.SIAK REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
SICHERHEITSAKADEMIE

.SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis

Bociurko, Michaela-Maria (2008):

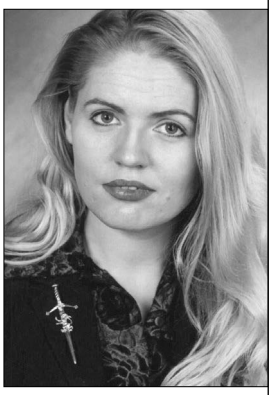
Die elektronische Signatur im öffentlichen Dienst

SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (2), 80-89.

doi: 10.7396/2008_2_H

Online publiziert: 3/2013

DIE ELEKTRONISCHE SIGNATUR IM ÖFFENTLICHEN DIENST



MICHAELA-MARIA BOCIURKO,
Leiterin der technischen Redaktion und des Kurswesens am Zentralen Informatikdienst der Universität Wien.

Schneller, kostengünstiger, mobiler sind die Begriffe, die wir heute meist mit elektronischer Kommunikation verbinden – Vorteile, die sich auch eine moderne öffentliche Verwaltung zu Nutze machen möchte. So sollen mittels verstärkten Einsatzes von Informations- und Kommunikationstechnologien eine erhöhte Kundenorientierung und verkürzte Bearbeitungszeiten erwirkt werden. Mit dem Inkrafttreten des E-Government-Gesetzes samt den Novellierungen des Allgemeinen Verwaltungsverfahrensgesetzes und des Zustellgesetzes wurde hierfür in Österreich der rechtliche Rahmen geschaffen.

Der elektronischen Signatur als zentrale Basistechnologie für sensible Kommunikation im Internet kommt dabei eine wesentliche Bedeutung zu, ermöglicht sie doch die Identifizierung und Authentifizierung von Personen, die mit der Behörde elektronisch in Kontakt treten. Aber auch umgekehrt ist es für die Behörde relevant, dass sie gegenüber der Partei oder gegenüber einer anderen Behörde ausweisen kann, dass ein elektronisch ausgestelltes Dokument tatsächlich von ihr stammt und dass dessen Inhalt nicht manipuliert wurde. Schließlich nehmen Betrugsversuche wie Phishing (das Ausspähen vertraulicher Informationen mittels gefälschter E-Mails und Webseiten) sukzessive zu. Auch wenn sich ein Großteil der Angriffe auf Banken konzentriert, gibt es auch immer wieder Fälle, in denen die Betrüger z.B. vorgeben als Behörde zu handeln. Gerade wegen des großen Vertrauens, das Bürger in behördliches Handeln setzen, ist es hier die Pflicht der Behörde, die Verantwortung für behördliche elektronische Dokumente deutlich sichtbar zu machen und deren Fälschungssicherheit zu erhöhen. Die digitale Signatur kann hier einen wesentlichen Beitrag zur Rechtssicherheit elektronischen Verwaltungshandelns leisten. In den rechtlichen Vorgaben wurden bereits die Rahmenbedingungen für den Einsatz der elektronischen Signatur im Verwaltungsverfahren definiert. Es ist nun an den Behörden, die für den Einsatz der elektronischen Signatur notwendigen technischen und organisatorischen Voraussetzungen zu schaffen.

1. ALLGEMEIN: FUNKTIONSWEISE, TECHNIK

1.1. PRAKTISCHE ANWENDUNG: DIE DIGITALE 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.[1] Die hier vorliegende Begriffsbestimmung wurde technologieneutral gestaltet und erlaubt

verschiedenste technische Realisierungen. In der Praxis werden elektronische Signaturen zumeist als so genannte digitale Signaturen unter Verwendung von asymmetrischen Kryptoalgorithmen und Zertifikaten verwirklicht.[2]

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

1. das Dokument tatsächlich von ihm stammt (Authentizität des Kommunikationspartners) und dass
2. der Inhalt des Dokuments nicht verändert wurde (Integrität der Daten).

Absender A erstellt ein Dokument und signiert dieses digital: Mithilfe eines mathematischen Verfahrens (Hash-Verfahrens) wird aus den Zeichen des Dokuments eine Prüfsumme (der sog. Hash-Wert) ermittelt – quasi ein „elektronischer Fingerabdruck". Diese Prüfsumme wird nun mit dem privaten Schlüssel des Absenders A verschlüsselt (der private Schlüssel ist dabei ausschließlich dem Signaturschlüsselinhaber, also Absender A zugänglich). Das Ergebnis dieser Verschlüsselung ist die so genannte digitale Signatur.

Dem Empfänger B wird nun 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 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 demjenigen zugerechnet werden kann, der Zugriff auf den privaten Schlüssel hat.

Grafik: Bociurko

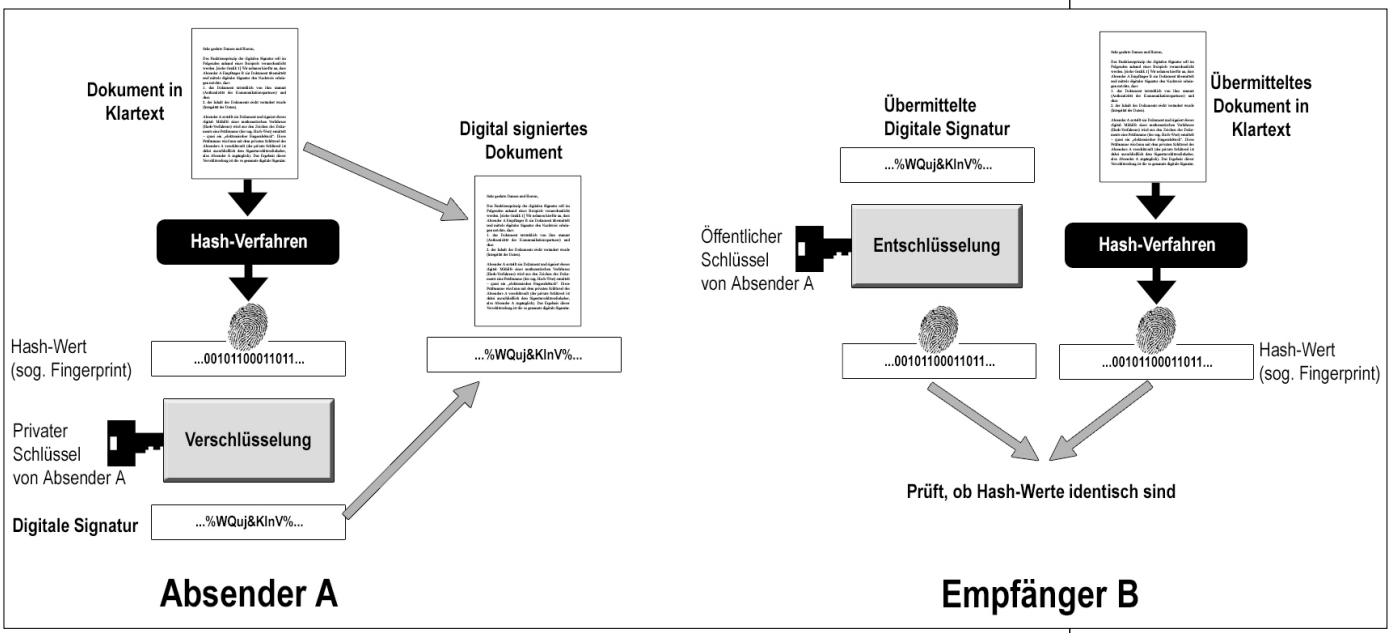


Abb. 1: Funktionsprinzip Digitale Signatur

1.2. ZERTIFIKATE

Empfänger B kann daraus aber noch nicht ableiten, dass es sich bei der signierenden Person tatsächlich um den z.B. im Absenderfeld angegebenen Herrn Mustermann handelt. Um der digitalen Signatur vertrauen zu können, muss eine korrekte Zuordnung des öffentlichen Schlüssels zu einer Person (bzw. Institution/Behörde) sichergestellt werden. Diese Zuordnung erfolgt mittels so genannter Zertifikate.

Durch ein Zertifikat können AnwenderInnen den öffentlichen Schlüssel einer Identität zuordnen.

Die Ausstellung und Administration von Zertifikaten sollte dabei selbstredend von einer vertrauenswürdigen Instanz übernommen werden, damit die AnwenderInnen sich auf die in den Zertifikaten enthaltenen Informationen verlassen können. In der Regel obliegt dies den so genannten 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[3], über den die Empfänger digital signierter Dokumente die Zertifikate nachprüfen können.[4]

Die Struktur und der Inhalt von digitalen Zertifikaten werden durch verschiedene Standards (wie X.509, RFC 2440, ISO7816, …) vorgegeben. Das am weitesten verbreitete Zertifikatsformat ist X.509. Ab Version 3 von X.509 bietet sich die Möglichkeit von Erweiterungen (Extensions) – dies sind quasi Zusatzinformationen, die im Rahmen gewisser Formatvorschriften neben den Kerndaten in das Zertifikat eingebracht werden können. Um ein Zertifikat als einer Verwaltungsorganisation zugehörig auszuweisen, kann die Verwaltungseigenschaft als Extension aufgenommen werden. Der zugehörige Object Identifier ist in „Object Identifier der öffentlichen Verwaltung“ (OID) definiert.

1.3. GEWÄHRLEISTUNG DER SICHERHEIT DES PRIVATEN SCHLÜSSELS

Wie bereits vorweg erwähnt, kommen bei asymmetrischen Algorithmen zwei Schlüssel zum Einsatz. Diese bilden ein Schlüsselpaar und stehen zueinander in einem mathematischen Verhältnis. Der öffentliche Schlüssel errechnet sich dabei durch Anwendung einer so genannten Einwegfunktion aus dem privaten Schlüssel. Umgekehrt darf aber der private Schlüssel 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, ...).

Aber auch andere Aspekte sind entscheidend für die Sicherheit des Verfahrens wie etwa die sichere Verwahrung und Geheimhaltung des privaten Schlüssels.

Es sind entsprechende Maßnahmen zu ergreifen, um 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. Eine Möglichkeit wäre etwa, den Schlüssel auf einer Festplatte oder auf einem Server zu speichern und durch ein Passwort zu sichern. Bei

dieser Lösung ist der private Schlüssel aber prinzipiell aus dem Speichermedium auslesbar – er wird also nur durch das Wissen um das Passwort geschützt. Ein höheres Sicherheitsniveau wird erreicht, wenn der private Schlüssel auf einem nichtauslesbaren Speichermedium wie etwa auf einem Hardware-Token aufgebracht ist. Ein solcher Token kann technisch ganz unterschiedlich realisiert werden (z.B. als USB-Stick, Chipkarte/Smartcard, Handy). Als derzeit sicherstes Medium für die Aufbewahrung des privaten Schlüssels gelten Smartcards. Smartcards 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/PIN geschützt.

Mindestens ebenso wichtig wie die technischen Maßnahmen zur Sicherung des privaten Schlüssels ist freilich der verantwortungsvolle und umsichtige Umgang der AnwenderInnen mit Passwort und Token. So kann etwa nicht oft genug betont werden, dass Passwörter/PINs niemals weitergegeben oder niedergeschrieben werden sollten.

2. DIE ELEKTRONISCHE SIGNATUR – RECHTLICHE GRUNDLAGEN

2.1. SIGNATURRICHTLINIE, SIGG, NOVELLIERUNG 2007

Im Rahmen der EU hat man sich im Jahr 1999 auf gemeinschaftliche Rahmenbedingungen für elektronische Signaturen geeinigt.[5] Die Umsetzung der EU-Signaturrichtlinie erfolgte in Österreich durch das Signaturgesetz (SigG). Dieses gibt den rechtlichen Rahmen für die Erstellung und Verwendung von elektronischen Signaturen vor.[6]

Allerdings gab es am SigG diverse Kritikpunkte. So wurde beispielsweise immer wieder betont, dass mit dem österreichischen SigG „über das Ziel hinausgeschossen“ wurde: Es ginge zum Teil über die EU-Richtlinie hinaus und schaffe eine „Überregulierung“ – die geforderten Auflagen seien zu hoch und in der Folge zu kostenintensiv. Auch gab es Bedenken hinsichtlich einzelner Begrifflichkeiten, da diese nicht EU-konform bzw. missverständlich wären (Beispiel „sichere“ Signatur). Mit der umfangreichen Novellierung 2007 wurden indes viele dieser Kritikpunkte entschärft.

2.2. ELEKTRONISCHE SIGNATUREN NACH DEM SIGG

Das aktuelle SigG kennt verschiedene Ausprägungen von elektronischen Signaturen. Diese Ausprägungen unterscheiden sich zum Teil wesentlich hinsichtlich ihrer Sicherheitsanforderungen sowie ihrer Bedeutung im Rechtsverkehr.

2.2.1. DIE (EINFACHE) ELEKTRONISCHE SIGNATUR

Der bereits eingangs zitierte § 2 Z. 1 SigG definiert die elektronische Signatur als elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung des Signators dienen. Diese (einfache) elektronische Signatur beruht auf einem (einfachen) Zertifikat. Als (einfaches) Zertifikat 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 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 nicht als Beweismittel ausgeschlossen werden (§ 3 Abs. 1 SigG).

2.2.2. DIE QUALIFIZIERTE ELEKTRONISCHE SIGNATUR (VORMALS „SICHERE“ SIGNATUR)

Ist nach dem österreichischen Signaturgesetz eine elektronische Signatur, die ausschließlich dem Signator[7] 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 mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass jede nachträgliche Veränderung der Daten festgestellt werden kann (d.h. Einsatz eines geeigneten Hash-Verfahrens notwendig). Zudem muss die qualifizierte Signatur auf einem qualifizierten Zertifikat beruhen und unter Verwendung von technischen Komponenten und Verfahren erstellt werden, die den Sicherheitsanforderungen des SiG 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. Damit kann das zivilrechtliche Formerfordernis der Schriftform auch durch Beisetzung einer qualifizierten Signatur zu einem elektronischen Dokument erfüllt werden.[8]

2.2.3. DIE FORTGESCHRITTENE ELEKTRONISCHE SIGNATUR

In die Novellierung des SigG 2007 wurde zudem der Begriff der „fortgeschrittenen elektronischen Signatur“ aufgenommen. Von dem Begriff der qualifizierten elektronischen Signatur unterscheidet sich dieser Begriff einzig dadurch, dass die Signatur nicht notwendigerweise auf einem qualifizierten Zertifikat beruht (das bedeutet z.B. unter anderem, dass vor der Ausstellung des Zertifikates nicht unbedingt ein Lichtbildausweis geprüft werden muss) und dass die Signatur nicht notwendigerweise mit einer sicheren Signaturerstellungseinheit (wie z.B. einer entsprechend geprüften und bescheinigten Chipkarte) erstellt werden muss.

3. DIE ELEKTRONISCHE SIGNATUR IM ÖFFENTLICHEN DIENST

3.1. RECHTLICHE RAHMENBEDINGUNGEN

In Österreich wurde in den letzten Jahren die Entwicklung zum Electronic Government maßgeblich vorangetrieben. Mit dem E-Government-Gesetz, das am 1. März 2004 in Kraft trat, wurden hierfür die rechtlichen Rahmenbedingungen geschaffen. Erklärtes Ziel ist es dabei, rechtserhebliche elektronische Kommunikation zu fördern und den elektronischen Verkehr mit öffentlichen Stellen zu erleichtern.

Der Einsatz von IT-Technologie soll dazu beitragen, Verwaltungsverfahren effizienter und benutzerfreundlicher zu gestalten.

Die Anpassung des Verwaltungsverfahrens an die elektronische Verwaltungsführung nach dem Konzept des E-GovG erforderte zahlreiche Änderungen im Allgemeinen Verwaltungsverfahrensgesetz 1991 (AVG). Die wesentlichsten Bestimmungen zur Verwendung von elektronischen Signaturen im Verwaltungsverfahren auf Seiten der Behörde finden sich im § 18 Erledigungen. Auch das Zustellgesetz musste an die elektronische Verwaltungsführung angepasst werden. Die elektronische Übermittlung behördlicher Schrift-

stücke wurde im Rahmen des ZustG neu geregelt.

2007 erfolgte eine umfassende Novellierung der Verwaltungsverfahrensgesetze (Verwaltungsverfahrens- und Zustellrechtsänderungsgesetz 2007) sowie des E-Government-Gesetzes (E-GovG-Novelle 2007). Diese Novellen sind nun seit Jahresbeginn 2008 in Kraft.

3.2. SONDERFORMEN ELEKTRONISCHER SIGNATUREN IN DER VERWALTUNG

Das E-GovG kennt neben den im SigG definierten elektronischen Signaturen zwei Sonderformen: Der Bürger/Antragsteller authentifiziert sich im Rahmen des Bürgerkartenkonzepts gegenüber der Behörde mittels Verwaltungssignatur bzw. qualifizierter Signatur. Die Behörde authentifiziert sich gegenüber der Partei (Bürger, Unternehmen) mittels Amtssignatur.

3.2.1. VERWALTUNGSSIGNATUR

Die Verwaltungssignatur war eigentlich eine Übergangslösung – quasi eine „abgespeckte Version der qualifizierten elektronischen Signatur". 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.

3.2.2. AMTSSIGNATUR

Die Amtssignatur ist eine elektronische Signatur, die ausschließlich von Behörden (bzw. von einem Auftraggeber des öffentlichen Bereichs) verwendet werden darf. Sie wird auf elektronischen Erledigungen seitens der Behörde angebracht und macht damit kenntlich, dass es sich um ein amtliches Schriftstück handelt.

Bisher gab es keine Vorgaben bezüglich der Qualität der Amtssignatur (ob hierfür beispielsweise eine qualifizierte oder eine einfache elektronische Signatur verwendet werden sollte). Die Entscheidung oblag einzig der Beurteilung durch die Behörde. Mit der Novellierung des E-GovG 2007 wurde jedoch ein Mindeststandard festgelegt: Die Amtssignatur hat nun einer fortgeschrittenen elektronischen Signatur im Sinne des Signaturgesetzes zu entsprechen. Die sichere Verwahrung des Signaturschlüssels liegt damit in der Verantwortung des Signators. Werden entsprechende technisch-organisatorische Sicherheitsmaßnahmen gesetzt, dann ist die Sicherheit im Sinne des Signaturgesetzes gegeben. Trotz der Anhebung des Sicherheitslevels ergibt sich seitens der Behörde für die technische Umsetzung beispielsweise keine zwingende Notwendigkeit der Aufbewahrung der Signaturerstellungsdaten auf einer Krypto-Hardware. Die Amtssignatur kann somit auch auf einem softwarebasierten Signaturzertifikat beruhen.[9]

Da es sich eben um eine fortgeschrittene Signatur handelt, benötigt die Amtssignatur auch kein qualifiziertes Zertifikat.

Sehr wohl erforderlich ist jedoch, dass das (einfache) Zertifikat die Zertifikatserweiterung Verwaltungseigenschaft beinhaltet. Zudem ist die Amtssignatur durch eine Bildmarke, die die Behörde im Internet als die ihre gesichert veröffentlicht hat, sowie durch einen Hinweis im Dokument, dass dieses amtssigniert wurde, darzustellen.

Für die technische/organisatorische Umsetzbarkeit der Amtssignatur brachte die Novelle ganz allgemein einige Erleichterungen: So musste bisher etwa die Signaturprüfung über die Rückführung der Ansicht des gesamten Dokuments in eine Form, die die Signaturprüfung zulässt, möglich sein. In der Praxis erwies sich diese Anforderung als technisch problematisch umzusetzen. In der Novellierung ist nun die Rückführbarkeit des Ausdrucks in die elektronische Form nicht mehr zwingend erforderlich – das Dokument kann nun auch durch andere Vorkehrungen der Behörde verifiziert werden. Die Art der Verifikation ist dabei den Behörden überlassen. Diese Neuformulierung eröffnet verschiedene Umsetzungsoptionen wie die Echtheit von Dokumenten überprüft werden könnte (z.B. online abrufbares Archiv, Auskunftsstelle der Behörde, ...).

3.3. ANWENDUNGSBEREICHE DER AMTSSIGNATUR

In welchen Fällen kommt nun die Amtssignatur zum Einsatz? Die wesentlichen Bestimmungen zur Verwendung von elektronischen Signaturen im Verwaltungsverfahren auf Seiten der Behörde finden sich im Allgemeinen Verwaltungsverfahrensgesetz (AVG).

Bisher galt, dass die elektronische Beurkundung bei internen Erledigungen („Dokumentation“) mit elektronischer Signatur zu erfolgen hat und dass bei externen schriftlichen Erledigungen entweder eine Unterschrift, eine Beglaubigung oder eine Amtssignatur erforderlich ist. Für diese Bestimmungen galt ein Übergangszeitraum bis 31. Dezember 2007.

In der Novellierung des AVG 2007 wurde der § 18 gänzlich neu gefasst. Die Unterscheidung zwischen „internen“ und „externen“ Erledigungen wurde aufgegeben. Erforderlich ist die Amtssignatur nun nur mehr bei schriftlichen Ausfertigungen in elektronischer Form. Bei Ausfertigungen in Papierform gilt, dass Ausfertigungen in Form von Ausdrucken von mit einer Amtssignatur versehenen elektronischen Dokumenten oder von Kopien solcher Ausdrucke keine weiteren Voraussetzungen zu erfüllen brauchen. Sonstige Ausfertigungen in Papierform bedürfen jedoch einer Unterschrift vom Genehmigenden bzw. einer Beglaubigung von der Kanzlei. Um schriftliche Erledigungen zu genehmigen, ist prinzipiell eine Unterschrift vom Genehmigungsberechtigten erforderlich. Wurde die Erledigung elektronisch erstellt, so kann an deren Stelle ein Verfahren zum Nachweis der Identität (§ 2 Z. 1 E-GovG) des Genehmigenden und der Authentizität (§ 2 Z. 5 E-GovG) der Erledigung treten – es muss also nicht zwingend die Amtssignatur verwendet werden.

3.4. ÜBERGANGSFRIST

Da es bereits absehbar war, dass man seitens der Behörden bis Jahresende 2007 kaum allerorts die Voraussetzungen für den Einsatz der elektronischen Signatur schaffen würde, wurde die in § 82 Abs. 14 zweiter Satz AVG vorgesehene Übergangsfrist im Rahmen der Novellierungen um drei weitere Jahre verlängert und gilt nun bis zum 31. Dezember 2010. Bis dahin bedürfen schriftliche Ausfertigungen von elektronisch erstellten Erledigungen sowie schriftliche Ausfertigungen, die an einer elektronischen Zustelladresse zugestellt werden sollen, keiner Amtssignatur.

4. TECHNISCHE UMSETZUNGSOPTIONEN SEITENS DER BEHÖRDE

Auch wenn die Frist verlängert wurde – für die Behörden ergibt sich aus den geschilderten rechtlichen Rahmenbedingungen ein Handlungsbedarf hinsichtlich der Schaffung von geeigneten technischen und organisatorischen Voraussetzungen zur

Implementierung der Amtssignatur. Es gilt, sich nun mit der Thematik auseinanderzusetzen und Konzepte für eine zeitgerechte Umsetzung zu schaffen. Dabei ist prinzipiell festzuhalten, dass die gesetzlichen Vorgaben ausreichend Spielraum gewähren bei der technischen Realisierung. Um dies zu veranschaulichen, sollen im Folgenden exemplarisch zwei Umsetzungsoptionen näher beleuchtet werden.

4.1. SOFTWAREBASIERT (SIGNATUR AUF SOFTWAREBASIERTEM SIGNATURZERTIFIKAT)

Eine denkbare Lösung wäre z.B. eine zentrale Instanz, d.h. alle beteiligten Schlüssel befinden sich auf einem zentralen Server. Der Ablauf könnte dann in etwa so aussehen: Die Behörde installiert einen Signaturserver, stellt eine entsprechende Software-Infrastruktur bereit und erwirbt von einem ZDA Zertifikate (A-Cert und A-Trust bieten hierfür eigens zugeschnittene Zertifikats-Produkte wie a.sign corporate Amtssignatur bzw. A-CERT GOVERNMENT – Amtssignaturzertifikat). Diese werden in einer Datei auf dem Server abgelegt. Die Signatursoftware verwendet diese Datei, um Dokumente zu signieren. Alle Verschlüsselungs- und Signiervorgänge werden direkt am Server vorgenommen. Zugang zum privaten Schlüssel erhält der Signator mittels Eingabe eines Passworts/PINs.

Am kostengünstigsten ließe sich diese Lösung mit den sog. MOA-Modulen (sog. Module für Online Applikationen[10]) realisieren, die sich bereits in diversen Best Practices bewährt haben. Sie sind quasi das serverseitige Gegenstück auf Seiten der Verwaltung zur so genannten Bürgerkartenumgebung (BKU) des Bürgers. Die Lizenzen werden vom Bund für die Umsetzung von E-Government-Diensten kostenfrei zur Verfügung gestellt. Vorteilhaft sind hier auch die standardisierten Schnittstellen.

Da eine fortgeschrittene Signatur (was die Amtssignatur ja mindestens sein muss) wie eingangs erwähnt kein qualifiziertes Zertifikat und keine sichere Signaturerstellungseinheit erfordert, wäre eine solche softwarebasierte Lösung denkbar. Notwendig wäre aber in jedem Fall die Einführung organisatorischer Formalismen – ordentlicher Betriebsguidelines – nach denen das MOA-Modul betrieben wird. Wichtig ist, dass hier klare Berechtigungen gesetzt wurden (wer darf wann was verwenden). Technisch sollte das dann auch mittels Logfiles protokolliert werden, um einen eventuellen Missbrauch feststellen zu können.

4.2. HARDWAREBASIERT (LOKAL BKU[11], EXTERNES SPEICHERMEDIUM Z.B. SMARTCARD)

Bei dieser Lösung wird lokal (am Arbeitsplatz) via Bürgerkartenumgebung, z.B. smartcardbasiert, signiert. Das erworbene Zertifikat und der private Schlüssel befinden sich auf der Smartcard. Der Signator schiebt die Karte in ein Kartenlesegerät und aktiviert durch Eingabe eines PIN-Codes oder durch einen vergleichbaren Auslösevorgang die Signatur.

Thematisch fällt diese Lösung in den Bereich E-Dienstkarte. Da Smartcards multifunktional sind, liegt es nahe, auf den Chipkarten (je nach Bedarf) verschiedenste Funktionalitäten zu bündeln wie etwa Dienstausweis, Single Sign-On (d.h. Anmelden am PC und bei allen IT-Verfahren mittels eines einzigen Anmeldevorgangs), Zutrittssteuerung von Räumen und Gebäuden, Bürgerkarte etc. Die elektronische Signatur wäre in diesem umfassenden Konzept somit nur ein Aspekt unter vielen. Dabei sollte nicht außer Acht gelassen werden, dass das Beamtendienstrechtsgesetz (BDG) ohnehin vorsieht, dass neu auszustellende Dienstkarten bürgerkartentauglich sein müssen (d.h. dass bereits die

technischen Möglichkeiten vorhanden sein müssen – Chip).[12]

Für eine smartcardbasierte Lösung spricht zum einen der hohe Sicherheitslevel (so wäre auch eine qualifizierte Signatur möglich), zum anderen der vielfache Nutzen/Mehrwert, der aus einer solchen multifunktionellen E-Dienstkarte gezogen werden könnte. Aufwand und Kosten sind bei dieser Lösung selbstredend schon aufgrund der großen Stückzahl an Workstations (im BM.I wären es insgesamt etwa 17.000) in einer anderen Dimension angesiedelt.[13] Zudem sind technisch und organisatorisch zahlreiche zusätzliche Schritte zur Implementierung notwendig, wie etwa das Ausrollen der Bürgerkartenumgebung an allen Arbeitsplätzen, das Bereitstellen der zentralen und lokalen Infrastruktur, Kartenproduktion und -management (Definition der Workflows) etc. Bedenkt man die große Anzahl an notwendigen Zertifikaten, wäre es hier eventuell auch schon lohnenswert das Betreiben einer eigenen Authority anzudenken.

Da sich aufgrund der rechtlichen Vorgaben für die Amtssignatur keine speziellen Anforderungen an die Qualität von Karte und Chip ergeben, liegt es hier im Ermessen der Behörde, die technischen Anforderungen an die Smartcard (den Chip) zu definieren.

5. RESÜMEE

Vergleicht man die rechtlichen Rahmenbedingungen für den Einsatz der elektronischen Signatur im Verwaltungsverfahren vor und nach den umfassenden Novellierungen 2007, so kann festgestellt werden, dass man seitens des Gesetzgebers sehr bemüht war, die im Laufe des Umsetzungsprozesses in den letzten Jahren erkannten Problematiken mit den nun bereits in Kraft getretenen Novellierungen zu entschärfen. Ganz allgemein wurde die technische Umsetzung der Amtssignatur durch die Novellierungen erleichtert (Beispiel Rückführbarkeit), und auch bei den Begriffen konnte mehr Klarheit geschaffen werden. Zuweilen werfen die neuen Gesetzesgrundlagen aber auch neue technische bzw. organisatorische Fragen auf, wie etwa: Wie realisiert man z.B. Alternativen zur Rückführbarkeit? Auch die vorgesehene Anhebung der Qualität der Amtssignatur auf den Level der fortgeschrittenen Signatur (die aus sicherheitstechnischen Überlegungen sehr zu begrüßen ist) erfordert bei einigen Lösungen zusätzliche Vorkehrungen (wie beispielsweise Freigabemechanismen), die bisher nicht zwingend erforderlich waren.

Der Ball ist nun erneut bei den Behörden, die angehalten sind, bis zum 31. Dezember 2010 geeignete technische und organisatorische Voraussetzungen zur Implementierung der Amtssignatur zu schaffen.

Aus den im Rahmen dieses Aufsatzes geschilderten rechtlichen Rahmenbedingungen ergeben sich klare Anforderungen an die Amtssignatur – die grundsätzliche Frage, wie diese technisch realisiert werden soll, obliegt jedoch letztlich dem Ermessen der Behörde. So sind sowohl software- als auch hardwarebasierte Lösungen zulässig. Entscheidend für die Auswahl wird zuvorderst der use case sein. Dabei ist es Aufgabe der internen Verantwortlichen, welche mit den spezifischen Organisationsabläufen, den Applikationen sowie der Infrastruktur vertraut sind, die notwendigen organisatorischen und technischen Erfordernisse in den einzelnen Bereichen zu definieren.

Letztlich handelt es sich dabei auch um eine Grundsatzentscheidung: Sollen lediglich (mit geringstmöglichen Kosten und Aufwand) die Voraussetzungen für den

Einsatz der Amtssignatur nach dem AVG geschaffen werden oder betrachtet man die digitale Signatur vielmehr als einen Teilaspekt eines umfassenden IT-Konzeptes, das hinsichtlich diverser Zusatzfunktionalitäten (wie Single-Sign-On, Zutrittskontrolle, …) skalieren soll? Nur auf der Basis dieser Antwort wird es letztlich möglich sein, eine stimmige und nachhaltige Lösung aus den vorhandenen Optionen auszuwählen.

Abschließend sei erlaubt, nochmals darauf hinzuweisen, dass Bürger großes Vertrauen in behördliches Handeln setzen. Es ist somit Aufgabe der Behörde, alle notwendigen Maßnahmen zu ergreifen, um das elektronische behördliche Verfahren sicher zu gestalten. Insbesondere das BM.I als innerer Sicherheitsexperte/-garant sollte sich hier nicht „hinten einreihen", sondern sich vielmehr aktiv in derlei IT-Sicherheitsdebatten einbringen, Lösungen mitgestalten sowie eine ambitionierte Rolle im österreichweiten Umsetzungsprozess anstreben.

[1] *SigG § 2 Z. 1.*

[2] *Quelle: http://www.bsi.de/esig/esig.pdf#technische.*

[3] *Damit eine digitale Signatur auf ihre Urheberschaft überprüft werden kann, muss die Zertifizierungsstelle alle von ihr ausgestellten Zertifikate in einem über die öffentlichen Netze zugänglichen Verzeichnis nachprüfbar halten.*

[4] *Quelle: http://www.ecin.de/sicherheit/signatur/.*

[5] *Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen.*

[6] *Bundesgesetz über elektronische Signaturen; idF BGBl I Nr. 164/2005.*

[7] *Bei dem Signator handelt es sich nach der Novellierung um eine natürliche bzw. juristische Person bzw. sonstige rechtsfähige Einrichtung.*

[8] *Es wurden hierbei jedoch einige Ausnahmen definiert – siehe § 4 Abs. 2 SigG.*

[9] *Vielmehr ist es auch ausreichend, dass der Zertifikatswerber die Signaturerstellungsdaten in einer kennwortgeschützten Datei aufbewahrt.*

[10] *Es stehen hier verschiedene Module zur Verfügung (beispielsweise MOA-SS zum Erstellen von Serversignaturen, MOA-SP zum Überprüfen von Signaturen, …).*

[11] *Die für die Umsetzung der Schnittstelle Security Layer notwendige Software wird Bürgerkartenumgebung genannt.*

[12] *Quelle: Interview Mag. Dr. Bernhard Karning (BKA).*

[13] *Andererseits bedingt die hohe Stückzahl auch wiederum relativ niedrige Stückpreise.*