch zum Leben erwacht, dass es jemand aufführt. Wenn der Regisseur beschließt, dass Gretchen mit einem langhaarigen Studenten durchbrennt und Faust den Pakt mit dem Teufel storniert und stattdessen lieber nackt im Mondschein baden geht, kann ihn das Stück nicht daran hindern. Auch die Bürgerkartenumgebung kann einen korrupten Computer nicht hindern, etwas anderes zu tun, als sie vorschreibt. Und die Karte ist ebenfalls machtlos: Sie weiß ja nicht, was sie zu signieren glaubt.

Kartenlesegeräte der Sicherheitsklassen 1 bis 3

© Bastian Fuhrmann, Wikipedia

Kartenleser Klasse 1: ohne Tastatur und Display

© Steffen Heinz, Wikipedia

Kartenleser Klasse 2: mit Tastatur, ohne Display

© Journey234, Wikipedia

Kartenleser Klasse 3: mit Tastatur und Display

Um diesem Problem vorzubeugen, gibt es Kartenleser der Klasse 3. Diese verfügen über ein eigenes Display, das zumindest die wichtigsten Eckdaten anzeigen könnte, bevor die Signatur ausgelöst wird. „Könnte“ steht im irrealen Konjunktiv, die Bürgerkartenumgebung kann von derartigen Lesegeräten nämlich keinen Gebrauch machen.

Ein letzter Punkt noch: Wenn die Chipkarte ein Computer ist, kann man sie nicht ebenfalls hacken oder mit Malware infizieren? Unmöglich ist das zwar nicht, aber es ist ungleich schwieriger als beim PC, weil die Kartensoftware nicht im Entferntesten so leistungsfähig und komplex wie bei einem PC ist. Auch gegen ein Auslesen unter dem Elektronenmikroskop und gegen sogenannte Side Channel Attacks, in denen Schwankungen im Stromverbrauch oder im Timing-Verhalten ausgenutzt werden, hat man sich einiges einfallen lassen. Allerdings kann ein Fehler in der Karte, falls einer entdeckt wird, nur durch Kartentausch und nicht durch einfaches Internetupdate korrigiert werden.

Ähnliches gilt auch für den Kartenleser. In der Tat ist die Strategie, wichtige Operationen aus dem unsicheren PC herauszulösen und in vermeintlich kontrollierbarere Umgebungen zu transferieren, nicht ohne Nebeneffekte: Die Zahl der Beteiligten und damit die Zahl der möglichen Angriffsszenarien wächst exponentiell: Karte gegen Kartenleser, Kartenbetriebssystem gegen Kartenanwendung, verschiedene Kartenanwendungen gegeneinander etc. Darauf einzugehen, würde den Rahmen dieses Artikels sprengen.

Na und? Die Unterschrift oder den Ausweis kann man auch fälschen!

Auch herkömmliche, nichttechnische Verfahren sind alles andere als unfehlbar und die Verbrechensstatistik beweist, dass Low-tech- oder No-tech-Betrug regelmäßig vorkommen und dass die Gesellschaft gelernt hat, damit umzugehen. Die E-isierung erfordert aber ein radikal höheres Maß an Sicherheit, weil die Gefahrenqualität eine völlig andere ist:

- Ein Tatwerkzeug – ein PC – ist problemlos, unauffällig und ohne großen finanziellen Aufwand zu beschaffen.
- Die physische Anwesenheit oder Nähe des Täters ist in der Regel nicht erforderlich, es gibt keinerlei Fingerabdrücke, DNA-Spuren etc.
- Die Gefahr, erwischt zu werden, ist verschwindend gering.
- Computer sind naiv und werden aus Erfahrung nicht klüger, Menschen schon.
- Computer haben weder Launen noch unterschiedlichen Charakter, ihr Verhalten ist plan- und vorhersehbar.
- Massenhafte und automatisierte Begehung ist mit geringem Aufwand möglich.
- Manipulationen an Daten sind durch ihren hohen Abstraktionsgrad nicht nachweisbar.

E-Government, E-Commerce und dergleichen stehen, was die Sicherheit betrifft, einer gewaltigen Herausforderung gegenüber. Selbst der vorsichtige Laie hat keine Chance, zu erkennen oder im Ernstfall nachzuweisen, dass sein Computer „hereingelegt“ worden ist. Das bedeutet eine Risikoverschiebung zu Ungunsten des Bürgers (bzw. Konsumenten). Dazu muss einerseits durch vertrauenswür-

dige Sicherheitsmaßnahmen entgegengetreten werden, andererseits muss im Zweifelsfall dem Wort des Menschen mehr Glauben geschenkt werden, als einer Datenstruktur, so komplex sie sein mag.

Zusammenfassung

Bei E-Government und E-Commerce lassen sich die Gefahren des unsicheren Trägernetzes Internet leicht beherrschen, dafür stellt sich überraschenderweise der PC der Anwenderin/des Anwenders als entscheidender Schwachpunkt heraus, da er die Schnittstelle zwischen Mensch und Maschine bildet. Ist dessen Sicherheit nicht gewährleistet – und das ist sie letztlich nie –, greifen alle kryptographischen Maßnahmen ins Leere.

Wie virulent das Problem mit den von Spyware erschnüffelten Geheimcodes ist, illustriert ein Screenshot der Telebanking-Oberfläche der PSK: Hier wird als Alternative zur TAN-Eingabe per Tastatur vorgeschlagen, mit der Maus auf das Ziffernfeld zu klicken, weil das für neugierige Malware schwieriger zu erfassen ist. Diesen Aufwand unternehmen Banken deshalb, weil Spyware, die PINs und TANs ihrer Kunden erschnüffelt, zu einem realen Problem geworden ist.

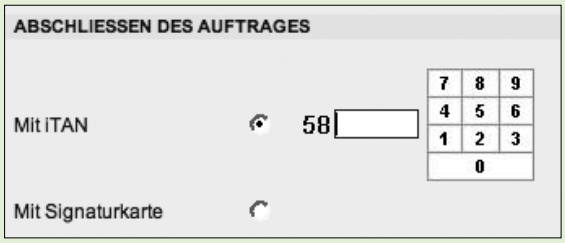

Abb. 6: Feld zur TAN-Eingabe bei Onlinebanking: Klicken der Ziffernfelder mit der Maus statt einer Tastatureingabe erschwert es Malware, Eingaben abzufangen.

Die Chipkarte vermag mangels Tastatur und Bildschirm das Schnittstellenproblem nicht zu lösen. Ihr Einsatz begrenzt bestenfalls den Zeitraum und den Ort, an dem ein Missbrauch stattfinden kann. Damit ist die Chipkarte ein wirksames Werkzeug gegen Phishing, kann aber nur bedingt etwas gegen Malware am PC ausrichten. Chipkarten sollten, wenn die Integrität der PCs auch nur im Entferntesten in Frage steht, nur mit Lesegeräten mit eigener Tastatur verwendet werden – gerade im Urlaub im Internetcafé.

Dem Sicherheitsgewinn stehen hohe Kosten und der Verlust der Möglichkeit, jederzeit und überall auf die geschützten Services zuzugreifen, gegenüber. Auf keinen Fall darf man aus den Augen verlieren, dass Chipkarten Computermissbrauch nicht gänzlich verhindern und daher muss rechtzeitig ein sozial verträglicher Ausgleich für diese Risiken vorgesehen werden.

Alexander Talos-Zens

Notizen

uniADSL endgültig eingestellt

Das Service uniADSL des ZID wurde endgültig eingestellt. Alle Zugänge, die nicht bis Ende April 2009 unter `https://data.univie.ac.at/adsl/` selbst gekündigt wurden bzw. zu einem anderen Provider gewechselt sind, werden vom ZID per Ende Mai 2009 bei der Telekom Austria gekündigt.

Beachten Sie auch unsere Informationen zur Auflassung von uniADSL im Artikel *Die Breitbandzugänge der Uni Wien werden aufgelassen* in comment 07/3, Seite 6 (`http://comment.univie.ac.at/07-3/6/`).

WLAN-Umstellung

Das WLAN-Service (kabellose Internetverbindung) und die kabelgebundenen Internetzugänge des ZID wurden mit 30. November 2008 umgestellt.

Neuerungen

- Das gesicherte WLAN-Netz Datentankstelle802.1X wird aufgelassen, da die Verschlüsselung nicht mehr den aktuellen Sicherheitsstandards entspricht. Statt dessen wird nur noch das **verschlüsselte** und international nutzbare WLAN-Netz **eduroam** angeboten.
- **Unverschlüsselt** steht das neue **u:connect**-Netz zur Verfügung. Die Authorisierung erfolgt nach erfolgreicher Verbindung über die Login-/Logout-Webseite. Alle anderen nicht sicheren WLAN-Netze (Datentankstelle, eduroamWeb) werden deaktiviert.
- Die **kabelgebundenen** Zugänge sind via **u:connect-wired** verfügbar und verwenden dieselbe Login-/Logout-Webmaske wie u:connect.

Bitte verwenden Sie vorzugweise das verschlüsselte Netz eduroam (Infos: `www.eduroam.at`).

Weitere Informationen, Anleitungen und WLAN-Standorte finden Sie unter:

`www.univie.ac.at/ZID/wlan/`

Bei Fragen oder Problemen steht Ihnen der Helpdesk des ZID zur Verfügung (4277 140 60; `www.univie.ac.at/ZID/helpdesk/`).