

Funktion „Bürgerkarte“

Mit der Funktion „Bürgerkarte“ können Behördenangelegenheiten erledigt werden. Unter anderem können Schusswaffen damit angemeldet und Meldungen im Vereinswesen abgegeben werden, von Anwendungen in der Finanzverwaltung ganz abgesehen.

Die Bürgerkarte ist eine Funktion, mit der ein bestehender Datenträger, etwa die E-Card oder das Handy, ausgestattet werden kann. Ihre rechtliche Grundlage hat die Bürgerkarte im E-Government-Gesetz, BGBl I 2004/10, zuletzt idF BGBl I 2010/111. § 4 E-GovG spricht in der Überschrift auch ausdrücklich von der Funktion Bürgerkarte.

Sie dient dem Nachweis der eindeutigen Identität eines Einschreiters und der Authentizität des elektronisch gestellten Anbringens in Verfahren, für die ein Auftraggeber des öffentlichen Bereichs eine für den Einsatz der Bürgerkarte taugliche technische Umgebung eingerichtet hat (Abs. 1). Der Definition nach (§ 2 Z 10 E-GovG) ist sie „eine logische Einheit, die unabhängig von ihrer technischen Umsetzung eine qualifizierte elektronische Signatur (§ 2 Z 3a des Signaturgesetzes – SigG, BGBl. I Nr. 190/1999) mit einer Personenbindung (§ 4 Abs. 2) und den zugehörigen Sicherheitsdaten und -funktionen sowie allenfalls mit Vollmachtsdaten verbindet“.

In der Praxis wird ein Datenträger elektronisch mit einer Person verbunden und in weiterer Folge ist, geschützt durch PIN oder Passwort, gewährleistet, dass nur diese Person die mit der Bürgerkarte verbundenen Anwendungen in Anspruch nimmt. Es handelt sich um einen Ausweis für die elektronische Welt – der allerdings noch weitere Möglichkeiten eröffnet. Die Sicherheit wird hergestellt durch Besitz (der Smart-Card, des Handys



Die Bürgerkartenfunktion ermöglicht elektronische Amtswege.

bzw. der übermittelten TANs) und Wissen (der PIN oder des Passwortes) – somit eine Zwei-Faktoren-Authentifizierung.

Verwendungsmöglichkeiten. Diese Anwendungen können zunächst darin bestehen, sich elektronisch auszuweisen (Identifizierung, Authentifizierung). Nach dieser Ausweiseleistung öffnen sich beispielsweise nur dem legitimen Benutzer offen stehende Datenbanken.

Man kann darüber hinaus auch elektronisch unterschreiben (signieren). Der Inhaber oder Empfänger eines solchen elektronisch übermittelten oder generierten Dokuments kann in zweierlei Hinsicht sicher sein: Erstens, dass dieses tatsächlich vom Unterzeichner (Signator) stammt, und zweitens, dass keine Veränderungen im Text erfolgt sind.

Zu diesem Zweck sind auf dem Datenträger (Smart-Card) bereits bei der Erzeugung zwei Schlüssel aufgebracht, der öffentliche und der private. Beide Schlüssel sind jeweils für sich sehr ho-

he Primzahlen. Während es technisch sehr leicht ist, Primzahlen miteinander zu multiplizieren, ist es mit vertretbarem Aufwand sehr schwer, das Produkt wieder in die beiden Faktoren zu zerlegen¹. Die einzige Möglichkeit hierzu ist, alle Teiler durchzuprobieren – und das kann auch leistungsstarke Rechner überfordern.

Die Unterschrift wird mit dem privaten Schlüssel geleistet. Wendet der Empfänger den ihm entweder bekannten oder bei der Registrierungsstelle aufliegenden öffentlichen Schlüssel des Signators an, kann er sicher sein, dass die Nachricht von diesem stammt.

Veränderungen im Text zu erkennen, wird technisch dadurch ermöglicht, dass von dem Dokument mit mathematischen Verfahren ein Zahlenwert errechnet wird. „Dieser Hash-Wert² kann, würde man ihn ausdrucken, durchaus eine A4-Seite füllen“, erklärt Michael Butz, MSc, Geschäftsführer der A-Trust GmbH. Jede nachträgliche Veränderung würde beim Empfänger einen anderen Hash-Wert ergeben und

damit eine Kompromittierung erkennbar werden. Diese Methode ist sogar sicherer als bei Papierdokumenten, an denen vorgenommene Änderungen wie Radierungen oder gefälschte Unterschriften mitunter nur kriminaltechnisch erkannt werden können. Oder wie will man beispielsweise erkennen, ob bei einem mehrseitigen Dokument Seiten ausgewechselt wurden?

Allerdings können nur Dokument-Formate auf diese Art signiert werden, die kein dynamisches Datum oder eine Weiß-auf-weiß-Darstellung erlauben. Word-Dokumente müssen somit in PDF- bzw. XML-Dateien oder JPG-Bilddateien umgewandelt werden.

Die Prüfung der Echtheit der Unterschrift sowie der Unverfälschtheit des Inhalts kann über die RTR-GmbH oder A-Trust durchgeführt werden. Über die URLs <https://pruefung.signatur.rtr.at/> bzw. <https://www.a-trust.at/Support/PDFVerifikation.aspx> muss das gesamte Dokument hochgeladen werden. Eine weitere Prüfmöglichkeit wird von IT-Solution unter <http://www.signaturpruefung.at/verifier> angeboten.

Auch E-Mails können als solche (und nicht nur mitgesendete Dokumente) signiert werden, allerdings nicht mit dem Handy und weniger rechtsverbindlich (keine qualifizierte Signatur).

Weiters können elektronische Zustelldienste wie www.meinbrief.at; www.postserver.at; www.sendstation.at in Anspruch genommen werden. Es ist auch möglich, Texte, Dokumente usw. zu



„A-Trust-Infoday“: Information über den derzeitigen Stand der elektronischen Signatur.

verschlüsseln. Der Verschlüsselnde verwendet hierzu seinen öffentlichen Schlüssel. Nun kann der Text nur mehr mit dem nur ihm bekannten oder dem Empfänger mitgeteilten privaten Schlüssel entschlüsselt werden.

Als Datenträger kommen die vom Hauptverband der Sozialversicherungsträger ausgestellten E-Cards in Betracht, nicht etwa der österreichische Personalausweis (wohl aber der von Liechtenstein), und auch nicht der Führerschein im Scheckkartenformat. Auch die verschiedensten Ausweise von Mitarbeitern (Dienstausweise) sind zumindest technisch geeignet, wenn sie als Chipkarten (Smart-Cards) ausgeführt sind. Der Inhaber muss damit rechnen, dass bei einem Ausscheiden aus dem Unternehmen der Mitarbeiterausweis entzogen wird und damit das Zertifikat nicht mehr benutzt werden kann.

Freischaltung (Aktivierung). Bei einer Aktivierung der Funktion „Bürgerkarte“ muss man mit der Registrierungsstelle und damit mit dem Zertifizierungsdiensteanbieter (ZDA, 3. Abschnitt

SigG; derzeit ist nur die *A-Trust GmbH* als ein solcher akkreditiert) in Kontakt treten. Der ZDA muss letztlich sicher sein, dass die von ihm ausgestellte Bestätigung, das Zertifikat, die richtige Person betrifft.

Bei der Freischaltung einer E-Card (oder ähnlicher Smart-Cards) liest der ZDA über die Bürgerkarten-Software den öffentlichen Schlüssel der Karte aus und verbindet ihn mit der Stammzahl. Diese wird ihm bei der Anfrage im *Zentralen Melderegister* geliefert, und zwar als Ergebnis einer Verschlüsselung der unverwechselbaren Melderegisterzahl (ZMR-Zahl; § 16 Abs. 4 MeldeG) mit kryptografischen Verfahren so, dass die Stammzahl auf die ZMR-Zahl nicht wieder rückführbar ist.

Durch diese Verbindung zwischen der Person und deren öffentlichem Schlüssel ist die Personenbindung (§ 4 Abs. 2 E-GovG) bewirkt; der Datenträger ist zur „Bürgerkarte“ geworden. Für nicht im ZMR enthaltene Personen wird eine Eintragung im Ergänzungsregister angelegt. Der öffentliche Schlüssel wird mit dem privaten Schlüssel des ZDA signiert und in seinem Verzeichnis-

dienst eingetragen sowie auf der Karte abgespeichert. Damit ist die Voraussetzung für das qualifizierte Zertifikat hergestellt, das rechtlich einer Unterschrift gleichgestellt ist.

Bei der Handy-Signatur wird eine Verbindung mit der Telefonnummer hergestellt. Damit bleibt die Funktion der Bürgerkarte auch erhalten, wenn die SIM-Karte in einem anderen Handy verwendet wird. Die Personenbindung wird beim Handy mit den anderen Daten am Hochsicherheitsserver des ZDA abgelegt.

Hat man eine aktivierte E-Card, können ein oder mehrere Handys ohne weitere Ausweisleistung online aktiviert werden³. Mit der Handy-Signatur kann man allerdings nur sich authentifizieren sowie signieren, nicht aber Inhalte verschlüsseln. Letztlich kann man auch auf dem Postweg eine Freischaltung herbeiführen⁴. Den Aktivierungscode erhält man durch einen an die Hauptmeldeadresse zugestellten RSA-Brief. Die eigenhändige Zustellung kommt dem Identitätsnachweis gleich (§ Abs. 1 Z 2 SigV).

Wer bereits bei Finanz-Online angemeldet ist, kann

seine E-Card über diese Einrichtung als Bürgerkarte aktivieren⁵. Die Bestätigung der Identität gegenüber dem ZDA wird von Finanz-Online übernommen.

Bei der Registrierung muss der Signator zwei Zahlenwerte festlegen, die die Schlüssel für die Verwendung der Funktion Bürgerkarte sind: den vierstelligen Karten-PIN (Geheimhaltungsschlüssel), der den Zugriff auf die Karte oder das Handy ermöglicht, und den sechsstelligen Signatur-PIN (Signatursschlüssel), der zur Leistung einer rechtsgültigen Unterschrift verwendet wird. Auch ein Widerrufspasswort wird festgelegt.

Als „Bürgerkartenumgebung“ (BKU) wird die Software bezeichnet, die zur Nutzung der Funktion Bürgerkarte benötigt wird. An Hardware braucht man bei der Handy-Signatur außer dem Handy weiter nichts mehr. Bei Verwendung einer Smart-Card werden ein Internet-Anschluss, ein Kartenleser samt Treiberprogramm sowie ein Programm aus der BKU benötigt. Derartige Programme stehen im Internet zum Herunterladen kostenlos zur Verfügung (www.buergerkarte.at;

www.a-trust.at). Kartenleser gibt es in 3 Klassen. Bei Lesern der Klasse 1, die etwa 7 Euro kosten, müssen die Passwörter im Computer eingegeben werden. Kartenleser der Klasse 2 (bei A-Trust 57,60 Euro) ermöglichen die Eingabe der PINs über die Tastatur des Lesers. Die Geheimzahlen verlassen in diesem Fall den Leser nicht und können daher nicht abgefangen werden. Kartenleser der Klasse 3 (ca. 80 Euro) – die von der Bürgerkarte noch nicht unterstützt werden – weisen zusätzlich ein Display auf, mit dem eine Endkontrolle des signierten Dokuments möglich ist. Dadurch wird eine unverfälschte Weitergabe des signierten Dokuments gewährleistet und verhindert, dass Schadprogramme eine verfälschte Wiedergabe am Bildschirm bewirken.

Die Firma *Cherry* bietet Tastaturen mit bereits eingebautem Kartenleser der Klasse 2 an. Zur Installation des Kartenlesers muss das Treiberprogramm geladen werden, üblicherweise durch Abruf aus dem Internet. Nach Installation der Anwendungsprogramme kann die Nutzung der vielfältigen Funktionen der Bürgerkarte beginnen.

Anwendungen. Bei den E-Government-Anwendungen wie help.gv.at kann man, wenn man nicht nur bloß informationshalber surft, sondern beispielsweise seine persönlichen Konten (Pensionskonto, Sozialversicherungszeiten u. a.) einsehen oder rechtsgültig Anträge (Arbeitnehmerveranlagung, Meldeauskunft, -bestätigung, Strafregisterbescheinigung, DVR-Abfrage u. a.)⁶ stellen will, in der Login-Box entscheiden, ob man sich mit Karte oder Handy identifizieren und in weiterer Folge rechtsgültige Erklärungen abgeben will. Einloggen mit



Rudolf Kemler: „In der Verwaltung hat sich die elektronische Signatur weitgehend durchgesetzt.“

dem Handy erfordert die Eingabe der Mobiltelefonnummer und des Passwortes, das man bei der Freischaltung selbst gewählt hat. Über den Button Identifizieren ist man dem System gegenüber ausgewiesen und erhält über SMS (im Inland kostenfrei) eine TAN, die fünf Minuten lang auf dem Display aufscheint. Durch Ablesen und Eintippen der TAN ist man dem System gegenüber als Person identifiziert.

Bei Verwendung einer Smart-Card als Bürgerkarte hat man die entsprechenden, bei der Registrierung selbst gewählten Passwörter in die entsprechenden Felder am Bildschirm einzugeben.

Die nach der Übergangsbestimmung des § 58 Abs. 2 WaffG erforderliche Registrierung von am 1. Oktober 2012 bereits im Besitz befindlichen Schusswaffen der Kategorie C, die bis zum 30. Juni 2014 zu erfolgen hat, kann auch mit Bürgerkarte im elektronischen Verkehr erfolgen, ohne dass ein Waffengewerbetreibender mit der Registrierung befasst werden muss.

Die an die Vereinsbehörde zu erstattenden Meldungen über die bestellten organischen Vertreter sowie jede Änderung der für Zustellungen an den Verein maßgeblichen Anschrift (§



Reinhard Posch: „Österreich ist bei E-Government im europäischen Raum nach wie vor an der Spitze.“

14 Abs. 2 und 3 VerG), die Änderungen im ZVR bewirken, können durch einen vom Verein der Behörde namhaft gemachten organischen Vertreter unter Verwendung der Bürgerkarte für die Behörde vorgenommen werden (§ 19 Abs. 6 VerG).

Nach Maßgabe der technischen Möglichkeiten können Meldeauskünfte auch im Datenfernverkehr aus dem Zentralen Melderegister unter Verwendung der Bürgerkarte verlangt und erteilt werden (§ 18 Abs. 1a MeldeG).

E-Tresor. *A-Trust*, der einzige Anbieter qualifizierter Zertifikate in Österreich, stellt mit dem *E-Tresor Basic* (www.e-tresor.at) den Nutzern der Bürgerkarte kostenlos einen gesicherten Datenspeicher von zwei Gigabyte zur Verfügung. Erst für ein darüber hinausgehendes Speichervolumen muss bezahlt werden. Dann kann auch eine Umgebung für mehrere Benutzer mit Ordnerstruktur und individueller Rechteverwaltung eingerichtet werden.

Der *E-Tresor* kann zur sicheren Ablage von wichtigen Dokumenten verwendet werden, etwa Personaldokumente, Zeugnisse, medizinische Befunde, Verträge, Versicherungspolizzen,

Bankdaten und Rechnungen. Sicherheit bedeutet nicht nur die Sicherheit vor fremdem Zugriff (der Login kann nur durch Identifizierung mit Karte oder Handy erfolgen), sondern auch vor Verlust oder Beschädigung. Die Ablage kann unter den schon eingerichteten Registern erfolgen. Elektronische Dokumente können direkt abgespeichert werden. Papierdokumente müssen, um in die elektronische Form übergeführt zu werden, gescannt werden. Besonders wichtige Dokumente kann man von einem Notar elektronisch signieren lassen, wodurch sie zu beglaubigten Kopien werden.

Der Tresor kann über die bei der Anmeldung vergebene E-Mail-Adresse beschickt werden – und damit auch von Personen, denen der Berechtigte die zur Nutzung des Tresors ihm mitgeteilte E-Mail-Adresse weitergegeben hat. Die Dokumente gelangen in die Inbox, von der aus sie verwaltet, bearbeitet und abgelegt werden. Auch direktes Hochladen von einem Datenträger (Festplatte, USB-Stick u. a.) ist möglich. Dokumente können direkt im Tresor signiert und von dort per E-Mail verschickt werden. Mit der „Unterschriftenmappe“ werden Vorgänge des täglichen Lebens virtuell abgebildet.

Fertig bearbeitete Dokumente können in der Show-Box abgelegt werden. Von dort können sie, allenfalls zeitlich eingeschränkt, von Empfängern heruntergeladen werden, denen das hierfür vom Berechtigten individuell bestimmte Passwort bekannt gegeben wurde.

Der übrige Inhalt des Tresors bleibt ihnen nach wie vor verschlossen. Durch die Einrichtung des *E-Tresors* sind wichtige Dokumente weltweit rund um die Uhr verfügbar – auf Rechnern, die sich alle in Österreich



Franz Lang: „Es muss der Sicherheitsaspekt stärker in den Vordergrund gerückt werden.“

befinden und hier verwaltet werden.

Beim A-Trust Infoday am 24. Oktober 2012 in Wien wurden die etwa 320 Teilnehmer eingehend über den derzeitigen Stand der elektronischen Signatur informiert. In Diskussionsrunden wurden neue Entwicklungen erörtert.

„Österreich ist, was das E-Government betrifft, im europäischen Raum nach wie vor an der Spitze“, betonte der CIO der Bundesregierung, Univ.-Prof. Dr. DI Reinhard Posch. „Über 200 Anwendungen stehen dem Bürger über *help.gv.at* zur Verfügung“.

Im Verwaltungsbereich (E-Government) habe sich die elektronische Signatur weitgehend durchgesetzt, sagte Rudolf Kemler, seit 1. November 2012 Vorstandsvorsitzender der Staatsholding ÖIAG. Der Nutzen liege hierbei durch Verwaltungsvereinfachung beim Staat.

In der Wirtschaft hingegen bestehe noch Nachholbedarf. Ihr gegenüber müsse als Nutzen der Sicherheitsaspekt stärker in den Vordergrund gerückt werden. Die Wichtigkeit dieses Aspekts angesichts der steigenden Cyber-Kriminalität betonte General Franz Lang, Direk-



Hermann Feiner: „Personenstandsregister der Standesämter wird als ZPR zentral elektronisch geführt.“

tor des Bundeskriminalamts. Sektionschef Hermann Feiner, Leiter der Sektion IV (Service und Kontrolle) im Innenministerium, kündigte an, dass ab 1. April 2013 das bisher von den Standesämtern geführte Personenstandsregister als ZPR zentral elektronisch geführt wird. Dadurch kann bei Amtswegen die Vorlage von Geburts- und sonstigen Personenstandsurkunden (Staatsbürgerschaftsnachweis) entfallen.

Die entsprechenden Informationen stehen den Behörden online zur Verfügung. Mitte 2013 werde es möglich werden, mit der Autorisierung durch die Bürgerkarte Anzeigen elektronisch zu erstatten. *Kurt Hickisch*

¹ Näheres unter www.buergerkarte.at/hintergrund-informationen.de.php#signieren.

² Beispiele: www.hashgenerator.de

³ Anleitung unter www.buergerkarte.at/anleitungen/buergerkarte-handy-atrust.pdf.

⁴ Anleitung unter www.buergerkarte.at/anleitungen/RSa_BK-Aktivierung_e-card.pdf.

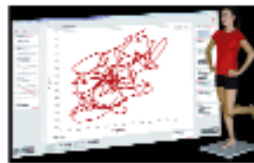
⁵ Anleitung unter www.buergerkarte.at/anleitungen/FON_BK-Aktivierung_e-card.pdf.

⁶ Auflistung unter www.buergerkarte.at/anwendungen.de.php.

FOTOS: KURT HICKISCH

mem mechanische und elektronische Meßtechnik

Modulare Testsysteme für Sport- & Rehabilitations-Medizin



Messen, testen und überwachen von RF-Signalen. Elektromog Messung von Mobiltelefon und WLAN Frequenzen



mem

mem - mechanic & electronic measurement
Freundgasse 8 A - 1040 VIENNA
Tel.: +43 1 943 42 54
Fax.: +43 1 943 42 51
Mobile: +43 699 1 943 42 55
e-mail: office@mem-vienna.com
www.mem-vienna.eu

Sicherheit auf Knopfdruck.

Laut ÖWD-IMAG-Üniversität
„das zuverlässigste und kompetenteste Wach- und Sicherheitsunternehmen Österreichs“.



ÖWD

ÖSTERREICHISCHER WACHDIENST

Wachdienste • Dienstleistungen • Dienstleistungen • Parkraumbewirtschaftung • Alarmvermittlung • Messservice und Messdienstleistungen • 24-Stunden-Notruf-Service Österreich



Flächendeckend in ganz Österreich
Info unter: 0800/34 51-0
info@zentrale@owd.at

März 2008