Entwurf

Verordnung des Bundeskanzlers, mit der die sicherheitstechnischen und organisatorischen Randbedingungen der Verwaltungssignatur festgelegt werden (Verwaltungssignaturverordnung – VwSigV)

Auf Grund des § 25 des Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz – E-GovG), BGBl I Nr. 10/2004 Art. 1, wird verordnet:

Signaturerstellungsdaten

§ 1. (1) Die Signaturerstellungsdaten der Verwaltungssignatur müssen hinsichtlich ihrer Schlüssellänge und ihrer Verwendbarkeit in Algorithmen den Signaturerstellungsdaten der sicheren Signatur im Sinne des § 2 Z 3 des Signaturgesetzes (SigG), BGBl. I Nr. 190/1999, entsprechen.

(2 Die Erzeugung der Signaturerstellungsdaten muss auf zufälligen Werten beruhen und es muss ausgeschlossen sein, dass sich Signaturerstellungsdaten eines Signators aus den Signaturerstellungsdaten anderer Signatoren errechnen lassen. Spezielle Hardwareelemente für die Erzeugung der Signaturerstellungsdaten sind nicht vorgeschrieben.

(3) Der eingesetzte Zufall muss auch mit hinreichend hoher Sicherheit ausschließen, dass es bei der Grundmenge an erwartbaren Zertifikaten zu zwei Zertifikaten mit gleichen Signaturerstellungsdaten kommen kann. Dazu müssen mindestens 128 Bit Zufall in die Erzeugung der Signaturerstellungsdaten eingehen und diese so gestaltet sein, dass die gesamten Signaturerstellungsdaten vom Zufall abhängig sind.

Signaturcode des Benutzers

§ 2. Der Signaturcode (PIN) des Benutzers einer Verwaltungssignatur darf in keinem System gespeichert sein und darf nach seiner Erstellung nur für den Benutzer verfügbar sein. Das System muss so ausgelegt sein, dass ein eingegebener PIN ausschließlich zur Erstellung von Signaturen und zum Wechsel des Signaturcodes an einen allenfalls beteiligten Sicherheitsserver übermittelt werden kann. Dabei darf der PIN weder auf dem Weg zur Signaturerstellungseinheit noch in der Signaturerstellungseinheit selbst über diese Transaktion hinaus gespeichert werden. Sofern der PIN nicht frei durch den Signator gewählt wird, muss die Erstellung des PIN ebenfalls auf Zufallselementen beruhen, sodass ein Errechnen des PIN aus den Schlüsselwerten oder aus anderen PINs nicht möglich ist.

Signaturerstellungsgeräte

§ 3. Signaturerstellungsgeräte für die Verwaltungssignatur können entweder Geräte beim Signator sein, die die Signaturerstellungsdaten hinreichend schützen, oder Signaturservices, die im Auftrag des Signators auf Sicherheitsservern eingerichtet sind. Die eigentlichen kryptographischen Funktionen der Signatur (z.B. RSA-Algorithmus oder elliptische Kurven) müssen den nachfolgenden besonderen Sicherheitsbedingungen genügen:

1. Im Falle des Signaturerstellungsgeräts beim Signator:
   a) Als Signaturerstellungsgeräte beim Signator sind nur Geräte zugelassen, die auf der Grundlage geeigneter Hardware die Signaturerstellungsdaten vor dem Ausspähen und Auslesen sowie vor der unbefugten Verwendung (ohne Einsatz der korrekten Signaturcodes) schützen.
   b) Der Schutz vor der unbefugten Verwendung hat auch den Schutz vor dem „wiederholten Ausprobieren“ von Signaturcodes zu beinhalten.

c) Die kryptographischen Operationen, die von den Signaturerstellungsdaten abhängig sind oder Zufallselemente benötigen, müssen zur Gänze auf dem Signaturerstellungsgerät durchgeführt werden. Ein Ermitteln der Hashwerte der zu signierenden Daten außerhalb des Signaturerstellungsgerätes ist zulässig.

d) Eine Evaluierung nach einem Protection Profile (A9C Referenznummern, Common Criteria) ist nicht zwingend vorgeschrieben. Liegt keine Evaluierung vor, so hat ein Gutachten gemäß § 4 Abs. 2 die Einhaltung der lit. a bis c zu bestätigen. Die Signatursoftware, die außerhalb des Signaturerstellungsgeräts zur Anwendung gelangt (Programmcode), muss nicht explizit geprüft sein, doch müssen die Unterlagen für eine allfällige Anlassprüfung durch den Hersteller verfügbar gehalten werden. Eine derartige Prüfung im Anlassfall ist bei Zwischenfällen oder bei begründetem Verdacht auf Kosten des Herstellers bzw. der ausgebenden Stelle durchzuführen.

2. Im Falle des Signaturerstellungsgeräts auf einem Sicherheitsserver

a) Das Erfordernis des Verbleibens der Signaturerstellungsdaten in der Verfügungsgewalt des Signators durch die Verwendung von nicht systematisch ermittelbaren Einmalcodes oder hinreichend starken kryptographischen Authentifizierungsmechanismen muss sichergestellt sein. Derartige Einmalcodes müssen, sofern diese unabhängig vom Signaturprozess an sich erzeugt werden können, auch gegen den Missbrauch durch das eigene Personal des Betreibers des Sicherheitsservers geschützt sein (z.B. durch alternative Verteilungswege). Auf diese Weise zu schützende (sicherheitskritische) Komponenten sind jedenfalls

aa) der Sicherheitsserver,

bb) der Mechanismus des Einmalcodes (Besitzkomponente, ausschließliche Verfügungsgewalt) und

cc) die Erzeugung und Verwendung des Signaturcodes (Wissenskomponente).

b) Der Einmalcode ist in den Fällen, in welchen das Gerät zur Präsentation des Einmalcodes an den Signator auch für andere Zwecke als zur Signatur verwendet wird oder die Abgabe von Einmalcodes nicht durch eine Wissenskomponente geschützt ist (PIN), mit einem Signaturcode zu kombinieren, damit die bewusste Verwendung im Rahmen der Signatur sichergestellt ist. Sofern der Einmalcode in einem Gerät oder mit einer Methode beim Signator erzeugt oder vorgehalten wird, muss der Signator in der Lage sein, sich hinreichend vor der missbräuchlichen Verwendung des Einmalcodes zu schützen. Außerdem muss sichergestellt sein, dass sowohl verwendete als auch nicht verwendete Einmalcodes aus der Vergangenheit nicht weiter verwendbar bleiben.

c) Als Sicherheitsserver wird jene Komponente bezeichnet, innerhalb der die Signaturerstellungsdaten des Signators zur Verwendung entschlüsselt werden können und auf Verfügung des Signators zur Anwendung gebracht werden. Der Sicherheitsserver darf nur sicherheitskritische Funktionen vergleichbarer Sicherheitsstufen umfassen (Signaturerstellung, Sperre und Widerruf, Vernichten von Signaturerstellungsdaten, Verschlüsselung, Erzeugung von Zufallswerten für die Kryptographie, Timestamping, etc.). Die Funktionen müssen vollständig dokumentiert sein und dürfen nicht dynamisch ergänzt werden.

d) Der Zugriff auf den Sicherheitsserver ist auf das absolut notwendige Mindestmaß beschränken (z.B. durch eine Firewall, die nur einen Dienst offen hält). Die Art der Beschränkung ist nachprüfbar zu dokumentieren.

e) Signaturerstellungsdaten dürfen außer zur Verwendung entsprechend der Verfügung des Signators während der Abarbeitung einer Signatur auf dem Sicherheitsserver nur in verschlüsselter Form abgelegt sein. Signaturerstellungsdaten können zum Betrieb und zur Sicherung außerhalb des Sicherheitsservers verschlüsselt gespeichert werden, wenn durch geeignete, starke kryptographische Maßnahmen sichergestellt ist, dass diese ausschließlich durch den Sicherheitsserver entschlüsselt werden können. Dieser Schlüssel muss organisatorisch (Vieraugenprinzip und Protokoll) und technisch (Safe) gesichert sein. In den Schlüssel zur verschlüsselten Speicherung ist der Signaturcode des Signators oder eine kryptographische Sicherung, die den Zugriffswillen des Benutzers zum gegebenen Zeitpunkt technisch sicherstellt, einzubinden, damit sichergestellt ist, dass ein Zugang zu den Signaturerstellungsdaten selbst dann nicht möglich ist, wenn die Inhalte der Speichermedien freigesetzt würden. Als Verschlüsselungsalgorithmen sind nur „starke“ Verschlüsselungen zulässig (> 100 Bit symmetrisch).

f) Signaturcodes und Einmalcodes sind auf dem Transport vom Benutzer zum gesicherten Bereich in geeigneter Weise kryptographisch zu schützen. Vorzugsweise ist eine Verschlüsselung vom Endgerät bis zum Sicherheitsserver vorzusehen.

g) Der Sicherheitsserver muss ohne Bedienung arbeiten. Sofern zu Betriebs- oder Wartungszwecken irgendwelcher Art ein Zutritt notwendig ist, ist dieser organisatorisch (Vieraugenprinzip und Protokoll) und technisch (geeignete Absperrung des Raumes) abzusichern.

h) Ein Zugang über Datenübertragung zum gesicherten Bereich ist außer für die definierten Sicherheitsservices nicht einzurichten (keine Remote Konsole, kein Telnet etc.)

i) Im Wartungsfall dürfen keine Datenträger aus der Hand gegeben werden. Diese sind, sofern sie nicht mehr verwendet werden oder nicht mehr verwendbar sind, in geeigneter Weise zu löschen und zu vernichten.

j) Es sind sämtliche Betriebs- und Wartungsarbeiten, soweit das System dies zulässt, auch automatisch zu dokumentieren. Die Dokumentation ist zumindest 5 Jahre aufzubewahren und muss allfälligen Audits zur Verfügung stehen.

Anforderung an die Prüfung der Geräte und Mechanismen

§ 4. (1) Eine Prüfung oder Zertifizierung nach einem Schutzprofil ist nicht vorgeschrieben. Jedenfalls ist aber ein Gerät als geeignet anzusehen, wenn es die Bedingungen der sicheren Signatur oder die Bedingungen der Geräte der Zertifizierungsdiensteanbieter für qualifizierte Zertifikate erfüllt.

(2) In den übrigen Fällen ist ein Gutachten über die Erfüllung der vorgenannten Bedingungen von einer Bestätigungsstelle im Sinne des § 19 SigG beizubringen. Das Gutachten hat auf die einzelnen Punkte der vorgenannten Bedingungen einzugehen und hat auch festzustellen, in welchen Zeiträumen ein Audit zur Aufrechterhaltung der Sicherheit notwendig ist. Die Schlussaussage des Gutachtens muss „nach den Anforderungen für die Verwaltungssignatur geeignet“ oder „nach den Anforderungen für die Verwaltungssignatur nicht geeignet“ lauten. Notwendige Betriebsbedingungen können in einem derartigen Gutachten festgestellt werden.

(3) Der Umstand, dass das Gerät für die sichere Signatur geeignet ist oder die Bedingungen der Geräte für Zertifizierungsdiensteanbieter erfüllt sowie dass notwendige Betriebsbedingungen in einem Gutachten festgestellt wurden, ist im Sicherheitsstatement des Zertifizierungsdiensteanbieters festzuhalten.

Identifikation

§ 5. Die Identifikation des Signators bei der Registrierung muss bei seiner Anwesenheit aufgrund der Vorlage eines amtlichen Lichtbildausweises erfolgen, andernfalls durch Zustellung der für die Freischaltung der Verwaltungssignatur notwendigen Informationen zu eigenen Handen.

Verzeichnisdienste

§ 6. Verzeichnisdienste für die Zertifikate der Verwaltungssignatur müssen verfügbar sein. Darüber hinausgehende Auflagen der Verfügbarkeit und Sicherheit werden nicht gestellt, sofern bei den verwendeten Signaturformaten in der Verwaltung das Zertifikat dem gültig signierten Dokument beigelegt wird.

Widerrufsdienste

§ 7. Der Widerruf eines Zertifikates ist zu veröffentlichen (Widerrufsdienst), es sei denn dass die Signaturerstellungsdaten ausschließlich im Sicherheitsserver verwendbar sind und infolge dessen mit dem Widerruf das Vernichten der Signaturerstellungsdaten sichergestellt ist. Das Vorliegen des letzteren Falles ist im Sicherheitsstatement des Zertifizierungsdiensteanbieters festzuhalten und als „automatischer und impliziter Widerrufsdienst“ zu bezeichnen.

Vorblatt

Probleme:

Gemäß § 25 DES E-Government-GesetzES (E-GovG), BGBl I Nr. 10/2004, dürfen im Rahmen der Bürgerkartenfunktion bis zum 31. Dezember 2007 auch Verwaltungssignaturen verwendet werden, die in diesem Zusammenhang den sicheren Signaturen gleichgestellt sind. Verwaltungssignaturen sind Signaturen, die im zulässigen Bereich ihrer Verwendung hinreichende Sicherheit bieten, auch wenn sie nicht notwendigerweise allen Bedingungen der Erzeugung und Speicherung von Signaturerstellungsdaten der sicheren Signatur genügen und nicht notwendigerweise auf einem qualifizierten Zertifikat beruhen. Die Definition der Eigenschaften einer Verwaltungssignatur hat gemäß § 25 Abs. 1 letzter Satz E-GovG durch Verordnung zu erfolgen.

Lösung:

Zur Festlegung der sicherheitstechnischen und organisationsrelevanten Voraussetzungen für das Vorliegen einer Verwaltungssignatur wird gemäß § 25 Abs. 1 letzter Satz E-GovG diese Verordnung erlassen.

Alternativen:

Keine. Die Schaffung dieser Verordnung ist der im E-Government-Gesetz vorgegebene Weg.

Auswirkungen auf die Beschäftigung und den Wirtschaftsstandort Österreich:

Die Schaffung von Verwaltungssignaturen ist für die Entwicklung der elektronischen Kommunikation in Österreich von großer Bedeutung und wird daher indirekt auch den Wirtschaftsstandort Österreich fördern.

Finanzielle Auswirkungen:

Keine:

Verhältnis zu Rechtsvorschriften der Europäischen Union:

Es bestehen keine entsprechenden gemeinschaftsrechtlichen Vorgaben..

Besonderheiten des Normerzeugungsverfahrens:

Keine.

Erläuterungen:

Die vorliegende Verordnung richtet sich in erster Linie an die Anbieter von Verwaltungssignaturen und Bürgerkarten. Es werden die dafür notwendigen sicherheitstechnischen und organisatorischen Randbedingungen klargestellt. Dabei wird die Einhaltung der Verordnung dadurch sichergestellt, dass bei der Ausstellung von Bürgerkarten die Mitwirkung der Stammzahlenregisterbehörde erforderlich ist.

Das Bürgerkartenkonzept des E-GovG geht an sich vom Einsatz sicherer Signaturen aus. Die sichere elektronische Signatur im Sinne der Signaturrichtlinie 1999/93/EG hat sich jedoch bisher nur wenig durchgesetzt. Dies ist ein Phänomen, das europaweit feststellbar ist. Daher wurde in den EU-Mitgliedstaaten auch verschiedentlich versucht, für eine Übergangszeit die Bedingungen der gegenüber der Verwaltung verwendbaren Signaturen so zu gestalten, dass möglichst viele Personen teilnehmen können und die Gefahr der Entwicklung einer Zweiklassengesellschaft verringert wird. In diesem Lichte sind auch die – bis 2008 einsetzbare – Verwaltungssignatur in Österreich und das Signaturbündnis in Deutschland zu sehen.

Die Signaturrichtlinie enthält keine Regelungen, die für den Eintritt bestimmter Rechtswirkungen die Verwendung bestimmter elektronischer Signaturen – insbesondere etwa der sicheren elektronischen Signatur -vorschreiben. Sie überlässt es vielmehr, wie in Erwägungsgrund 17 der Signaturrichtlinie ausgeführt wird, dem einzelstaatlichen Recht, Formvorschriften (in Gestalt bestimmter Signaturarten) für die Erzielung bestimmter Rechtswirkungen festzulegen. Nichts hindert daher den österreichischen Gesetzgeber, für die rechtliche Erheblichkeit von elektronischen Signaturen im öffentlichen Bereich auch Signaturen zuzulassen, die von den Erfordernissen für sichere Signaturen abweichen; Art. 3 Abs. 7 der Signaturrichtlinie zieht eine Grenze nur "nach oben" ein, indem er für die Verwendung von elektronischen Signaturen im öffentlichen Bereich festlegt, dass zwar zusätzliche Anforderungen – unter gewissen Voraussetzungen – aufgestellt werden dürfen, diese aber grenzüberschreitend für den Bürger kein Hindernis darstellen dürfen. Keinesfalls darf aus Art. 3 Abs. 7 geschlossen werden, dass die Signaturrichtlinie von einem Konzept ausgeht, wonach im öffentlichen Bereich grundsätzlich strengere Anforderungen an elektronische Signaturen zu stellen wären – sie erlaubt nur, dass dies in speziell zu begründenden Einzelfällen – ausnahmsweise – geschieht.

Die österreichische Verwaltungssignatur genügt den Anforderungen der Signaturrichtlinie: Sie weicht von den Erfordernissen für sichere elektronische Signaturen nur geringfügig ab – im wesentlichen nur dahingehend, dass ihr kein qualifiziertes Zertifikat zugrunde liegt – und sie stellt auch keine grenzüberschreitenden Hindernisse auf, da sie nach dem österreichischen Bürgerkartenkonzept auch Personen zugänglich ist, die weder österreichische Staatsbürger noch in Österreich wohnhaft sind. Die Verwaltungssignatur wird auch voraussichtlich wesentlich zur Aufgabe der Mitgliedstaaten beitragen können, die Verbreitung der elektronischen Signatur und die Stärkung des Vertrauens in dieses Instrument zu fördern, da sie geeignet ist, – insbesondere in Form der Handysignatur – einen größeren Teil der Bevölkerung zu erreichen, als dies die sichere Signatur auch infolge ihrer Kosten bisher vermocht hat.

Ein wesentlicher Grund für die Einführung der Verwaltungssignatur ist auch die Absicht der Mobilfunkbetreiber, elektronische Signaturen mittels Handy anzubieten. Es ist zu erwarten, dass damit ein besonderer Akzeptanzschub für die elektronische Signatur bewirkt werden kann. Der oft befürchteten Entwicklung einer Zweiklassengesellschaft könnte angesichts der extrem hohen Verbreitung der Mobiltelefone durch die Handysignatur wohl wirksam entgegengesteuert werden.

In einigen Bereichen der Verwaltung sind bereits elektronische Signaturen unter erleichterten Bedingungen eingeführt: So grenzt etwa die Verordnung über die elektronische Rechnungslegung die Anwendung der einschränkenden Bedingungen der sicheren Signatur deutlich ein und will mit dem Abstellen auf die „fortgeschrittene elektronische Signatur“ dieses Instrument ebenfalls einem breiteren Publikum zugänglich machen.

Die vorliegenden Regelungen über die Verwaltungssignatur verfolgen ähnliche Ziele: Sie gehen allerdings wesentlich deutlicher als die Regelungen über die fortgeschrittene Signatur im Bereich der elektronischen Rechnungslegung auf die konkreten Bedingungen der Verwendung der Signatur ein. Die Übernahme dieser konkretisierenden Bedingungen für die vor allem im Wirtschaftsbereich eingesetzte Signatur zur elektronischen Rechnungslegung wäre aus der Sicht des E-Government wünschenswert.

Eine Erleichterung der Bedingungen für die Verwaltungssignatur ist aus folgenden Gründen gerechtfertigt:

a) Durch die mit der Verwaltungssignatur in der Bürgerkarte verbundene Personenbindung ist eine hohe Qualität der die Person beschreibenden Daten (Identitätsdaten) sichergestellt.

b) Mit der Verwaltungssignatur wird ein Prüf- und Widerrufsmechanismus ermöglicht, der in seiner Qualität die Praxis der Prüfung manueller Unterschriften weit übersteigt.

c)In Umsetzung des Art. 3 Abs. 7 der europäischen Signaturrichtlinie können in einzelnen besonders begründeten Fällen auch noch zusätzliche Sicherheitsanforderungen getroffen werden, die dann auch im Einzelfall zu begründen sind.

Durch die Verwendung der Mechanismen, die das E-Government-Gesetz anbietet, wird in der Praxis gegenüber den bestehenden Verfahren im allgemeinen und gegenüber den bestehenden elektronischen Verfahren im besonderen eine deutliche Verbesserung der Kommunikationssicherheit erzielt.

Wesentliches Anliegen der vorliegenden Verordnung ist es auch, die von E-Government-Verfahren verlangte eindeutige Identifikation umzusetzen. Daher stellt die Verwaltungssignatur hinsichtlich der Feststellung der Identitätsdaten des Signators auf einen amtlichen Lichtbildausweis bzw. auf Verfahren ab, die auch nach der bestehenden Verwaltungspraxis den Nachweis der eindeutigen Identität bewirken. So etwa die Zustellung einer Zugangsberechtigung zu eigenen Handen, durch die z.B. bereits jetzt im Verfahren Finanz Online gewährleistet wird, dass die Identität des Zugangsberechtigten anlässlich der Zustellung überprüft wird.

In der vorliegenden Verordnung wird die spezielle Ausgestaltung der für sichere Signaturen gemäß § 2 Z 3 lit. a bis d SigG geltenden Anforderungen für die Verwaltungssignaturen näher geregelt. Die Vereinfachung der Anforderungen an Verwaltungssignaturen ist dabei insbesondere auch deswegen gerechtfertigt, weil die Randbedingungen ihres Einsatzes klar definiert sind. Angesichts ihrer Verwendung in Bürgerkarten-tauglichen Verfahren bedarf etwa der Aspekt einer gesicherten Anzeige des zu signierenden Inhalts keiner eigenen Regelung, da die Anzeige des Inhalts im Bereich von E-Government-Verfahren durch die Applikation selbst definiert wird und im Wege des Security Layer der Bürgerkarte spezifiziert ist.

a) Zum Erfordernis, dass die Signatur ausschließlich dem Signator zugeordnet sein muss (§ 2 Z 3 lit. a SigG):

Diese Bedingung wird durch die Pflicht zur ordnungsgemäßen Feststellung der Identität des Signators und durch die Definition der Anforderungen an die für die Erzeugung der Signaturerstellungsdaten einzusetzenden Algorithmen erfüllt.

b) Zum Erfordernis, dass das Signaturzertifikat die Identifizierung des Signators ermöglichen muss (§ 2 Z 3 lit. b SigG):

Abgesehen vom Fehlen der Kennzeichnung als „qualifiziertes Zertifikat“ unterscheidet sich das Zertifikat einer Verwaltungssignatur nicht von jenem einer sicheren Signatur. Da der Einsatz der Verwaltungssignatur im Rahmen der Bürgerkarte erfolgt, bedarf die Identifizierung des Signators der Verwaltungssignatur keiner zusätzlichen Regelung, da sie durch die Stammzahl in der Personenbindung auf der Bürgerkarte mit der Qualität einer ZMR-Abfrage gewährleistet ist. Eine darüber hinausgehende Identifizierung ist in Verwaltungsverfahren nicht üblich.

c) Zum Erfordernis, dass die Signatur mit Mitteln erstellt wird, die der Signator unter seiner alleinigen Kontrolle halten kann (§ 2 Z 3 lit. c SigG):

Auf diese Anforderung ist in der Verordnung das Hauptaugenmerk gerichtet, und zwar sowohl hinsichtlich der Technik der Signaturerstellung als auch hinsichtlich der Verwendung der Signaturerstellungsdaten. In der Verordnung wird auch die Umsetzung dieser Anforderung für den Fall der Verwendung eines Sicherheitsservers zur Erbringung des Signaturservice im Auftrag des Signators geregelt. Da dieser Fall bisher im wesentlichen nur im Bereich der Zertifizierungsdiensteanbieter vorgekommen ist, also in einem kontrollierten und hinsichtlich von Signaturen mit qualifizierten Zertifikaten auch der Aufsicht unterstellten Bereich, erscheint es sinnvoll, passende Rahmenbedingungen für den Einsatz von Sicherheitsservern für die Verwaltungssignatur festzulegen. Im Rahmen dieser Bedingungen wird z. B. auch die Vergabe von Signaturcodes besonders angesprochen.

d) Zum Erfordernis, dass die Signatur mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass jede nachträgliche Veränderung festgestellt werden kann (§ 2 Z 3 lit. d SigG):

Diesbezüglich sind besondere Regelungen hinsichtlich der Verwaltungssignatur nicht erforderlich, da ihre Verwendung im Rahmen der Bürgerkarte beziehungsweise durch die Applikation festgelegt ist und damit keine Gelegenheit besteht, von der Erfüllung dieser Bedingungen abzuweichen.

Die vorliegende Verordnung legt Randbedingungen für den Einsatz einer elektronischen Signatur nur gegenüber Behörden fest und greift nicht in den Gebrauch elektronischer Signaturen im zivilrechtlichen Bereich ein. Die Verwendung der Verwaltungssignatur und der im Zusammenhang damit festgelegten Bedingungen und Mechanismen ist allerdings auch im privaten Bereich aufgrund besonderer

Vereinbarung zulässig (vgl. Erwägungsgrund 16 der Signaturrichtlinie. Diesfalls wäre es ratsam, auf die gesamte Bürgerkartenspezifikation und nicht nur auf die Bedingungen der Verwaltungssignatur zurückzugreifen, da damit ein höheres Maß an Sicherheit und Vertrauen sichergestellt wäre. Bei der Verwendung von Signaturen im Zusammenhang mit wirtschaftsbereichsspezifischen Personenkennzeichen wird dies jedenfalls zu beachten sein.