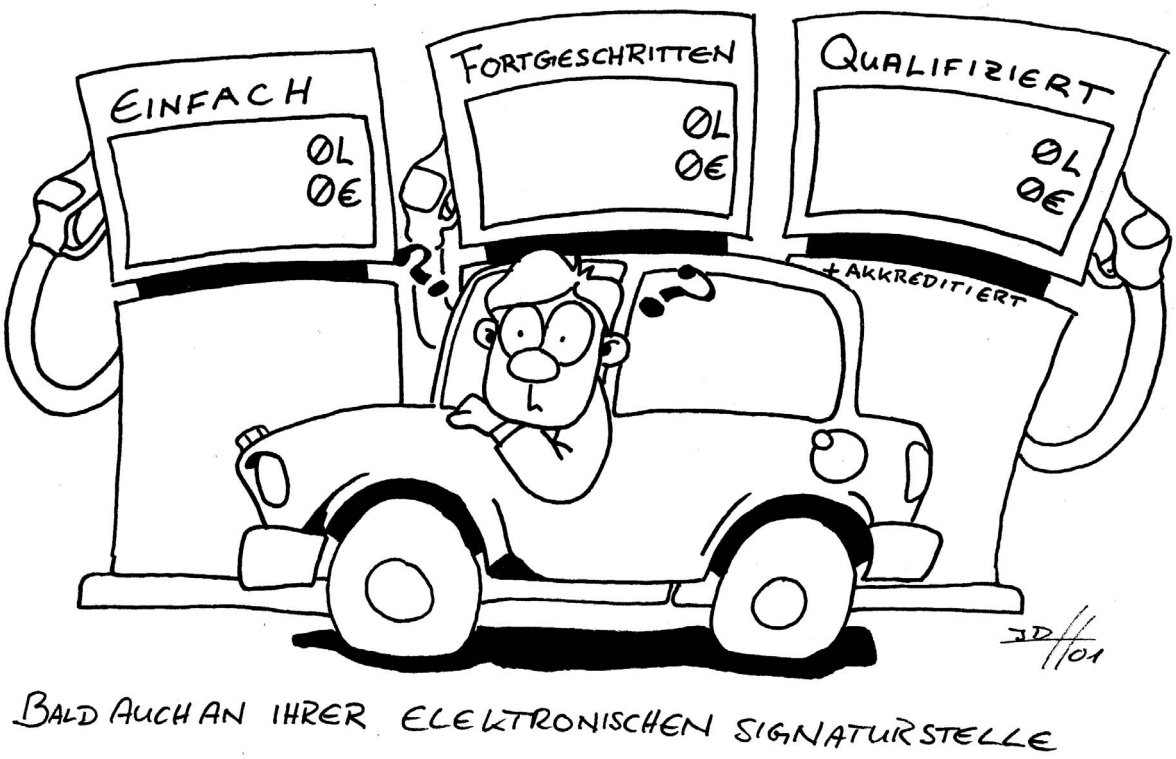
Deutscher Städtetag

Welche elektronische Signatur braucht die Kommunalverwaltung?



Geschlechtsneutrale Bezeichnungen

In der folgenden Ausarbeitung wird i.d.R. der Plural verwendet. Im Hinblick auf eine leichtere Lesbarkeit wurde auf die jeweils weibliche und männliche Form verzichtet. Der Plural soll selbstverständlich beide umfassen.

Zitate

Originalzitate sind in kursiv gesetzt.

Abkürzungsverzeichnis

BGB	Bürgerliches Gesetzbuch
BSI	Bundesamt für Sicherheit in der Informationstechnik
i.d.F.	in der Fassung
IT	Informationstechnologie
KBSt	Koordinierungs- und Beratungsstelle der Bundesregierung beim Bundesinnenministerium
PKI	Public Key Infrastructure
RegTP	Regulierungsbehörde für Telekommunikation und Post
RleS	EU - Richtlinie über gemeinschaftliche Regelungen für elektronische Signaturen
SigG	Signaturgesetz
SigV	Signaturverordnung
StGB	Strafgesetzbuch
VwVfG	Verwaltungsverfahrensgesetz
VwVfG-E	Verwaltungsverfahrensgesetz – Entwurf
ZPO	Zivilprozessordnung

Verfasser

Arbeitskreis „Digitales Rathaus“ im Deutschen Städtetag, Arbeitsgruppe 1
Dr. Peter Behringer, Stadt Karlsruhe
Jörg Blumenthal, Stadt Mannheim
Klaus Eisele, Stadt Nürnberg
Richard Stelzer, Bayerischer Städtetag
Hans-Volker Winkler, Landeshauptstadt München
Wolfgang Willberger, Landeshauptstadt München

Stand: Mai 2002

Lindenallee 13 - 17
50968 Köln

Management Summary

1. Welche Qualitätsstufen von Signaturen gibt es und worin liegen die wesentlichen Unterschiede?

Nach der Neufassung des deutschen Signaturgesetzes werden insgesamt vier Stufen der elektronischen Signatur unterschieden:

- Die **(einfache) elektronische Signatur** (z.B. eingescannte Unterschrift) ist nicht zweifelsfrei einer Person zuzuordnen. Sie erfüllt keine besonderen Sicherheitsanforderungen und hat daher wenig Beweiswert. Sie kommt nur für formfreie Vorgänge in Betracht. Im Verwaltungsverfahren ist dies der Regelfall, der allerdings in verschiedenen Vorschriften durch Formerfordernisse durchbrochen wird.
- **Fortgeschrittene Signaturen** genügen bereits erhöhten Anforderungen, lassen insbesondere eine Authentifizierung des Signaturschlüssel-Inhabers und die Überprüfung der Integrität der übermittelten Daten zu. Sie ersetzen jedoch weder im Zivil- noch im öffentlichen Recht eine etwa vorgeschriebene Schriftform.
- **Qualifizierte elektronische Signaturen** (ohne Anbieterakkreditierung) erfüllen die Voraussetzungen der fortgeschrittenen Signaturen und werden mit einer sicheren Signaturerstellungseinheit erzeugt. Sie werden von Zertifizierungsdiensteanbietern (Trust-Center) ausgestellt, deren Betrieb zwar genehmigungsfrei ist, die jedoch gesetzlich geforderte Voraussetzungen erfüllen müssen. Die Aufnahme des Betriebs ist der Regulierungsbehörde für Post und Telekommunikation (RegTP) anzuzeigen. Die qualifizierte elektronische Signatur erfüllt hohe Sicherheitskriterien, ist für die Authentifizierung geeignet und bietet ein hohes Maß an Beweiskraft. Die Zertifikate müssen für den Gültigkeitszeitraum sowie fünf weitere Jahre aufbewahrt werden. Qualifizierte elektronische Signaturen können sowohl im Zivilrecht und künftig auch im öffentlichen Recht die Schriftform ersetzen.
- **Qualifizierte elektronische Signaturen mit Anbieterakkreditierung** erfüllen die Voraussetzungen der qualifizierten elektronischen Signaturen und entfalten grundsätzlich die gleichen Rechtswirkungen. Darüber hinaus garantieren die Zertifizierungsdiensteanbieter jedoch eine nachgewiesene organisatorische und technische Sicherheit. Vor Aufnahme des Betriebs erfolgt eine umfassende Sicherheitsüberprüfung, die Anbieter erhalten anschließend ein „Gütesiegel“. Ein weiterer Unterschied liegt in der langfristigen Überprüfbarkeit der Zertifikate (mindestens 30 Jahre).
  Zusätzliche Anforderungen wie z.B. die dauerhafte Überprüfbarkeit können im öffentlichen Recht für einzelne, genau bestimmte Vorgänge als Voraussetzung festgelegt werden. Eine generelle Festlegung dieser Signaturstufe ist jedoch nicht möglich. Im Zivilrecht kann diese Stufe überhaupt nicht gefordert werden.

2. Welche elektronische Signatur wird benötigt?

- **Signaturen für die Behördenkommunikation der Bürger und der Wirtschaft**

  Soweit eine Schriftformerfüllung durch Unterschrift erforderlich ist, wird sich für Verfahrenshandlungen des Bürgers und der Wirtschaft mit der Verwaltung die qualifizierte elektronische Signatur als Standard herausbilden. Für einzelne, genau bezeichnete Handlungen, kann zwar auch eine qualifizierte Signatur mit dauerhafter Überprüfbarkeit, wie sie von der Signatur mit Anbieterakkreditierung erfüllt wird, vorgeschrieben werden. Der Rahmen hierfür ist jedoch einerseits relativ eng gesteckt und würde andererseits zu einer gewissen „Verwirrung“ bei Bürgern und Wirtschaft führen, welche Signatur nun für welchen Vorgang erforderlich ist.

  Ist keine Schriftformerfüllung durch Unterschrift erforderlich, sollte für Handlungen des Bürgers bzw. der Wirtschaft keine Signatur, d.h. auch keine niedrigere Signaturstufe (insbes. fortgeschrittene Signatur), vorgeschrieben werden. Für Handlungen, die bisher formlos (auch mündlich bzw. durch Telefonanruf) angestoßen werden konnten, dürfen künftig nicht aufgrund der Verfügbarkeit einer neuen Technik (elektronische Signatur) höhere Hürden gesetzt werden.

  Unabhängig davon ist die Verwendung von einfachen Signaturen (z.B. eingescannte Unterschrift, Namenszeichen) immer möglich. Soweit keine besonderen Formerfordernisse eine qualifizierte Signatur erfordern, steht es Bürgern und Wirtschaft grundsätzlich frei, auch fortgeschrittene Signaturen bei der Kommunikation mit der Verwaltung einzusetzen. Aufgrund der großen Vielzahl unterschiedlicher Produkte und Standards bei den fortgeschrittenen Signaturen kann es allerdings - vor allem bei älteren Versionen - wegen der häufig nicht gegebenen Interoperabilität zu technischen Problemen kommen. Dies kann soweit führen, dass eingehende - nur signierte und nicht verschlüsselte - Nachrichten nicht mehr les- und verarbeitbar sind.

- **Signaturen für die Verwaltung**

  Soweit Verwaltungen fiskalisch handeln und dabei eine ggf. erforderliche Schriftform durch eine elektronische Signatur ersetzen möchten, benötigen sie hierfür eine qualifizierte Signatur nach dem Signaturgesetz.

  Für Handlungen auf dem Gebiet des öffentlichen Rechts ist prinzipiell eine abgestufte Sichtweise denkbar. Es wird auch künftig viele Handlungen der Verwaltung geben, die ohne Signatur durchgeführt werden können, denn Verwaltungsakte bedürfen nicht grundsätzlich der Schriftform. Für viele Handlungen im rein internen Verkehr wäre grundsätzlich eine fortgeschrittene Signatur ausreichend. Hierdurch wären bereits erste Sicherheitsfeatures umsetzbar, z.B. die Prüfung der Dateikonsistenz („wurden die Daten auf dem

Transportwege verändert?“). Allerdings ist die Schriftformerfüllung durch diese Signaturstufe nicht möglich. Gerade für die Kommunalverwaltung, mit der Bürger und Wirtschaft eine Vielzahl ihrer Behördenkontakte abwickeln, gibt es jedoch zahlreiche Fälle, bei denen in der internen und externen Kommunikation die Schriftform vorgeschrieben ist. Diese kann nur durch die qualifizierte elektronische Signatur abgebildet werden, wobei in definierten Einzelfällen durch Rechtsverordnung auch die dauerhafte Überprüfbarkeit und damit faktisch die qualifizierte Signatur eines akkreditierten Zertifizierungsdiensteanbieters vorgeschrieben werden kann.
Die derzeit am Markt verfügbaren qualifizierten Signaturen stammen weit überwiegend von akkreditierten Zertifizierungsdiensteanbietern.

- **Zusammengefasst ergeben sich damit für die Städte folgende Möglichkeiten:**

  - Die Mitarbeiter erhalten mindestens eine qualifizierte Signatur, soweit sie Aufgaben erfüllen, für die diese Stufe erforderlich ist. Die übrigen Mitarbeiter erhalten bei Bedarf eine niedrigere Stufe (fortgeschrittene Signatur). Eine derart heterogene Ausstattung würde jedoch aus verschiedenen Gründen zu erheblichen Problemen führen, nicht zuletzt deshalb, weil die verschiedenen Produkte nur eingeschränkt zueinander kompatibel sind. Auch stehen den eingesparten Sachkosten höhere administrative Aufwände gegenüber.

  - Um diese Heterogenität zu vermeiden und um den Administrationsaufwand so gering wie möglich zu halten, bietet es sich an, alle Mitarbeiter, die Aufgaben erledigen, für die eine qualifizierte elektronische Signatur vorgeschrieben ist, auch mit dieser auszustatten. Aufgrund der o.g. Argumente spricht viel dafür, dazu qualifizierte Signaturen eines akkreditierten Anbieters einzusetzen.

    Weitere Mitarbeiter würden nur bei Bedarf mit personenbezogenen qualifizierten elektronischen Signaturen ausgestattet werden. Möglicherweise können die Zertifikate darüber hinaus auch für andere dienstliche Zwecke eingesetzt werden (z.B. elektronischer Dienstausweis, Anmeldung an elektronische Systeme).

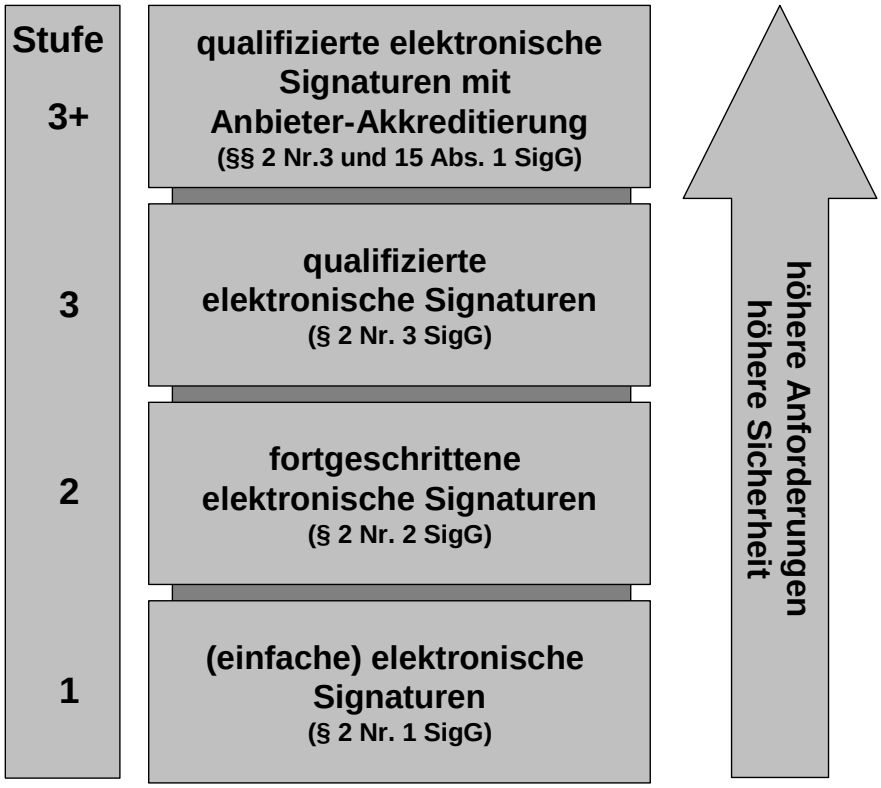
    Die - häufig im Vordergrund stehende - Frage der Verschlüsselung ist über andere Wege zu lösen.

Inhaltsverzeichnis

1. Welche Qualitätsstufen von Signaturen gibt es und worin liegen die wesentlichen Unterschiede?

Am 22.05.2001 ist das „Gesetz über die Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften“ (SigG) in Kraft getreten. Durch dieses Gesetz wurde die „EU-Richtlinie 1999/93/EG vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen“ (RLeS) in nationales - also deutsches - Recht umgesetzt; gleichzeitig wurde das bisherige „Gesetz zur digitalen Signatur“ i.d.F. vom 13. Juni 1997 (Signaturgesetz – SigG 1997) aufgehoben.

Wer sich erwartet hatte, dass das SigG gegenüber dem „alten“ Signaturgesetz von 1997 Vereinfachungen bringen würde, wurde leider enttäuscht. Während nämlich das SigG 1997 nur zwischen „signaturgesetzkonformen“ und „nicht signaturgesetzkonformen“ Signaturen unterschied, differenziert das neue Signaturgesetz - nicht zuletzt aufgrund der Vorgaben durch die EU-Richtlinie - nunmehr zwischen drei, bzw. bei genauer Betrachtung, vier unterschiedlichen Qualitätsstufen. Diese sollen nachfolgend näher beschrieben und ihre wesentlichen Unterschiede dargestellt werden.



1.1 (Einfache) Elektronische Signaturen

“Elektronische Signaturen“ im Sinne des SigG sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen (§ 2 Nr. 1 SigG).

(Einfache) elektronische Signaturen können damit Namenszeichen (z.B.: gez. Müller), Autosignaturen der Mailprogramme, elektronische Visitenkarten, aber auch eingescannte Unterschriften unter einem Dokument sein. Da sie nicht zweifelsfrei einer Person zugeordnet werden können, besitzen sie wenig Beweiswert; sie eignen sich für formfreie Vorgänge.

1.2 Fortgeschrittene elektronische Signaturen

Unter “fortgeschrittenen elektronischen Signaturen“ im Sinne des § 2 Nr. 2 SigG versteht man elektronische Signaturen, die

- ausschließlich dem Signaturschlüssel[1]-Inhaber zugeordnet sind,
- die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
- mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann[2] und
- mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Wenngleich gesetzlich kein Verzeichnisdienst gefordert wird, können „fortgeschrittene Signaturen“ - z.B. Pretty Good Privacy (PGP), Verisign und SPHINX - somit grundsätzlich Personen zugeordnet werden. Auch lassen sie die Integrität der signierten Dokumente, d. h., dass nachträgliche Veränderungen festgestellt werden können, erkennen.

Gleichwohl können „fortgeschrittene Signaturen“ weder im Privatrecht noch im Verwaltungsrecht eine gesetzlich angeordnete „schriftliche Form“ mit „eigenhändiger Unterschrift“ ersetzen.[3]

1Signaturschlüssel sind einmalige elektronische Daten wie private kryptografische Schlüssel, die zur Erstellung einer elektronischen Signatur verwendet werden (§ 2 Nr. 4 SigG)
2 Privater Schlüssel z.B. auf Diskette, die vor unbefugter Benutzung geschützt werden kann
3 § 126 a Abs. 1 BGB ; §§ 3 u. 37 VwVfG-E, Stand 01.03.2002 siehe: http://www.staat-modern.de/projekte/beschreib/Daten/g_verwaltungsverfahren.pdf (Zugriff am 21.05.2002)

1.3 Qualifizierte elektronische Signaturen

"Qualifizierte elektronische Signaturen" sind gemäß § 2 Nr. 3 SigG elektronische Signaturen, die zusätzlich zu den Qualitätsmerkmalen der „fortgeschrittenen elektronischen Signaturen"

- auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat[4] beruhen und
- mit einer sicheren Signaturerstellungseinheit[5] erzeugt werden.

"Qualifizierte Signaturen" werden von „Zertifizierungsdiensteanbietern"[6] ausgestellt. Sie entsprechen den europaweit geltenden Anforderungen der RLeS. „Qualifizierte Signaturen" können sowohl im Privatrecht als auch (künftig) im öffentlichen Recht die eigenhändige Unterschrift ersetzen, soweit gesetzlich nichts Anderes bestimmt ist (z.B. § 126 a Abs. 1 BGB; §§ 3a und 37 VwVfG-E).

Bei den „qualifizierten Signaturen" wird zwischen folgenden zwei Ausprägungen unterschieden:

- qualifizierte Signaturen **ohne** Anbieterakkreditierung
- qualifizierte Signaturen **mit** Anbieterakkreditierung[7].

1.3.1 Qualifizierte elektronische Signaturen ohne Anbieterakkreditierung

Der Betrieb eines Zertifizierungsdienstes im Rahmen des SigG ist genehmigungsfrei (§ 4 Abs. 1 SigG). Einen Zertifizierungsdienst darf jedoch nur betreiben, wer die nach § 4 Abs. 2 SigG geforderten Voraussetzungen erfüllt. Die Aufnahme des Betriebs eines Zertifizierungsdienstes ist der zuständigen Behörde (Regulierungsbehörde für Telekommunikation und Post; RegTP) anzuzeigen. Wesentlich dabei ist, dass die Erfüllung der genannten Voraussetzungen „nur" in geeigneter Form darzulegen ist (§ 4 Abs. 3 SigG). Es erfolgt somit grundsätzlich keine technische Überprüfung durch die RegTP.

---

4 „Zertifikate" sind elektronische Bescheinigungen, mit denen Signaturprüfschlüssel (sog. öffentliche Schlüssel; s. § 2 Nr. 5 SigG) einer Person zugeordnet werden und die Identität dieser Person bestätigt wird (s. § 2 Nr. 6 SigG).
„Qualifizierte Zertifikate" sind qualifizierte elektronische Bescheinigungen, welche die Voraussetzungen des § 7 SigG erfüllen und öffentliche Schlüssel natürlichen Personen zuordnen. Sie werden von Zertifizierungsdiensteanbietern ausgestellt, die mindestens die Anforderungen nach den §§ 4 bis 14 oder 23 des SigG und der sich darauf beziehenden Vorschriften der Rechtverordnung nach § 24 SigG erfüllen (s. § 2 Nr. 7 SigG).
5 „Sichere Signaturerstellungseinheiten" sind Software- oder Hardwareeinheiten zur Speicherung und Anwendung des jeweiligen Signaturschlüssels, die mindestens die Anforderungen nach § 17 oder 23 des SigG und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 SigG erfüllen und für qualifizierte elektronische Signaturen bestimmt sind (s. § 2 Nr. 10 SigG)
6 „Zertifizierungsdiensteanbieter" sind natürliche oder juristische Personen, die qualifizierte Zertifikate oder qualifizierte Zeitstempel ausstellen (s. § 2 Nr. 8 SigG)
7 Nach § 15 Abs. 1 SigG können sich Zertifizierungsdiensteanbieter auf Antrag von der RegTP akkreditieren lassen. Die Akkreditierung ist zu erteilen, wenn der Zertifizierungsdiensteanbieter nachweist, dass die Vorschriften des SigG und der Rechtsverordnung nach § 24 SigG erfüllt sind.

Ähnlich verhält es sich mit der über die gesamte Zeitdauer des Betriebs eines Zertifizierungsdienstes geforderten Erfüllung der in § 4 Abs. 2 SigG genannten Voraussetzungen. Die Zertifizierungsstellen unterliegen zwar der Aufsicht der RegTP, doch erfolgen keine regelmäßigen Prüfungen „von Amts wegen“, ob die Betriebsvoraussetzungen noch vorliegen. Der Zertifizierungsdiensteanbieter hat vielmehr „Umstände, die dies nicht mehr ermöglichen, der zuständigen Behörde unverzüglich anzuzeigen“ (§ 4 Abs. 4 SigG).

Für qualifizierte elektronische Signaturverfahren ohne Anbieterakkreditierung müssen die Dokumentation und der Verzeichnisdienst über die ausgestellten Zertifikate i.d.R. nur ab dem Zeitpunkt der Ausstellung für den im jeweiligen Zertifikat angegebenen Gültigkeitszeitraum sowie fünf weitere Jahre ab dem Schluss des Jahres, in dem die Gültigkeit des Zertifikats endet, aufbewahrt werden (s. § 10 SigG i.V. mit § 4 Abs. 1 und § 8 Abs. 2 SigV). Dieser Zeitraum kann sich verkürzen, falls ein nicht akkreditierter Zertifizierungsdiensteanbieter seinen Betrieb einstellt, da § 13 Abs. 1 SigG eine Übernahme durch einen anderen Anbieter oder die RegTP nicht zwingend vorsieht.

Qualifizierte elektronische Signaturverfahren ohne Anbieterakkreditierung garantieren somit technische und organisatorische Sicherheit, die allerdings nicht umfassend durch die RegTP geprüft ist. [8]

1.3.2 Qualifizierte elektronische Signaturen mit Anbieterakkreditierung

Qualifizierte elektronische Signaturen mit Anbieterakkreditierung stellen die höchste Stufe der elektronischen Signaturen dar. Sie entsprechen den Anforderungen, die das ursprüngliche Signaturgesetz an die digitalen Signaturverfahren gestellt hat.

Nach § 15 Abs. 1 SigG können sich Zertifizierungsdiensteanbieter auf Antrag von der RegTP akkreditieren lassen. Die Akkreditierung ist zu erteilen, wenn der Zertifizierungsdiensteanbieter nachweist, dass die Vorschriften des SigG und der SigV erfüllt sind. Akkreditierte Zertifizierungsdiensteanbieter erhalten ein Gütezeichen der RegTP.

Diese Stufe kann nach Art. 3 Abs. 7 RLeS für bestimmte Vorgänge des öffentlichen Bereichs gefordert werden. Diese Verwaltungsvorgänge müssen im Einzelfall genau festgelegt werden.

---

8 Siehe auch Rossnagel, „Die elektronische Signatur im Verwaltungsrecht“, in „Die Öffentliche Verwaltung“ – März 2001, S. 224

Akkreditierte Zertifizierungsdiensteanbieter werden von Prüf- und Bestätigungsstellen sowie von der RegTP vor der Aufnahme ihres Betriebes geprüft. Diese Prüfung und Bestätigung ist nach sicherheitserheblichen Veränderungen sowie in regelmäßigen Zeitabständen zu wiederholen (s. § 15 Abs. 2 SigG).

Qualifizierte elektronische Signaturverfahren mit Anbieterakkreditierung gewährleisten aber auch eine langfristige Prüfbarkeit der Zertifikate, da

- die ausgestellten qualifizierten Zertifikate ab dem Zeitpunkt ihrer Ausstellung für den im jeweiligen Zertifikat angegebenen Gültigkeitszeitraum sowie mindestens 30 weitere Jahre ab dem Schluss des Jahres, in dem die Gültigkeit des Zertifikates endet, in einem Verzeichnis zu führen sind (§ 4 Abs. 2 SigV);
- die RegTP gemäß § 15 Abs 5 SigG im Falle eines Widerrufs oder der Rücknahme einer Akkreditierung oder der Einstellung der Tätigkeit eines akkreditierten Zertifizierungsdiensteanbieters eine Übernahme der Tätigkeit durch einen anderen akkreditierten Zertifizierungsdiensteanbieter sicherzustellen hat. Falls dies nicht möglich sein sollte, hat die RegTP die Dokumentation selbst zu übernehmen. Bei nicht-akkreditierten Stellen ist dies in der Form nicht gewährleistet.

Qualifizierte elektronische Signaturen mit Anbieterakkreditierung verfügen über eine nachgewiesene organisatorische und technische Sicherheit und gewährleisten eine langfristige Überprüfbarkeit. Empfänger einer digital erzeugten Willenserklärung, die mit einer qualifizierten elektronischen Signatur mit Anbieterakkreditierung signiert worden ist, können sicher sein, in den Genuss des gesetzlichen Anscheinsbeweises nach § 292 a ZPO zu gelangen.[9]

1.4 Ausländische qualifizierte elektronische Signaturen

Nach § 23 Abs. 1 SigG sind elektronische Signaturen, für die ein ausländisches qualifiziertes Zertifikat aus einem anderen Mitgliedstaat der EU oder aus einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum vorliegt, qualifizierten elektronischen Signaturen ohne Anbieterakkreditierung gleichgestellt, wenn sie die Anforderungen des Art. 5 Abs. 1 RLeS erfüllen.

Nach § 23 Abs. 2 SigG werden solche gleichgestellten ausländische elektronische Signaturen nur dann als qualifizierte elektronische Signaturen mit Anbieter-

9 Siehe auch Rossnagel, „Die elektronische Signatur im Verwaltungsrecht“, in „Die Öffentliche Verwaltung“ – März 2001, S. 224, 225

akkreditierung (§ 15 Abs. 1 SigG) anerkannt, wenn sie nachweislich die gleiche Sicherheit aufweisen.

Dieser Sicherheitsnachweis ist gemäß § 23 Abs. 3 letzter Satz i.V. mit § 15 Abs. 7 SigG auch für ausländische Produkte zu führen, die für akkreditierte Signaturverfahren eingesetzt werden sollen.

Da bei diesem Anerkennungsverfahren die gleichen Nachweise wie bei den deutschen Signaturverfahren zu erbringen sind, weisen ausländische Signaturverfahren, die den deutschen qualifizierten Signaturverfahren mit Anbieterakkreditierung gleichgestellt sind, auch die gleiche hohe Sicherheit auf.

2. Kriterien für den Einsatz elektronischer Signaturen und die Auswahl der Qualitätsstufe

Wie im vorherigen Kapiteln dargestellt, ist die Auswahl an Signaturverfahren größer geworden. Damit sind aber auch die Entscheidung zur Verwendung elektronischer Signaturen und deren Rechtsfolgen auf den ersten Blick nicht leichter sondern schwerer geworden.

Im Folgenden sollen betrachtet werden:

- Auswirkungen der Signaturrichtlinie auf den Einsatz der Signatur im Verwaltungsverfahren,
- die bisherige gesetzgeberische Tätigkeit in Deutschland,
- die Auswirkungen der geplanten Gleichstellung von Schriftform und elektronischer Form im Verwaltungsverfahren und
- die notwendigen Aktivitäten für Fachgesetze und Ortsrecht sowie
- weitere Anwendungsgebiete für Signaturen, Zertifikate und Schlüsselpaare auf Chipkarten.

2.1 Verpflichtet die RLeS zur Einführung elektronischer Verfahren?

Ziel der EU-Richtlinie ist es, die sichere elektronische Kommunikation und den elektronischen Geschäftsverkehr voran zu bringen. Nach Erwägungsgrund 21 Satz 3 der RLeS unterliegt die Festlegung der Rechtsgebiete, in denen elektronische Dokumente und elektronische Signaturen verwendet werden, einzelstaatlichem Recht.

Wenn aber elektronische Signaturen zum Einsatz kommen, haben die Mitgliedsstaaten nach Art. 5 Abs.1 RLeS dafür Sorge zu tragen, dass die qualifizierte Signatur rechtlich die gleiche Wirkung wie die handschriftliche Unterschrift hat und im Gerichtsverfahren als Beweismittel zugelassen wird. Daraus ergibt sich für die Bundesrepublik Deutschland der Auftrag zur gesetzgeberischen Tätigkeit.

2.2 Bisherige gesetzgeberische Tätigkeit

Im Zuge der Umsetzung der RLeS gibt es eine Reihe von gesetzgeberischen Aktivitäten:

- Das Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (SigG) ist am 22.05.2001 in Kraft getreten. Es trifft aber zur Frage der Rechtswirkung der Signaturverfahren keine Aussagen.

- Die Verordnung zur elektronischen Signatur (Signaturverordnung - SigV)[10] wurde ebenfalls angepasst.
- Im Privatrecht wurde mit dem Gesetz zur Änderung des BGB[11], das am 01.08.2001 in Kraft getreten ist, durch einen neuen § 126a BGB die sogenannte elektronische Form unter Einsatz der qualifizierten elektronischen Signatur im Sinn des § 2 Nr. 3 SigG der Schriftform nach § 126 BGB gleichgestellt. In § 292 a ZPO wurde für die qualifizierte elektronische Signatur mit Anbieterakkreditierung der gesetzliche Anscheinsbeweis eingeführt.
- Für das Verwaltungsverfahrensrecht liegt der Entwurf eines Änderungsgesetzes vom 01.03.2002 vor[12] der für das Verwaltungsverfahrensgesetz des Bundes unter anderem in einem neuen § 3a Abs.2 bestimmt:

  Eine durch Rechtsvorschrift angeordnete Schriftform kann, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden .In diesem Fall ist das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen .Die Signierung mit einem Pseudonym , das die Identifizierung der Person des Signaturschlüsselinhabers nicht ermöglicht, ist nicht zulässig.

  Dies gilt grundsätzlich auch für den Verwaltungsakt nach den im Entwurf neu formulierten §§ 3a u.37 VwVfG-E als Ersatz für die durch Rechtsvorschrift vorgeschriebene Schriftform, wobei an die Signatur und das ihr zugrundeliegende qualifizierte Zertifikat hinsichtlich deren dauerhafter Überprüfbarkeit und deren technischer und administrativer Sicherheit zusätzliche Anforderungen gestellt werden können. Einzelheiten zur Erfüllung dieser Anforderungen sollen durch Rechtsverordnung des Bundesministeriums des Innern mit Zustimmung des Bundesrates geregelt werden können. Außerdem muss nach § 37 Abs. 3 Satz 3 VwVfG-E ein Verwaltungsakt, für den eine Schriftform vorgeschrieben ist, im elektronischen Verfahren die erlassende Behörde erkennen lassen. Diese soll dem zugrunde liegenden qualifizierten Zertifikat oder einem zugehörigen Attributzertifikat zu entnehmen sein.

  Diese Gleichstellung soll gleichermaßen in allen Verwaltungsverfahren in den Fällen gesetzlich angeordneter Schriftform gelten, sofern in den Fachgesetzen nicht ausdrücklich etwas anderes bestimmt ist.

---

10 Siehe BGBL I vom 21.11.2001, Seite 3074
11 Siehe Artikel 1 Nr.9 des Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 13.Juli 2001 BGBl. Nr.35 vom 18.Juli 2001 S.1542 ff.
12 Entwurf für das „Dritte Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften (3.VwVfÄndG)“ Stand 01.03.2002

- § 14 Abs. 4 Umsatzsteuergesetz wurde bereits dahingehend geändert, dass als Rechnung auch eine mit einer qualifizierten elektronischen Signatur mit Anbieterakkreditierung versehene elektronische Abrechnung gilt.

2.3 Was ist für die Fachgesetze, Verordnungen und das Ortsrecht zu tun?

Die Auswirkungen der elektronischen Signatur auf das Verwaltungsverfahren werden sowohl in rechtlicher als auch organisatorischer Hinsicht vielfältig sein. An dieser Stelle sollen nur solche näher betrachtet werden, die aus der Gleichstellung mit der Schriftform resultieren und für die erforderliche Qualität des Signaturverfahrens relevant sind.

Das Verwaltungsverfahren ist nach § 10 VwVfG an bestimmte Formen nicht gebunden, soweit keine Rechtsvorschriften für die Form des Verfahrens bestehen. Das Verwaltungsrecht enthält jedoch viele Vorschriften, in denen förmliches Handeln der Beteiligten gefordert wird. Die am meisten geforderte Form ist die Schriftform. Davon betroffen sollen ca. 3900 Vorschriften des deutschen Rechts sein, von denen die überwiegende Zahl dem öffentlichen Recht angehören dürften[13].

In der Definition der Schriftform unterscheiden sich allerdings Privatrecht und öffentliches Recht.

Für das **Privatrecht** definiert § 126 Abs. 1 BGB die Schriftform als eine Urkunde, die vom Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens unterzeichnet werden muss. Eigenhändig bedeutet dabei, dass der Aussteller sie auch tatsächlich selbst ausführt und eine Unterzeichnung durch Stempel, Maschinenschrift, Faksimile oder sonstige mechanische Hilfsmittel unzulässig ist.

Im **öffentlichen Recht** gilt § 126 Abs.1 BGB nur für materiell-rechtliche Willenserklärungen, nicht jedoch für Verfahrenshandlungen. Ist für ein bestimmtes Verfahren die Schriftform vorgeschrieben, so verlangt das Verwaltungsverfahrensrecht keine eigenhändige Unterschrift, sondern lässt nach § 37 Abs.2 VwVfG die Namenswiedergabe des zuständigen Behördenbediensteten ausreichen. Eine elektronische Abwicklung ist derzeit in den Fällen ausgeschlossen, in denen ein Fachgesetz neben der eigentlichen Schriftform noch ausdrücklich die eigenhändige Unterschrift vorschreibt.

13 Siehe Alexander Rossnagel, „Möglichkeiten für Transparenz und Öffentlichkeit im Verwaltungshandeln“ in „Verwaltungsrecht in der Informationsgesellschaft, S. 51

Auf den ersten Blick scheint mit der Änderung des VwVfG und der Verwaltungsverfahrensgesetze der Länder die Frage der elektronischen Abwicklung von Verwaltungsprozessen als beantwortet. Allerdings würde die Neuregelung die bisherige Möglichkeit verhindern, gesetzliche Schriftformklauseln entsprechend ihres Schutzzweckes so auszulegen, dass je nach Einzelfall z.B. auch eine einfache E-Mail ausreicht. Hier sollten Überlegungen ansetzen, die Einführung von E-Government auch als Chance zur Vereinfachung, zum Regelungsabbau und damit zur Entbürokratisierung von Verwaltungshandeln zu begreifen.

In den Fällen jedoch, in denen erhöhte Sicherheit beim elektronischen Verwaltungshandeln zwingend vorgeschrieben ist, ist für den entsprechenden Verwaltungsakt u.U. auch eine Erhöhung der Anforderungen an elektronisches Verwaltungshandeln gegenüber der bisherigen Rechtslage in der „offline-Welt“ nach § 37 Abs. 2 VwVfG[14] erforderlich.

2.3.1 Überprüfung auf Formerfordernisse

Wenn nach § 3a Abs. 2 bzw. § 37 VwVfG-E die elektronische Form der gesetzlich angeordneten Schriftform gleichgestellt wird, müssen trotz und gerade wegen dieses Automatismus alle Fachgesetze, aber auch das Ortsrecht überprüft werden.

Dabei sollten folgende Kriterien eine wesentliche Rolle spielen:

- Generell sollte der Anlass genutzt werden, die gesetzlichen Bestimmungen im Hinblick auf Vereinfachung und Verschlankung der Verwaltungsprozesse zu deren Optimierung im Interesse von Bürgern und Verwaltung auf entsprechende Potentiale zu untersuchen und gegebenenfalls anzupassen. Dies sollte nicht nur für Schriftformerfordernisse sondern auch für andere Formvorschriften wie z.B. persönliches Erscheinen, Vorlage von Unterlagen - insbesondere wenn sie von anderen Behörden ausgestellt werden - gelten. So könnten amtliche Bescheinigungen, die zur Vorlage bei anderen Behörden bestimmt sind, auch direkt elektronisch und ggf. signiert an die jeweils andere Behörde gesandt werden.
- Die Anforderungen an das elektronische Verwaltungsverfahren sollten grundsätzlich nicht höher als in der bisherigen und weiterhin zu ermöglichenden Form sein.

14 Siehe Martin Eifert, Online-Verwaltung und Schriftform im Verwaltungsrecht, K&R 2000 Beilage 2 S.11 ff.

- So sind die Schriftformfunktionen - wenn sie auch weiterhin notwendig sind - darauf zu überprüfen, ob tatsächlich immer die mit einer elektronischen Signatur verbundene Form zum Einsatz kommen muss oder ob nicht auch eine einfache - nicht signierte - E-Mail ausreichen kann.
- Wenn eine Signatur für erforderlich gehalten wird, gilt es grundsätzlich abzuwägen, welche Form der Signatur dies sein muss.
- Bei der Überprüfung der Fachgesetze werden sich auch Fälle ergeben, in denen trotz der Vorteile des E-Government die elektronische Form selbst unter Einsatz einer qualifizierten Signatur eines akkreditieren Zertifizierungsdiensteanbieters nicht als geeignet anzusehen ist. Im Privatrecht schließt beispielsweise die Neufassung des BGB in § 766 Satz 2 eine Bürgschaftserklärung - wegen deren erheblicher Bedeutung - in elektronischer Form aus.[15]

2.3.2 Schriftformfunktionen und ihre Umsetzungsmöglichkeiten im elektronischen Verwaltungsprozess

Die Schriftform hat im privaten und öffentlichen Recht bedeutsame Funktionen. Am Beispiel der Schriftformfunktionen wird in der als Anlage 2[16] beigefügten Übersicht im Hinblick auf die Notwendigkeit einer Signatur dargestellt, wie diese nach Prüfung und Abwägung im elektronischen Verfahren umgesetzt werden können.

Wichtig dabei ist, welche technische Qualität, d.h. insbesondere welche Form der Signatur ein elektronisches Dokument aufweisen muss, um als funktionales Äquivalent zur Schriftform gelten zu können.

Dabei ist zwischen umzusetzender Schutzfunktion, Aufwand und Nutzen beim Bürger, Verwaltungspraktikabilität, eigentlich bestehendem Verkehrsbedürfnis, derzeitiger Praxis und technischem Fortschritt abzuwägen und das jeweils erforderliche Sicherheitsniveau zu ermitteln.

Die als Ergebnis der Abwägung unterschiedlichen Sicherheitsniveaus elektronischer Formen erlauben es, das Sicherheitsbedürfnis bei einer formbedürftigen Erklärung genauer in rechtlichen Formerfordernissen abzubilden, als dies bei den Anforderungen der Schriftform der Fall ist. Entsprechend ist bei den bestehenden Formerfordernissen, auch soweit sie den Zweck einer Sicherheit der Identität des Absenders oder des Inhalts der Erklärung verfolgen, nicht pauschal auf eine funktionale Äquivalenz sicherer elektronischer Signaturen gegenüber der Schriftform

15 Siehe Artikel 1 Nr.9 des Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 13.Juli 2001 BGBl. Nr.35 vom 18.Juli 2001 S.1542 ff.
16 Siehe Klaus Eisele in „Rechtliche Rahmenbedingungen für das virtuelle Rathaus“ - Arbeitspapiere aus der Begleitforschung zum Städtewettbewerb Multimedia MEDIA@Komm, 4/2001, S.15 ff.

abzustellen, sondern das Sicherheitsbedürfnis eigenständig zu bestimmen und nach der entsprechend erforderlichen Abbildung in der „Online-Welt“ zu fragen.[17]

So kann die Abschlussfunktion durch textliche Erklärungen und deren Kontext und die Nutzung von elektronischen Formularen umgesetzt werden, ohne hierfür eine Signatur verlangen zu müssen. Für die Perpetuierungsfunktion ist keine Signatur notwendig, sondern ein entsprechend langfristig „lesbares“ Dateiformat. Für die Umsetzung der Kontroll- oder Integritätsfunktion kann für sich genommen auch eine Lösung unterhalb der qualifizierten Signatur zulässig sein.

2.4 Weitere Anwendungsgebiete für Signaturen, Zertifikate und Schlüsselpaare auf Chipkarten

2.4.1 Überprüfung der Identität

Gerade für das elektronische Verfahren wird vielfach gefordert, dass die Bürgerinnen und Bürger eindeutig identifizierbar sein müssten, um Missbrauch zu vermeiden. Hierzu werden derzeit in Fachkreisen vor allem folgende Lösungsmöglichkeiten diskutiert:

- **Zertifikatsdaten und Registrierungsdaten**

  Für die eindeutige Feststellung der Identität eines Bürgers sind die Zertifikatsdaten allein nicht ausreichend. Dies ist auch nicht Ziel der Signatur, die vielmehr eine Authentifizierung, d.h. Zuordnung von Signatur zu einer Person verfolgt.

  Im Streitfall müsste letztlich auf die bei der Registrierung erhobenen Daten wie Geburtsdatum, Wohnort, etc. zurückgegriffen werden können. Dies ist nach § 14 Abs. 1 Satz 3 SigG nur möglich, wenn es das Signaturgesetz erlaubt oder der Betroffene eingewilligt hat. Ein Auskunftsanspruch gegenüber den Zertifizierungsdienstanbietern besteht grundsätzlich nicht, bei Pseudonymen nur für die in § 14 Abs.2 SigG genannten Stellen und unter den dort genannten Voraussetzungen.

- **Zusätzliche Meldedaten auf der Chipkarte**

  Um eine Identifikation zu ermöglichen, könnten weitere Daten des Meldedatensatzes auf der Karte gespeichert werden. Eine solche Entwicklung hin zu

17 Siehe Martin Eifert, Online-Verwaltung und Schriftform im Verwaltungsrecht, K&R 2000 Beilage 2 S.15.

einem elektronischen Personalausweis ist derzeit nicht absehbar und für die Frage, welche Qualität von Signatur einzusetzen ist, nicht erheblich.

Gleiches gilt für Vorschläge, die Identifikationsnummer der Chipkarte oder die Zertifikatsnummer im Meldedatensatz zu speichern.

Allerdings sieht die künftige Interoperabilitäts-Spezifikation „ISIS-MTT“ ausdrücklich vor, dass Meldedaten (Geburtsdatum, Geburtsort, Geburtsname und ggf. Adresse) in das Signaturschlüsselzertifikat oder ein Attributzertifikat aufgenommen werden können.

- **Benutzerkennung und Passwort**

  Angesichts der noch niedrigen Verbreitung von elektronischen Signaturen in der Bevölkerung und dem Ziel der Minimierung des erwarteten Missbrauchspotentials einerseits und andererseits dem Bestreben, trotzdem kurzfristig Anwendungen anbieten zu können, wird von manchen Seiten eine Verwendung von Benutzerkennungen bzw. Passwörtern als Übergangslösung befürwortet. Dabei soll der Antragsteller bei seinem erstmaligen elektronischen Behördenkontakt eindeutig identifiziert werden.

  Dieser Weg nutzt keine Signaturen und lässt damit insbesondere die Vorteile von qualifizierten Signaturen und Zertifikaten außer Betracht.

2.4.2 Überprüfung der Integrität

Durch die elektronische Signatur kann festgestellt werden, ob ein Dokument verändert worden ist. Bei unsicheren Netzen, wie etwa dem Internet, sollte die Prüfung der Integrität grundsätzlich immer erfolgen.

Möglich ist eine Integritätsprüfung unter Verwendung asymmetrischer Schlüsselpaare mit fortgeschrittenen und qualifizierten Signaturen, gleich ob akkreditiert oder nicht. Sie erfolgt automatisch mit der Verifizierung der Signatur. Zusätzliche Kosten für Anfragen beim Zertifizierungsdiensteanbieters entstehen dabei nicht, da die Prüfung offline anhand des mit der Signatur mitgelieferten öffentlichen Schlüssels erfolgen kann.

2.4.3 Verschlüsselung

Für die Verschlüsselung von Daten können PKI-Strukturen (also Signaturen, Zertifikate und Schlüsselpaare) verwendet werden. Allerdings ergeben sich aus der datenschutzrechtlich oft zwingenden Notwendigkeit der Verschlüsselung von Kommunikationsdaten keine relevanten Kriterien für bestimmte Qualitäten der zu verwendenden Signatur.

- Es besteht **kein rechtlicher Zusammenhang** zwischen Verschlüsselung und Signatur. Die oben geschilderten gesetzlichen Regelungen im Zuge der Umsetzung der RLeS schaffen zwar einen Rahmen für das elektronische Signieren im Hinblick auf Zuordenbarkeit, Unverfälschtheit und Rechtswirksamkeit. Sie treffen aber keine Aussagen zur Gewährleistung der Vertraulichkeit. Solche finden sich in den verschiedenen Datenschutzgesetzen. Welche kryptographischen Verfahren dabei anzuwenden sind, ist Angelegenheit behördlicher Verantwortung und Sorgfalt, wobei beispielsweise die Hinweise der Datenschutzbeauftragten oder etwa des Bundesamtes für Sicherheit in der Informationstechnik (IT-Grundschutzhandbuch; http://www.bsi.de/gshb/deutsch/menue.htm) wichtige Anhaltspunkte sind.
- Eine sichere Verschlüsselung kann auch **unabhängig von PKI-Strukturen** realisiert werden. Namentlich bei der Verschlüsselung **synchroner** Kommunikation (z.B. Online-Auskunft) werden in der Regel aus Geschwindigkeitsgründen symmetrische Verfahren eingesetzt. Symmetrisch verschlüsselte Kommunikation beruht auf einem gemeinsamen, beiden Kommunikationspartnern bekannten Schlüssel, der nach Möglichkeit nur einmal zu verwenden ist (Sitzungsschlüssel)[18].

  Für die **asynchrone** Kommunikation (z.B. Versand von Dokumenten) sind auch asymmetrische (PKI-gestützte) Verschlüsselungsverfahren üblich. Die Qualitätsstufen von Signaturen (vgl. Nr. 1) haben allerdings keinen Einfluß auf die Qualität der Verschlüsselung. Diese wird durch andere Faktoren (z.B. Schlüssellänge) bestimmt.
- Die Verwendung "fortgeschrittener" oder "qualifizierter", also notwendig personenbezogener Zertifikate, impliziert eine **Ende-zu-Ende-Verschlüsselung** etwa vom Bürger zum kommunalen Sachbearbeiter. Das entspricht nicht den behördlichen Postordnungen und schafft Probleme im Vertretungsfall, die nur mit dem zusätzlichen Aufwand der Schlüsselhinterlegung zu bewältigen

18 Beispiel Secure Sockets Layer (SSL) bei der verschlüsselten Kommunikation mit einem Webserver. SSL schafft einen sicheren Tunnel im grundsätzlich offenen Internet auf der Basis symmetrischer Verschlüsselung. Lediglich der initiale Austausch des Sitzungsschlüssels erfolgt unter Verwendung eines zertifizierten öffentlichen Schlüssels (in der Regel des Servers), wobei der Client (Anwender) auch anonym bleiben kann.

sind[19]. Konzepte "sicherer Häfen" (z.B. elektronische Posteingangsstellen) sind deshalb bei der verschlüsselten Kommunikation mit Behörden vorzuziehen. Diese sind aber mit personenbezogenen Zertifikaten im Sinne des SigG schwierig zu realisieren.

Elektronische Signaturen sind "sicher" im Hinblick auf Authentizität, Integrität, Unabstreitbarkeit und Rechtswirksamkeit. Die Frage der Vertraulichkeit ist rechtlich davon getrennt zu sehen und technisch im möglichen, aber nicht im notwendigem Zusammenhang. Das heißt: vertrauliche elektronische Kommunikation ist nicht per se auch "sicher" im obigen Wortsinn - und umgekehrt. In der Praxis muß beides zusammengeführt werden. Verschlüsselungsanforderungen determinieren aber nicht die Qualität zu verwendender Zertifikate.

2.4.4 Zugangsberechtigung zu Datenbank, elektronischem Postfach, etc.

Ein weiterer Einsatzbereich kann die Authentifizierung von Nutzern sein, um Zugang zu einer Datenbank, einer Anwendung oder einem Postfach zu bekommen.

Um für diesen Zweck eine „starke“ und damit sichere Lösung anzubieten, könnten auch hier die Signaturzertifikate zum Einsatz kommen, wobei hierfür nicht die höchste Qualität erforderlich ist. Notwendig ist eine einmalige Bekanntmachung und Prüfung der Zertifikate bei der zuständigen Stelle, die dann eine Zugangberechtigung für das entsprechende Schlüsselpaar auf der Chipkarte einräumen kann.

Beispiele für eine solche „starke“ Authentifizierung sind der Zugang von Gemeinderatsmitgliedern zu nur ihnen zur Verfügung stehenden Sitzungsunterlagen mit unterschiedlichen Einsichtsrechten oder Zugänge zu Informationen für Nutzer, für die ein berechtigtes Interesse nachgewiesen werden muss, z.B. die Auskunft aus der Kaufpreissammlung.

19 Nicht zuletzt deshalb werden von den Zertifizierungsstellen getrennte Schlüsselpaare für das Signieren und für das Verschlüsseln ausgegeben.

3. Welche Qualitätsstufen der Signatur benötigen Bürger und Verwaltung für die Kommunikation miteinander?

Nach § 1 Abs.2 SigG ist die Verwendung von elektronischen Signaturen freigestellt, soweit nicht bestimmte Signaturen durch Rechtsvorschriften vorgeschrieben sind.

Die hierfür erforderliche Überprüfung der Fachgesetze wird noch einige Zeit in Anspruch nehmen.

Je nach dem Ergebnis der Abwägung werden sich für Bürger- und Verwaltungsseite unterschiedliche Anforderungen an die elektronische Abwicklung von Verwaltungsprozessen ergeben. So wird eine qualifizierte Signatur immer dann erforderlich sein, wo sie gesetzlich - z.B. über die Gleichstellung mit der Schriftform - vorgesehen ist. In anderen Fällen kann das Ergebnis sein, dass eine nur fortgeschrittene Signatur ausreicht oder überhaupt keine Signatur erforderlich ist. Schließlich darf aus der elektronischen Abwicklung nicht zwangsläufig die Notwendigkeit einer Signatur gefolgert werden.

Grundsätzlich sind also sowohl für Bürger als auch Verwaltung je nach Anwendung die verschiedenen Stufen der Signatur vorstellbar. Diese Skalierbarkeit entsprechend dem jeweils erforderlichen Sicherheitsniveau ermöglicht ein differenziertes Vorgehen.

Nachfolgend soll deshalb untersucht werden, welche Formen der Signaturen nach dem SigG aufgrund ihrer Eigenschaften, des mit ihnen zu realisierenden Sicherheitsniveaus und weiterer Rahmenbedingungen für einen Einsatz in Frage kommen sollten.

Einfache Signaturen nach § 2 Nr.1 SigG

Einfache elektronische Signaturen können technikneutral und ohne weitergehende Anforderungen - insbesondere nach dem SigG - angeboten und eingesetzt werden. Sie erfüllen keine Formerfordernisse und haben keinerlei Sicherheits- oder Beweiswert, können aber gleichwohl als Ausdruck einer Willensbekundung gelten und damit einen (formfreien) Verwaltungsakt auslösen. Sie können aber nicht als Unterschriften mit entsprechenden Rechtsfolgen, sondern allenfalls als Erkennenlassen des Ausstellers angesehen werden.

Fortgeschrittene Signaturen nach § 2 Nr.2 SigG

Fortgeschrittene elektronische Signaturen bieten zwar ein höheres Sicherheitsniveau als einfache, jedoch müssen keine spezifischen Anforderungen an die Sicherheit der organisatorischen Prozesse der Schlüsselverwaltung und der technischen Komponenten erfüllt werden. So können auch auf Software beruhende Schlüssel ohne Chipkarten verwendet werden.

Sie gehören ebenso wie die einfachen Signaturen zu den „folgenlosen“ sonstigen Verfahren nach § 1 Abs.2 SigG. Bisher werden in den Entwürfen zur Anpassung von Rechtsvorschriften stets die qualifizierte bzw. die dauerhaft überprüfbare Signatur (wird durch die qualifizierte Signatur eines akkreditierten Zertifizierungsdiensteanbieters erfüllt) verlangt.

Die elektronischen Signaturen im Sinn des § 2 Nr. 1 SigG und fortgeschrittenen elektronischen Signaturen im Sinn des § 2 Nr. 2 SigG sollten aus den nachfolgend genannten Gründen weder für Verfahrenshandlungen der Bürger noch der Verwaltung zum Einsatz kommen:

- Die oben beispielhaft genannte Vielfalt an Signaturen, die sich aus den unterschiedlichen Aufgaben ergibt, würde in der Praxis bei allen Beteiligten die Anforderungen an Verwaltungshandlungen hinsichtlich der erforderlichen bzw. zulässigen Signatur unüberschaubar machen und durch die unterschiedliche technische Ausgestaltung auch unpraktikabel sein. Hinsichtlich der Überprüfung auf der jeweiligen Empfängerseite würde sie unangemessenen Aufwand bedeuten. Der Eröffnung des Zugangs (vgl. § 3a VwVfG-E) kommt hier besondere Bedeutung zu. Die Verwaltung muß die von ihr verarbeitbaren Standards öffentlich bekannt geben können (z.B. über die Homepage).
- Mangels Kenntnis ihrer Qualität können auch fortgeschrittene elektronische Signaturen keine spezifische Handlungsform erfüllen und keine Beweiserleichterung genießen[20]. Nicht zuletzt aus diesen Gründen wird im BGB und den Entwürfen des Verwaltungsverfahrensgesetzes oder des Melderechtsrahmengesetzes soweit erforderlich die qualifizierte Signatur verlangt.

20 Siehe Alexander Rossnagel, Die elektronische Signatur im Verwaltungsrecht, Die öffentliche Verwaltung März 2001 Heft 6, S.224

3.1 Erforderliche Qualität der Signatur für Verfahrenshandlungen des Bürgers mit der Verwaltung

Nach den vorstehenden Ausführungen kommen für Verwaltungshandlungen der Bürger mit der Verwaltung nur folgende Alternativen in Frage:

- Für die elektronische Abwicklung ist keine elektronische Signatur erforderlich

  oder

- wenn eine Signatur notwendig ist, kommen nur eine qualifizierte oder eine qualifizierte Signatur eines akkreditieren Zertifizierungsdiensteanbieters in Frage.

Dabei wird vorausgesetzt, dass die elektronischen Verfahrenshandlungen der Bürger immer die für die Zuordnung zu einem Vorgang erforderlichen Absenderangaben enthalten.

3.1.1 Rahmenbedingungen für die Auswahl

Für die Beantwortung der Frage, welche Form der qualifizierten Signatur zum Einsatz kommen soll, sind neben den oben genannten Unterschieden auch einige Rahmenbedingungen zu berücksichtigen.

- Nach Art. 3 Abs. 7 RLeS können die EU-Mitgliedsstaaten den Einsatz elektronischer Signaturen im öffentlichen Bereich zwar möglichen zusätzlichen Anforderungen unterwerfen, diese müssen jedoch objektiv, transparent, verhältnismäßig und nichtdiskriminierend sein.

  So könnte in entsprechend begründbaren Ausnahmefällen zum Beispiel auch für Verfahrenshandlungen des Bürgers die qualifizierte Signatur eines akkreditierten Zertifizierungsdiensteanbieters verlangt werden.

  Häufig wird dies schon deswegen gefordert, weil die Signatur des Bürgers dauerhaft überprüfbar sein müsse und dies bei der qualifizierten Signatur eines nicht akkreditierten Zertifizierungsdiensteanbieters nur für einen zu kurzen Zeitraum möglich sei.

  Weitere Eigenschaften (siehe die eingangs dargestellten Unterschiede), die für die Notwendigkeit im Einzelfall sprechen können, sowie die geprüfte Sicherheit und die dadurch anzunehmende höhere wirksame Beweisvermutung, sollen dabei nicht verkannt werden.

- Art. 3 Abs. 7 RLeS verfolgt im Satz 3 aber auch das Ziel, jedem Bürger der EU die diskriminierungsfreie Wahl seines Signaturverfahrens zu ermöglichen, wenn es dort heißt, dass „diese Anforderungen für grenzüberschreitende

Dienste für Bürger kein Hindernis darstellen dürfen“. Dies kommt zum Beispiel für europaweite Ausschreibungen zum Tragen. Ein Hindernis würde eine Anforderung für grenzüberschreitende Zertifizierungsdienste für den Bürger darstellen, wenn er sie von einem anderen Mitgliedsstaat aus nicht erfüllen kann, z.B. weil Zertifikate von in Deutschland akkreditierten Trust-Centern in dem anderen Mitgliedsstaat nicht angeboten werden.

Dem folgt auch § 3a Abs.2 Satz 4 VwVfG-E.

- Die Forderung einer qualifizierten Signatur ist dem Bürger noch vermittelbar. Sie kommt auch im Privatrechtsverkehr mit entsprechenden Rechtswirkungen zum Einsatz[21].

  Die einzelfallbezogene Forderung nach einer qualifizierten Signatur eines akkreditierten Zertifizierungsdiensteanbieters mit dadurch wenigen Anwendungsfällen für den Bürger dürfte diese Akzeptanz beim E-Government nicht finden. Nutzer, deren elektronische Anträge zurückgewiesen werden, weil sie nur eine qualifizierte Signatur eines nicht akkreditierten Zertifizierungsdiensteanbieters haben, werden sich für diese wenigen Fälle keine zweite Signatur beschaffen.

- Die erstmalige und regelmäßige Überprüfung der administrativen und technischen Sicherheit durch die zuständige Stelle ist mit erheblichem Aufwand und Kosten verbunden, die von den akkreditierten Zertifizierungsdiensteanbietern zu erbringen sind.

  Ob sich dies auf die Kosten der einzelnen Karten, Lesegeräten und Dienstleistungen niederschlagen wird, ist derzeit noch nicht zu beurteilen. Gegenwärtig gibt es hierzu unterschiedliche Einschätzungen. Einerseits wird gesagt, es würden sich ohnehin alle Anbieter akkreditieren lassen, sodass es keine Kostenunterschiede geben werde, andererseits besteht die Ansicht, die Akkreditierung werde Auswirkungen auf die Kosten haben.

- Die bisher in der „offline - Welt“ grundsätzlich mögliche weitgehende Formfreiheit im Verwaltungshandeln stützt sich nicht zuletzt auch auf die Prüf- und Dokumentationspflichten der Verwaltung im Rahmen der Sachbearbeitung und Aktenführung. Wenn die Prüfung der Identität / Authentizität notwendig und wichtig ist, so gilt dies für die „offline- und online - Welt“ gleichermaßen: Nur dem antragsberechtigten Bürger steht ein Anwohnerparkausweis zu oder nur dieser darf Wohngeld erhalten.

21 Siehe Artikel 1 Nr.9 des Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 13.Juli 2001 BGBl. Nr.35 vom 18.Juli 2001 S.1542 ff.

Für die elektronische Signatur auf Bürgerseite bedeutet dies, dass die Verwaltung diese beim Eingang prüft und das Prüfungsergebnis bestätigt und aufbewahrt. Wenn dieses Prüfungsergebnis / Zertifikat wiederum von dem ausstellenden / bestätigenden Zertifizierungsdienstesanbieter signiert ist, sollte die Nachprüfbarkeit auch für die Zukunft gegeben sein, weil dessen Zertifikat wiederum bei der RegTP aufbewahrt wird.

- Das Verwaltungsverfahren endet im Regelfall mit einer Entscheidung der Behörde, die dem Bürger bekannt zu geben ist. Diese Entscheidung beinhaltet das Ergebnis vorangegangener Sachbearbeitung einschließlich Prüfung von Sachverhalten und Erklärungen. Sie beinhaltet - vor allem bei erstmaliger Bearbeitung eines Vorgangs - damit auch ein Prüfungsergebnis zur Identität des Antragstellers und seiner Angaben zur Person. Wenn diese Verwaltungsakte mit der qualifizierten Signatur eines akkreditierten Zertifizierungsdiensteanbieters der Behörde signiert werden (siehe Nr. 3.1.2) und damit lange nachprüfbar bleiben, sollte dies ausreichen.

3.1.2 Qualifizierte Signatur oder qualifizierte Signatur eines akkreditierten Zertifizierungsdiensteanbieters?

Für die qualifizierte Signatur mit Anbieterakkreditierung sprechen zunächst eine Reihe von Gründen:

- Geprüfte und bestätigte Sicherheit
- Qualifizierte Signaturen mit Anbieterakkreditierung verfügen über eine nachgewiesene organisatorische und technische Sicherheit (siehe Nr. 1.3.2). Als Nachweis der Sicherheit erhalten diese Signaturanbieter ein „Gütesiegel“.
- Langfristige Nachprüfbarkeit
  Für qualifizierte Signaturen mit Anbieterakkreditierung wird durch § 15 Abs. 6 SigG die langfristige Nachprüfbarkeit sichergestellt.

  Dabei ist zu berücksichtigen,

  - dass auch in der „offline - Welt“ bisher nicht in jedem Verfahren die Unterschrift unter einem Dokument oder die Integrität eines Dokuments überprüft werden. Etliche Verwaltungsverfahren können z.B. formlos, teilweise auch telefonisch, beantragt werden.

  - Wenn die Anforderungen gegenüber dem bisherigen Verfahren nicht unverhältnismäßig gesteigert werden sollen, wird auch im elektronischen Verfahren die Verifizierung der Signatur gegen das Trustcenter nicht der Regelfall sein müssen.

Da die Verifizierung von Signaturen gegen die Zertifizierungsdiensteanbieter mit Aufwand und Kosten verbunden ist, kann dabei auch differenziert vorgegangen werden:

- Bei einfacheren Verfahren mit kurzen Aufbewahrungsfristen kleiner fünf Jahre reicht die qualifizierte Signatur des nicht akkreditierten Zertifizierungsdiensteanbieters, da diese mindestens fünf weitere Jahre ab dem Schluss des Jahres, in dem die Gültigkeit des Zertifikates endet, in einem Zertifikatsverzeichnis geführt werden müssen und überprüft werden können.

  Die Begründung zu § 4 Abs.1 SigV führt dazu aus, dass „dieser Zeitraum im Hinblick auf die übliche Abwicklungsdauer der meisten Rechtsgeschäfte sowie eines Großteils der Verjährungsfristen – einschließlich der meisten Vermögensdelikte des StGB – und auch im europäischen Kontext angemessen erscheint.

- Bei komplexeren Verfahren insbesondere mit langen Aufbewahrungsfristen größer fünf Jahre könnte derselbe langfristige Nachweis auch bei der qualifizierten Signatur erreicht werden, wenn jede eingehende Signatur automatisch auf ihre Gültigkeit geprüft wird und das Prüfergebnis „in der Akte“ sicher und dauerhaft lesbar aufbewahrt wird. Wenn dieses Prüfergebnis des Zertifizierungsdienstanbieters obendrein noch mit dessen qualifizierter Signatur versehen ist, wäre die langfristige Nachprüfbarkeit für sich kein Grund für die Forderung einer qualifizierten Signatur eines akkreditierten Zertifizierungsdiensteanbieters.

- Wenn bei signierten elektronischen Dokumenten ein höheres Sicherheitsbedürfnis angenommen wird, muss davon ausgehend auch immer verifiziert und auch die Integrität überprüft werden. Mit dem Prüfergebnis kann wie oben bei komplexen Verfahren dargestellt, umgegangen werden.

Bezogen auf die langfristige Nachprüfbarkeit reicht für Verfahrenshandlungen des Bürgers mit der Verwaltung auch die qualifizierte Signatur eines nicht-akkreditierten Zertifizierungsdiensteanbieters. Das Ergebnis einer Abwägung und unter Berücksichtigung der Rahmenbedingungen kann deshalb entweder nur keine oder nur qualifizierte Signatur im Sinn des SigG lauten.

3.2 Erforderliche Qualität der Signatur für Verfahrenshandlungen der Kommune mit Außenwirkung

Die Kommune handelt nicht nur hoheitlich, sondern auch fiskalisch als Vertragspartner, z.B. bei Kauf- oder Mietverträgen. Deshalb sind sowohl die öffentlich-rechtlichen als auch die privat-rechtlichen Handlungen zu berücksichtigen.

3.2.1 Qualifizierte Signatur oder qualifizierte Signatur eines akkreditierten Zertifizierungsdiensteanbieters?

Für das **fiskalische Handeln** der Kommune im elektronischen Geschäftsverkehr ist nach den entsprechenden Bestimmungen des BGB (vgl. § 126 a BGB) die qualifizierte Signatur ausreichend. Im Hinblick auf die RLeS sind im Privatrecht auch keine darüber hinausgehenden Anforderungen zulässig.

Für die **öffentlich-rechtlichen Verfahrenshandlungen** der Verwaltung selbst muss die oben unter Nr. 2.3.1 aufgezeigte Prüfung von Fachgesetzen und Ortsrecht erfolgen.

Ansonsten kann nach § 3a Abs. 2 VwVfG-E ebenfalls eine auch nach Überprüfung durch Gesetz angeordnete Schriftform, soweit nicht Rechtsvorschriften etwas anderes bestimmen, durch die mit einer qualifizierten elektronischen Signatur im Sinn des Signaturgesetzes verbundenen elektronischen Form ersetzt werden.

Ist danach für einen Verwaltungsakt die Schriftform vorgeschrieben, können für die elektronische Form zusätzliche Anforderungen an die qualifizierte Signatur und das ihr zugrundeliegende Zertifikat gestellt werden. Diese zielen auf eine dauerhafte Überprüfbarkeit und deren technische und administrative Sicherheit. Das Bundesministerium des Innern kann die Einzelheiten zur Erfüllung dieser zusätzlichen Anforderungen durch eine Rechtsverordnung mit Zustimmung des Bundesrates regeln.

Solche zusätzlichen Anforderungen sind trotz Art. 3 Abs. 7 RLeS zulässig, da die RLeS nur Dienste für die Bürger regelt. Für die Verwaltungsseite können die Mitgliedstaaten den Einsatz elektronischer Signaturen im öffentlichen Bereich zusätzlichen Anforderungen unterwerfen.

Daraus ergeben sich Konsequenzen für die Wahl der Signatur im Verwaltungshandeln der Kommune:

- In verschiedenen Bereichen der Kommune wird für Verwaltungsakte die qualifizierten Signatur eines akkreditierten Zertifizierungsdiensteanbieters wegen

der weiterhin gesetzlich angeordneten Schriftform und § 37 VwVfG-E zum Einsatz kommen müssen, sofern sich die Kommune dem elektronischen Verfahren öffnet.

- Den Mitarbeiterinnen und Mitarbeitern kann ebenso wenig wie den Bürgerinnen und Bürgern zugemutet werden, unterschiedliche Signaturen für verschiedene Verfahrenshandlungen verwenden zu müssen. Verwaltungsintern entstünden dadurch außerdem zwangsläufig erhöhter Administrationsaufwand, Zusatzkosten und Akzeptanzprobleme. Es sollte also - soweit erforderlich - nur eine einzige Form der Signatur zum Einsatz kommen, nämlich die qualifizierte Signatur eines akkreditierten Zertifizierungsdiensteanbieters.
- Wenn man auf der Bürgerseite eine qualifizierte Signatur ausreichen lässt, weil die Verwaltung ihren Prüf- und Dokumentationspflichten nachkommt, dann muss hier die Sicherheit und langfristige Überprüfbarkeit gewährleistet werden. Damit können Verwaltungshandlungen und Ergebnisse der Sachbearbeitung langfristig nachprüfbar dokumentiert werden und eine Signaturstufe für alle notwendigen Fälle zum Einsatz kommen.
- Wenn die geprüfte und bestätigte administrative und technische Sicherheit sowie die langfristige Nachprüfbarkeit und in der Folge die Beweisvermutung des § 292a ZPO bei entsprechender Anwendung im Verwaltungsgerichtsverfahren wesentliche Vorteile der qualifizierten Signatur eines akkreditierten Zertifizierungsdiensteanbieters sind und nur durch eine solche gewährleistet werden können, sollte diese auch auf Verwaltungsseite zum Einsatz kommen.

Zusammenfassend ist der Verwaltung der Einsatz einer qualifizierten Signatur eines akkreditierten Zertifizierungsdienstanbieters aus folgenden Gründen zu empfehlen:

- sie kann für alle ihre Anwendungen bei Bedarf eine einheitliche Signatur einsetzen,
- sie muß dann nur diese administrieren,
- sie hat die Vorteile der geprüften und bestätigten Sicherheit sowie der Nachprüfbarkeit und
- auf Bürgerseite wird der Einsatz einer „nur qualifizierten Signatur“ ermöglicht.

3.2.2 Attributzertifikate

Die Behörden brauchen aus verschiedenen Gründen auch Attributzertifikate:

- Nach dem Entwurf des Änderungsgesetzes des VwVfG muss für den Verwaltungsakt nach § 37 die ausstellende Behörde entweder im Haupt- oder einem Attributzertifikat erkennbar sein.
- Da die elektronischen Signaturen nur für natürliche, nicht aber für juristische Personen - wie etwa Kommunen - ausgestellt werden, besteht die Möglichkeit, die Eigenschaft als Bediensteter einer Behörde oder den Zuständigkeitsbereich bei der Behörde über ein Attributzertifikat mitzuführen.

Aus diesem Grunde kommen einfache und fortgeschrittene Signaturen dann endgültig nicht mehr in Frage, da für sie gesetzlich keine Attributzertifikate vorgesehen sind.

4. Die elektronische Signatur bei der Kommunikation im internen Dienstbetrieb und mit anderen Behörden

Bei der elektronischen Kommunikation ist neben der Signatur (Authentizität und Integrität) auch die Verschlüsselung relevant: auf dem Weg vom Absender zum Empfänger wird die Nachricht vor der Kenntnisnahme durch Dritte geschützt. Bei der Kommunikation zwischen Behörden steht die Verschlüsselung häufig sogar im Vordergrund.

Pilotversuch SPHINX

Zur Vorbereitung von Sicherheitsmaßnahmen beim E-Mail-Verkehr in der gesamten Bundesverwaltung führte die KBSt in Zusammenarbeit mit dem BSI einen Pilotversuch zur „Ende zu - Ende-Sicherheit für den elektronischen Dokumentenaustausch“ durch. Zu diesem Zweck wurde eine Public Key - Infrastruktur (PKI) der öffentlichen Verwaltung durch das BSI aufgebaut und in Betrieb genommen. Diese PKI soll gemeinsam von Bund, Ländern und Kommunen genutzt werden. Die Piloterprobung diente dem Test und der Förderung von Produkten zur Signatur und Verschlüsselung von E-Mails mit dem Schwerpunkt einer „herstellerübergreifenden Interoperabilität“. Die in der PKI erzeugten Zertifikate ermöglichen Signaturen nach § 2 Nr. 2 SigG („fortgeschrittene elektronische Signatur“). Dies erlaubt die E-Mails generell zu verschlüsseln (für die Verschlüsselung hat der Gesetzgeber keine Regelungen erlassen), aber lediglich im formfreien Verwaltungshandeln elektronisch zu signieren.

Die elektronische Kommunikation fußt heute zum überwiegenden Teil auf der Anwendung des auf der Internet-Technologie basierenden E-Mail-Dienstes. Künftig werden elektronische Signaturen auch verstärkt Einzug in IT- gestützte Fachverfahren (z.B. Finanzverfahren, Dokumenten-Management-Systeme) halten.

Die „Aktenführung“ in der Verwaltung basiert überwiegend noch auf dem Medium Papier. Wenn auch das „papierarme Büro“ so schnell nicht Realität werden dürfte, werden künftig deutlich mehr Geschäftsfälle in elektronischer Form geführt werden.

Neben der „ad - hoc“ - Kommunikation via E-Mail werden - künftig zunehmend - Dokumente (als Teil oder Ganzes einer elektronischen Akte) in definierte, elektronisch abgebildete Verwaltungsabläufe (Workflows) eingespeist und ausgetauscht. In diesen Verfahren ist üblicherweise auch geregelt, wie die Unter- und Mitzeichnung erfolgen.

4.1 Anwendungsbereiche für die elektronische Signatur

Interne Kommunikation

Als interne Kommunikation wird hier die Verständigung auf elektronischem Wege zwischen Beschäftigten innerhalb einer Behörde verstanden. Dies bezieht sich z.B. auf den Nachrichten- und Dokumentenaustausch innerhalb einer Organisationseinheit (z.B. Sachgebiet, Abteilung) und darüber hinaus mit anderen Einheiten (z. B. zwischen zwei Verwaltungseinheiten), aber nicht außerhalb der (an ein gemeinsames logisches Netzwerk angeschlossenen) eigenen Verwaltung.

Weiter wird davon ausgegangen, dass die Kommunikation über ein sicheres Netz abgewickelt wird. Näheres dazu ist dem „IT- Grundschutzhandbuch“ des BSI[22] zu entnehmen.

Kommunikation mit anderen Behörden

Beim Nachrichtenaustausch mit anderen Behörden hat es die Kommunalverwaltung mit einer Vielzahl von Partnern zu tun. Obwohl diese zu der funktionalen Gruppe „Behörden“ gehören, herrschen höchst unterschiedliche Rahmenbedingungen.

Die Datenübermittlung erfolgt sowohl über offene (z. B. Internet) als auch geschlossene Netze (z. B. Behördennetze). Auch bei geschlossenen Netzen kann bei einer nicht mehr überschaubaren Anzahl von Teilnehmern nicht ohne weiteres auf ausreichende Sicherheit vertraut werden, da nicht bekannt ist, welche (ggf. ungeschützten) Übergänge aus dem geschlossenen Netz in unsichere offene Netze bestehen und Angriffe genauso „von innen“ versucht werden.

Es ist anzunehmen, dass die vielen verschiedenen Stellen (andere Kommunen, staatliche Stellen auf Landes-, Bundes- und Europaebene) unterschiedliche Verfahren der elektronischen Signatur anwenden.

4.2 Grundsätzliche Überlegungen

Welche Signatur bei der Kommunikation wofür in welcher Qualität eingesetzt werden soll, hängt von verschiedenen Faktoren ab, insbesondere:

22 Bundesamt für Sicherheit in der Informationstechnik (www.bsi.de)

- welche Qualitäts- bzw. Sicherheitsanforderung besteht im Einzelfall, z. B. aufgrund eines gesetzlichen Schriftformerfordernisses;
- was besagen behördeninterne Regelungen zur Unterschrift?

Nicht unberücksichtigt bleiben sollte auch, welche Signaturstufe eine Verwaltung für die externe Kommunikation einsetzt.

4.2.1 Sicherheitsanforderung

Die Unterschrift im internen behördlichen Geschäftsverkehr erfüllt keine andere Funktion als im Verkehr mit Bürgern und Wirtschaft. Sie kennzeichnet u. a. Abschluss-, Identitäts-, Kontroll- und Beweisfunktion.[23]

Zwischen Behörden wird ein gewisses Maß an gegenseitigem Vertrauen vorausgesetzt. Dies spricht zunächst dafür, dass eine starke Sicherung hinsichtlich der Authentifikation[24] nur von Fall zu Fall im Vordergrund steht. Die Datenintegrität[25] hängt u. a. vom gewählten Übertragungsweg und seiner Sicherheit ab.

Auch für die elektronische Kommunikation zwischen Behörden gilt grundsätzlich, dass die Sicherheitsanforderung im Einzelfall den Ausschlag für die Auswahl der angemessenen Signaturstufe gibt. Je höher der Sicherheitsanspruch, desto höher die Anforderung an die Qualität des Signaturverfahrens. Sind Formerfordernisse zu beachten oder wird eine Signatur aus sonstigen Gründen für notwendig erachtet, muss ein angemessenes Verfahren eingesetzt werden, auch wenn man vom erwähnten Vertrauensvorschuss ausgeht.

4.2.2 Nachprüfbarkeit

Neben der Sicherheit ist unter Umständen auch relevant, wie lange eine Signatur nachprüfbar bleiben muss. Zur Verpflichtung der Zertifizierungsdiensteanbieter, von ihnen ausgestellte qualifizierte Zertifikate in entsprechenden Verzeichnissen zu führen, vgl. Nr. 1.3.1. Vergleichbare Anforderungen gibt es für Zertifikate anderer Signaturverfahren (z. B. „einfache“ und „fortgeschrittene“ Signatur) nicht.

Die formale Anforderung, ein Dokument zu unterschreiben, ergibt sich entweder aus gesetzlichen Bestimmungen oder verwaltungsinternen Regelungen.

---

23 vgl. Fn 16; Anlage 2
24 „Entspricht der tatsächliche Absender dem angegebenen?“
25 „Wurden Daten auf dem Weg zwischen Absender und Empfänger verändert?“

In vielen anderen Fällen wird die Kommunikation trotzdem der Schriftform angeglichen abgewickelt, weil es sich um rechtserhebliche Vorgänge handelt bzw. es der Verwaltungspraxis entspricht.

4.3 Formerfordernisse

- **Einfache Signatur**
  Der Einsatz einer (einfachen) elektronischen Signatur im Sinn von § 2 Nr. 1 SigG ist nicht zielführend, da sie nicht zweifelsfrei einer Person zugeordnet werden kann und somit keinen ausreichenden Beweiswert besitzt. Gerade der Nachweis der Urheberschaft soll durch ein verwaltungsseitig festgelegtes Unterschriftserfordernis sicher gestellt werden - trotz der Ausgangslage, dass verwaltungsintern ein sicheres Netz vorhanden ist und behördenübergreifend ein gewisses Maß an Vertrauen vorausgesetzt wird.

  Neben der Authentifizierung des Absenders geht es bei der elektronischen Signatur auch um die Prüfung der Datenintegrität. Eine Manipulation an den Daten nach dem Signieren kann bei Einsatz einer einfachen elektronischen Signatur nicht nachgewiesen werden.

- **Fortgeschrittene Signatur**
  Signaturen nach § 2 Nr. 2 SigG bieten mehr Sicherheit als einfache elektronische Signaturen (vgl. dazu Nr. 1.2).

  Fortgeschrittene Signaturen erfüllen nicht die Voraussetzungen, um in der elektronischen Kommunikation bei Schriftformerfordernis die eigenhändige Unterschrift zu ersetzen. Für die interne wie für die behördenübergreifende Kommunikation ist überwiegend keine besondere Form erforderlich. In diesen Fällen würde deshalb eine fortgeschrittene Signatur ausreichen.

- **Qualifizierte Signatur**
  Nur Signaturverfahren, die auf qualifizierten Zertifikaten (§ 2 Nr. 3 SigG) oder qualifizierten Zertifikaten eines akkreditierten Zertifizierungsdiensteanbieters (§ 2 Nr. 3 i. V. m. § 15 SigG) beruhen, erfüllen die hier zugrunde liegenden Voraussetzungen - Nachweis von Authentizität und Integrität - und gelten als Substitut zur eigenhändigen Unterschrift.

4.3.1 Schriftformerfordernis aufgrund gesetzlicher Bestimmung

Ist aufgrund einer gesetzlichen Bestimmung die Schriftform erforderlich, muss bei der elektronischen Kommunikation ein adäquates Signaturverfahren zum Einsatz

kommen. Demnach ist mindestens eine qualifizierte elektronische Signatur (§ 2 Nr. 3 SigG) anzuwenden. Zu den unterschiedlichen Signaturstufen siehe Nr. 1.3.

Als Beispiel für eine gesetzlich angeordnete Signatur sei die Kassenanordnung im Haushaltswesen genannt (für Bayern: § 38 Abs. 1 Ziffer 9 KommHV; VV Nr. 20 zu Art. 70 BayHO).
Besondere gesetzlich festgelegte Formvorschriften gibt es z.B. auch für das Planfeststellungsverfahren (§§ 72 ff. VwVfG).

Soweit Vorschriften auch nach Anpassung des Rechts an den elektronischen Geschäftsverkehr in bestimmten Fällen besondere Formerfordernisse verlangen (z. B. Urkunde), bleiben diese unberührt.

4.3.2 Schriftformerfordernis aufgrund verwaltungsinterner Anordnung

Festlegungen zur Form der verwaltungsinternen Kommunikation liegen grundsätzlich in der Organisationshoheit des Verwaltungsträgers.

Allgemeine Regelungen zur Unterzeichnung finden sich meist in der „Allgemeinen Geschäftsanweisung“ bzw. „Allgemeinen Dienstordnung“ der jeweiligen Behörde.

Die Festlegungen, welche Schriftstücke von wem zu unterzeichnen sind, richten sich dabei nach dem Inhalt (z. B. Rats- und Ausschussvorlagen, Dienst- und Geschäftsanweisungen) bzw. der Form des Schriftstücks (z. B. Original) und / oder der Funktion der unterschriftsberechtigten Person (z. B. Oberbürgermeister). Dabei wird nicht explizit zwischen interner und externer Kommunikation unterschieden.

Besondere Unterschriftsregelungen liegen regelmäßig für bestimmte Fachbereiche wie z.B. das Haushalts-, Kassen- und Rechnungswesen vor.

Die bestehenden Unterschriftsregelungen sind überwiegend noch auf die papiergebundene Kommunikation ausgerichtet. Beim elektronischen Nachrichtenaustausch ist zu prüfen, ob die festgelegten Kriterien, die bislang ein Unterschriftserfordernis auslösen (formale und / oder materielle Voraussetzungen) gleichermaßen zutreffen. In der elektronischen Kommunikation läßt sich beispielsweise nicht mehr zwischen Original und Doppel unterscheiden.

Soweit verwaltungsintern ein Schriftformerfordernis gegeben ist, muss mindestens eine qualifizierte Signatur zur Anwendung kommen.

4.3.3 Kommunikation ohne Formerfordernisse

In den übrigen Fällen (weder gesetzlich oder verwaltungsintern geforderte Schriftform, noch sonstige besondere Formerfordernisse) besteht grundsätzlich Wahlfreiheit, die elektronische Kommunikation mittels elektronischer Signatur abzusichern.

Wie eingangs erwähnt, wird mittlerweile ein beträchtlicher Teil der elektronischen Kommunikation sowohl im internen Dienstbetrieb als auch zwischen Behörden formfrei über die elektronische Post abgewickelt. Diese E-Mails gelangen in der Regel vom Absender zum Empfänger, ohne dass beim Erhalt nachgeprüft wird bzw. werden kann, ob der behauptete mit dem tatsächlichen Absender übereinstimmt und ob der Nachrichteninhalt unterwegs verändert wurde. Diese Kommunikationsform hat sich in der Praxis herausgebildet, da in der Mehrzahl der Kommunikationsabläufe keine besonderen Sicherheitsanforderungen bestehen.

Ist eine Absicherung der Kommunikation mittels qualifizierter Signatur nicht notwendig, sollten keine zusätzlichen Verfahrensschritte (zwangsweise) eingebaut werden - auch wenn deren Handhabung noch so einfach sein sollte.[26]

4.4 Folgerungen

Ist aufgrund einer gesetzlichen Bestimmung die Schriftform bzw. eine vergleichbare elektronische Form gefordert, muss der Signatur ein Zertifikat zugrunde liegen, das der eigenhändigen Unterschrift gleichgestellt ist, d. h. eine qualifizierte Signatur nach § 2 Nr. 3 SigG.

Die verwaltungsinterne Kommunikation ist grundsätzlich formfrei und erfordert zum überwiegenden Teil keine Absicherung hinsichtlich Authentizität und Integrität.

Verlangen verwaltungsinterne Regelungen den Nachweis der Urheberschaft und die Gewissheit, dass der Nachrichteninhalt unverändert beim Empfänger angelangt ist - sei es in Form einer E-Mail oder als Anhang zu einer solchen - ist zumindest eine elektronische Signatur einzusetzen, deren Zertifikat eindeutig einer Person zugeordnet werden kann und die Datenintegrität gewährleistet (§ 2 Nr. 2 SigG).

[26] Angaben zum Absender in der elektronischen Nachricht stellen eine einfache Signatur i. S. d. § 2 Nr. 1 SigG dar (vgl. dazu auch Nr. 1.1). Absenderangaben sollte grundsätzlich jede elektronische Nachricht enthalten.

Die Frage, welche Signatur für die elektronische Kommunikation mit anderen Behörden notwendig ist, hängt neben eventuellen Formerfordernissen insbesondere davon ab, welcher Übertragungsweg gewählt wird (offenes oder geschlossenes Netz? Gilt das geschlossene Netz als sicher?).

Sinnvollerweise sollte nur **ein** Signaturverfahren Anwendung finden. Dieses muß die in bestimmten Fällen notwendigen hohen Qualitätsanforderungen (Ersatz für die eigenhändige Unterschrift) mit abdecken.

Zu beachten ist auch, welche Signaturstufe für die externe Kommunikation eingesetzt werden soll. Gerade die Kommunalverwaltung mit ihren vielen Beziehungen nach "draußen", kommt nicht ohne ein Signaturverfahren aus, das ebenfalls mindestens der eigenhändigen Unterschrift gleichgestellt ist (qualifizierte Signatur gem. § 2 Nr. 3 SigG). Es darf in Frage gestellt werden, ob ein paralleler Einsatz unterschiedlicher Signaturverfahren aufgrund einer Unterscheidung nach externer und interner Kommunikation Sinn machen würde. Man beachte den Verwaltungsaufwand, die Praktikabilität im alltäglichen Umgang, die Akzeptanz bei den Beschäftigten etc..

Unter Berücksichtigung der Ausführungen und Schlussfolgerungen des Kapitels 3 sollte verwaltungsintern die Signatur mit der höchsten organisatorischen und technischen Sicherheit eingesetzt werden.

5. Fazit

5.1 Signaturen für die Behördenkommunikation der Bürger und der Wirtschaft

Soweit eine **Schriftformerfüllung durch Unterschrift erforderlich** ist, wird sich für Verfahrenshandlungen des Bürgers und der Wirtschaft mit der Verwaltung die qualifizierte elektronische Signatur als Standard herausbilden. Für einzelne, genau bezeichnete Handlungen, kann zwar auch eine qualifizierte Signatur mit dauerhafter Überprüfbarkeit, wie sie von der Signatur mit Anbieterakkreditierung erfüllt wird, vorgeschrieben werden. Der Rahmen hierfür ist jedoch einerseits relativ eng und würde andererseits auch zu einer gewissen „Verwirrung“ bei Bürgern und Wirtschaft führen, welche Signatur für welchen Vorgang erforderlich wäre.

Ist **keine Schriftformerfüllung durch Unterschrift erforderlich**, sollte für Handlungen des Bürgers bzw. der Wirtschaft keine Signatur, d.h. auch keine niedrigere Signaturstufe (insbes. fortgeschrittene Signatur), vorgeschrieben werden. Für Handlungen, die bisher formlos (auch mündlich bzw. durch Telefonanruf) angestoßen werden konnten, dürfen künftig nicht aufgrund der Verfügbarkeit einer neuen Technik (elektronische Signatur) höhere Hürden gesetzt werden.

Unabhängig davon ist die Verwendung von einfachen Signaturen (z.B. Namenszeichen) immer möglich. Soweit keine besonderen Formerfordernisse eine qualifizierte Signatur erfordern, steht es Bürgern und Wirtschaft grundsätzlich auch frei, fortgeschrittene Signaturen bei der Kommunikation mit der Verwaltung einzusetzen. Aufgrund der großen Vielzahl unterschiedlicher Produkte und Standards bei den fortgeschrittenen Signaturen kann es allerdings - vor allem bei älteren Versionen - wegen der häufig nicht gegebenen Interoperabilität zu technischen Problemen kommen. Dies kann soweit führen, dass eingehende - nur signierte und nicht verschlüsselte - Nachrichten nicht mehr les- und verarbeitbar sind.

5.2 Signaturen für die Verwaltung

Soweit Verwaltungen **fiskalisch** handeln und dabei eine ggf. erforderliche Schriftform durch eine elektronische Signatur ersetzen möchten, benötigen sie hierfür mindestens eine qualifizierte Signatur nach dem Signaturgesetz.

Für Handlungen auf dem Gebiet des **öffentlichen Rechts** ist prinzipiell eine abgestufte Sichtweise denkbar. Es wird auch künftig viele Handlungen der Verwal-

tung geben, die – vor allem im internen Behördenverkehr - ohne Signatur durchgeführt werden können, denn Verwaltungsakte bedürfen nicht grundsätzlich der Schriftform.

Zusammengefasst ergeben sich damit für die Städte folgende Möglichkeiten:

- Die Mitarbeiter erhalten mindestens eine qualifizierte Signatur, soweit sie Aufgaben erfüllen, für die diese Stufe erforderlich ist. Die übrigen Mitarbeiter erhalten bei Bedarf eine niedrigere Stufe (fortgeschrittene Signatur). Eine derart heterogene Ausstattung würde jedoch aus verschiedenen Gründen zu erheblichen Problemen führen, nicht zuletzt deshalb, weil die verschiedenen Produkte nur eingeschränkt zueinander kompatibel sind. Auch stehen den eingesparten Sachkosten höhere administrative Aufwände gegenüber.

- Um diese Heterogenität zu vermeiden und den Administrationsaufwand so gering wie möglich zu halten, bietet es sich an, alle Mitarbeiter, die Aufgaben erledigen, für die eine qualifizierte elektronische Signatur vorgeschrieben ist, mit dieser auszustatten. Aufgrund der o.g. Argumente spricht jedoch viel dafür, qualifizierte Signaturen eines akkreditierten Anbieters einzusetzen.

  Weitere Mitarbeiter würden nur bei Bedarf mit personenbezogenen qualifizierten elektronischen Signaturen ausgestattet werden.

Möglicherweise können die Zertifikate darüber hinaus auch für andere dienstliche Zwecke eingesetzt werden (z.B. elektronischer Dienstausweis, Anmeldung an elektronische Systeme).

Die - häufig im Vordergrund stehende - Frage der Verschlüsselung ist über andere Wege zu lösen.

5.3 Verschlüsselung, Identifikation, Organisation der Signatureinführung

Zur Herstellung der Vertraulichkeit - vor allem bei der Übertragung personenbezogener Daten - ist eine Verschlüsselung der Daten erforderlich. Hierfür kann grundsätzlich die gleiche Technik wie bei der elektronischen Signatur verwendet werden. Die Zertifizierungsdiensteanbieter bieten diese Funktion i.d.R. auch mit eigenen Schlüsselpaaren auf der gleichen Chipkarte mit an. Die Verschlüsselung wird im Signaturgesetz nicht angesprochen und hat damit auch keinerlei Auswir-

kung auf die Frage der Qualitätsstufe von Signaturen. Sie war deshalb auch nicht Gegenstand dieser Ausarbeitung.

Mit den Zertifikatsangaben zu einer Person kann diese durch eine Online-Abfrage nicht eindeutig identifiziert werden. Hierzu wäre z.B. auch die Anschrift bzw. das Geburtsdatum erforderlich. Soweit im Rahmen eines elektronischen Geschäftsprozesses die Identität einer Person festgestellt werden muss, ist dies über andere Lösungen als der reinen Signatur zu realisieren.

Mit der Frage der Qualitätsstufe kann keine Aussage zur organisatorischen Einführung der Signatur (z.B. „Wie viele und welche Mitarbeiter erhalten eine Signatur?“) verbunden werden. Hierzu ist je nach Anforderung ein Einführungskonzept der jeweiligen Verwaltung erforderlich.

Die Fragen der Verschlüsselung, Identifikation und organisatorischen Einführung der Signatur werden in eigenen Ausarbeitungen des Deutschen Städtetags abgehandelt.

Anlage 1

Eigenschaften der verschiedenen Stufen der elektronischen Signaturen

Stufe der elektronischen Signatur	Eigenschaften							
	Die Signatur besteht aus elektronischen Daten, die anderen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen.	Die Signatur kann ausschließlich dem Signaturschlüssel-Inhaber zugeordnet werden.	Die Signatur wurde mit Mitteln erzeugt, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann.	Die Integrität der Daten wird durch die Signatur gewährleistet.	Die Signatur beruht auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat eines Zertifizierungsdiensteanbieters (ZA), welcher der staatlichen Kontrolle unterliegt.	Die Signatur wird mit einer sicheren Signaturerstellungseinheit erzeugt.	Eine Dokumentation und ein Verzeichnisdienst über die ausgestellten Zertifikate sind bis zum Ende des Jahres des Gültigkeitszeitraums vorgeschrieben.	Die unverzügliche Sperrung von Zertifikaten ist gewährleistet.
qualifiziert **mit** Anbieterakkreditierung (§ 2 Nr. 3 i.V.m. § 15 Abs. 1 SigG)	**X**	**X**	**X**	**X**	**X**	**X**	**zuzüglich 30 Jahre**	**X**
qualifiziert **ohne** Anbieterakkreditierung (§ 2 Nr. 3 SigG)	**X**	**X**	**X**	**X**	**X**	**X**	**zuzüglich 5 Jahre**	**X**
fortgeschritten (§ 2 Nr. 2 SigG)	**X**	**X**	**X**	**X**	–	–	–	–
einfach (§ 2 Nr. 1 SigG)	**X**	–	–	–	–	–	–	–

Eigenschaften der verschiedenen Stufen der elektronischen Signaturen

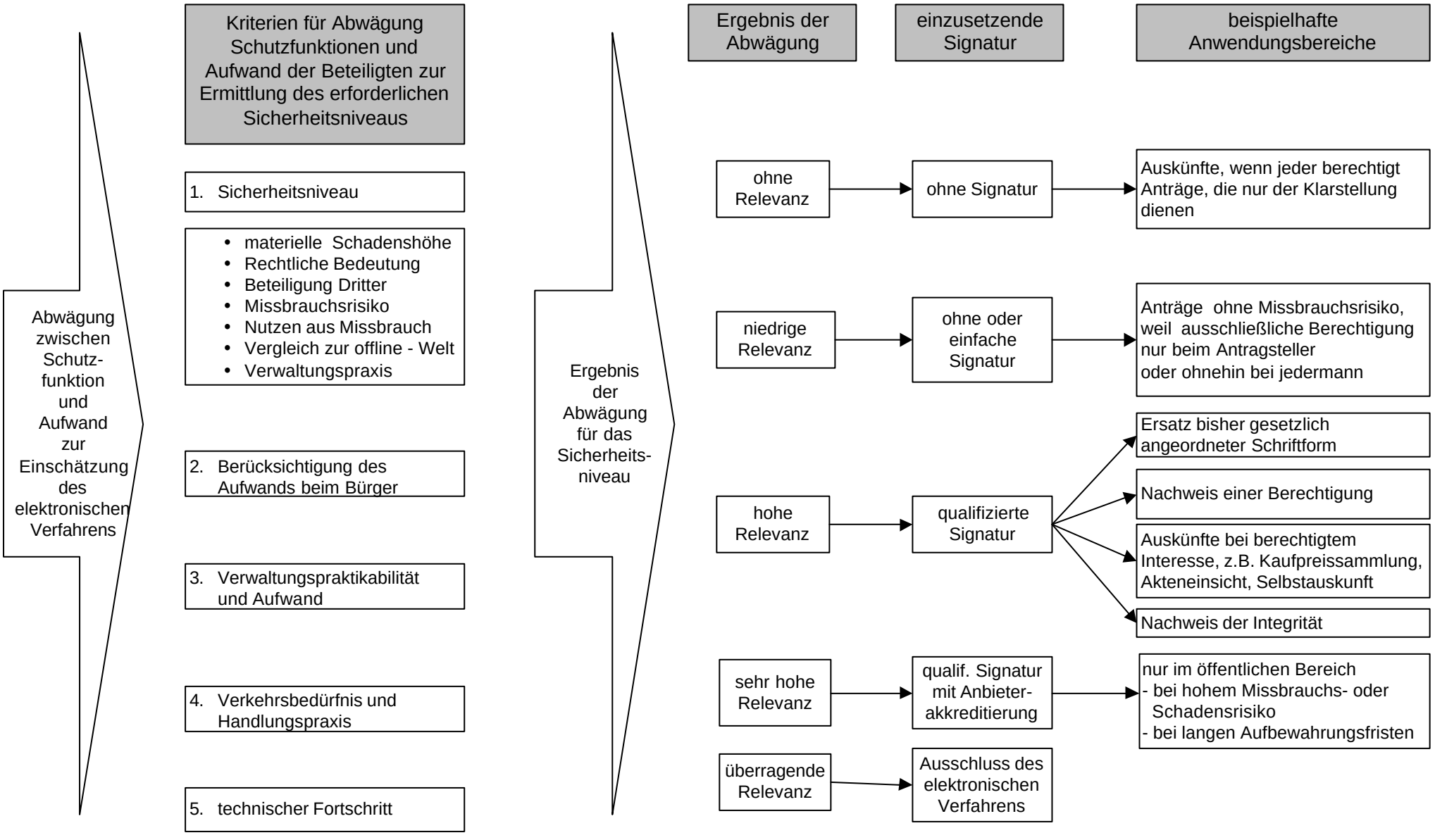
Stufe der elektronischen Signatur	Eigenschaften							
	Die Erfüllung der Anforderungen des SigG an die Signaturprüf und Signatur-anwendungskom-ponenten wird erklärt.	Der Zertifizie-rungsdienste-anbieter (ZA) ist bei der zuständi-gen Behörde (RegTP) akkreditiert.	Ein Nachweis dass die Anforderungen des SigG 2001 erfüllt werden, wird vom ZA vor Auf-nahme der Tätigkeit geführt.	Der ZA erhält ein Güte-zeichen der RegTP	Es erfolgt eine regelmäßige sicherheits-technische Überprüfung durch die RegTP	Eine Übernahme des Verzeichnisdienstes und der Dokumen-tation durch einen anderen akkre-ditierten ZA oder die RegTP wird bei Betriebs einstellung o. ä. garantiert.	Die elektronische Signatur ist geeignet, eine handschriftliche Unterschrift bei geforderter Schriftform zu ersetzen, falls gesetzlich nichts ande-res bestimmt ist.	Eine einfache Beweisführung durch den „Anscheins-beweis“ gemäß § 292 a ZPO ist möglich.
qualifiziert **mit** Anbieter-akkreditierung (§ 2 Nr. 3 i.V.m. § 15 Abs. 1 SigG)	**wird nachgewiesen**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
qualifiziert **ohne** Anbieter-akkreditierung (§ 2 Nr. 3 SigG)	**X**	–	–	–	–	–	**X**	**evtl.**
fortgeschritten (§ 2 Nr. 2 SigG)	–	–	–	–	–	–	–	–
einfach (§ 2 Nr. 1 SigG)	–	–	–	–	–	–	–	–

Anlage 2

Schriftformfunktionen und ihre Umsetzungsmöglichkeiten in elektronischen Verwaltungsprozessen

Zielsetzungen der Schriftform einschließlich Unterschrift	Funktionen	Sinn der Funktion	Umsetzbarkeit	grundsätzlich Rechts- änderung erforderlich
Schutzfunktionen				
Rechtsklarheit	Abschluss-funktion	Abgrenzung rechtsverbindlicher und willentlicher Erklärungen von bloßen Vorschlägen, Entwürfen,..	Sicherstellung über textliche Erklärung und deren Kontext Nutzung von Formularen	nein
	Identitäts-funktion	Erkennbarkeit des Erklärenden	Namensangabe des Ausstellers/ Absenders	nein
	Kontroll-funktion	Kontrollierbarkeit durch Dritte	Sicherstellung der Integrität durch Verschlüsselung und elektronische Signatur	nein
	Perpetuierungs-funktion	dauerhafte Lesbarkeit mit der Möglichkeit zur Überprüfung	"dauerhaftes" Dateiformat elektronische Archivierung	nein
Rechtssicherheit	Kontroll-funktion	Kontrollierbarkeit durch Dritte	Sicherstellung der Integrität durch elektronische Signatur	nein
	Echtheits-funktion	gewährleistet die inhaltliche Zuordnung der Erklärung zum Erklärenden und damit die Echtheit der Erklärung	Sicherstellung der Integrität und Authentizität des Ausstellers oder Absenders	ja
	Verifikations-funktion	Möglichkeit der Überprüfung der Echtheit durch den Empfänger insb. anhand der Unterschrift	Verifikation des Ausstellers/ Absenders und Prüfung der Integrität des Dokuments	ja
	Beweis-funktion	Herstellung dauerhafter Klarheit zum Nachweis der Erklärung	Anpassung des Prozessrechts Rechtsprechung	ja
Warnfunktion		der Erklärende wird zum Schutz vor übereilten Erklärungen auf die rechtliche Verbindlichkeit der Erklärung hingewiesen	- Warnhinweise in der Applikation - Nutzung von Formularen mit Hinweisen - Bestätigung vor dem Versand	ja

Anlage 3


Abwägung zwischen Schutz-funktion und Aufwand zur Einschätzung des elektronischen Verfahrens
Kriterien für Abwägung Schutzfunktionen und Aufwand der Beteiligten zur Ermittlung des erforderlichen Sicherheitsniveaus
1. Sicherheitsniveau
• materielle Schadenshöhe
• Rechtliche Bedeutung
• Beteiligung Dritter
• Missbrauchsrisiko
• Nutzen aus Missbrauch
• Vergleich zur offline - Welt
• Verwaltungspraxis
2. Berücksichtigung des Aufwands beim Bürger
3. Verwaltungspraktikabilität und Aufwand
4. Verkehrsbedürfnis und Handlungspraxis
5. technischer Fortschritt
Ergebnis der Abwägung für das Sicherheits-niveau
Ergebnis der Abwägung
einzusetzende Signatur
beispielhafte Anwendungsbereiche
ohne Relevanz
ohne Signatur
Auskünfte, wenn jeder berechtigt
Anträge, die nur der Klarstellung dienen
niedrige Relevanz
ohne oder einfache Signatur
Anträge ohne Missbrauchsrisiko, weil ausschließliche Berechtigung nur beim Antragsteller oder ohnehin bei jedermann
hohe Relevanz
qualifizierte Signatur
Ersatz bisher gesetzlich angeordneter Schriftform
Nachweis einer Berechtigung
Auskünfte bei berechtigtem Interesse, z.B. Kaufpreissammlung, Akteneinsicht, Selbstauskunft
Nachweis der Integrität
sehr hohe Relevanz
qualif. Signatur mit Anbieter-akkreditierung
nur im öffentlichen Bereich
- bei hohem Missbrauchs- oder Schadensrisiko
- bei langen Aufbewahrungsfristen
überragende Relevanz
Ausschluss des elektronischen Verfahrens