STELLUNGNAHME

eIDAS-Durchführungsgesetze

Stellungnahme zum Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) Nr. 910/2014 und zur Aufhebung der Richtlinie 1999/93/EG

Stand: 1. November 2016

VITAKO
Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e.V.

VITAKO
Bundes-Arbeitsgemeinschaft der
Kommunalen IT-Dienstleister e.V.

Markgrafenstr. 22
10117 Berlin
☏ 030 - 20 63 156-11
030 - 20 63 156-22
wulff@vitako.de
www.vitako.de

VITAKO e.V. – Markgrafenstr. 22 – 10117 Berlin

Bundesministerium für Wirtschaft und Energie

11019 Berlin

1. November 2016

Stellungnahme zum Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
Kurz eIDAS Durchführungsgesetze-Entwurf samt Vertrauensdienstgesetz-Entwurf – eIDAS-DG-E samt VDG-E –

Sehr geehrte Damen und Herren,

wir bedanken uns für die Möglichkeit zur Abgabe zu einer Stellungnahme, auch wenn die Frist hierfür sehr eng bemessen war.

Vitako begrüßt die Initiative des Bundeswirtschaftsministeriums, zur Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt einen Entwurf zur Durchführung der Aufhebung der Richtlinie 1999/93/EG in das Gesetzgebungsverfahren zu geben.

Insbesondere sind wir erfreut, dass mit Art. 1 ein Vertrauensdienstegesetz eingeführt werden soll, dass das überkommene Signaturrecht mit Art. 11 ablösen soll. Die überwältigende Mehrheit unser Mitglieder, überwiegend kommunale Datenzentralen und deren Kunden (in der Regel Gemeinden mit deren Behörden), hat aus deren Sicht eine lange Geschichte mit der elektronischen Signatur hinter sich, die mit viel Aufwand, Rückschlägen und enttäuschten Erwartungen (Stichwort Einheitlicher Ansprechpartner) verbunden ist. Eine Erneuerung des Signaturrechts war daher aus unserer Sicht schon seit Jahren überfällig. Aus diesem Grund haben wir die Gesetzgebung der eIDAS-VO auch verhalten positiv begleitet. Positiv deshalb, weil endlich, insbesondere mit der Einführung des elektronischen Siegels und der Möglichkeit von Fernsignaturen,

notwendige Schritte in die richtige Richtung unternommen werden. Verhalten deshalb, weil zum einen doch viele Fragen, insbesondere durch nicht erlassene Durchführungsrechtsakte, offen blieben und zum anderen, weil aufgrund der bisherigen Weitergeltung des deutschen Signaturrechts, sehr viele Unsicherheiten hinsichtlich der Anwendbarkeit des neuen europäischen Signaturrechts aufkamen. Diese Rechtsunsicherheit nun zu beseitigen, trifft unsere volle Zustimmung.

Es ist uns bewusst, dass die eIDAS-VO eine Reihe von Vorgaben an die nationalen Gesetzgeber in den Mitgliedstaaten enthält, die von diesen umzusetzen waren bzw. sind. Dies waren nach unserem Verständnis die Fragen der Zulassung, der Aufsicht, der Haftung bzw. der Höhe von Bußgeldern und der Anerkennung. Wenn nun Dinge darüber hinaus geregelt werden, stellt sich unmittelbar die Frage, ab welcher Regelungstiefe dies nicht schon gegen das europarechtliche Umsetzungsverbot verstößt, bzw. warum der deutsche Gesetzgeber, wie schon bei der Umsetzung der nun aufgehobenen Signaturrichtlinie 1999/93/EG, nationale Sonderwege beschreitet, die so in andern Mitgliedstaaten nicht üblich sind.

Frappierend wird dies, wenn alte Signaturgesetzregelungen, die für die Besonderheiten von Zertifizierungsdiensteanbietern modelliert waren, nun in das Vertrauensdienstegesetz übernommen und auf alle Vertrauensdienste gleichermaßen angewandt werden sollen. Bestimmte Vorgaben, die für einen Dienst, der sich am Ende an natürliche Personen als Teilnehmer richtet, können nicht für Dienste passen, die Behörden und öffentliche Träger als Kunden haben. Insbesondere sehen wir diese Problematik für Vertrauensdiensteanbieter in der Ausprägung Bewahrungsdiensteanbieter gem. Art. 3 Nr. 16c i.V.m Nr. 19 bzw. Art. 34 eIDAS-VO, aber auch für Dienste für die Zustellung elektronischer Einschreiben gem. Art. 3 Nr. 36 i.V.m Nr. 19 bzw. Art. 43 f. eIDAS-VO.

Von herausgehobener Stellung ist für die öffentliche Verwaltung die Einführung der elektronischen Siegel nach Art. 3 Nr. 25 ff. eIDAS-VO. Mit der gewerbe- und technikregulierenden Einführung in der eIDAS-VO und nun im VDG ist aber noch kein Anwendungsfall geschaffen. Insofern freuen wir uns über die Aufnahme erster gesetzlicher Anwendungsfälle in Art. 2, 6, 7 und 8 des eIDAS-Durchführungsgesetz-E. Andererseits sind dies aus unserer Sicht viel zu wenige Fälle. Eine Verankerung in § 3a Abs. 2 VwVfG samt Simultangesetzgebung in den Ländern ist aus unserer Sicht dringend erforderlich, um die für das eGovernment notwendigen Effizienzsteigerungseffekte zu erzielen.

Uns ist bewusst, dass dies die Frage nach der Rechtsnatur der qualifizierten elektronischen Siegel im Vergleich zu den qualifizierten elektronischen Signaturen berührt, die als Ersatz der Schriftform dienen soll. Wenn aber in § 3a Abs. 2 VwVfG in Nr. 2 und 3 bei der Regelung des Schriftformersatzes durch die De-Mail eines akkreditierten Anbieters dieses Problem für den Erklärungswillen beim Behördenhandeln schon einmal geregelt wurde, sehen wir keine grundsätzlichen Bedenken dies auch für die qualifizierten elektronischen Siegel zu schaffen.

Daraus ergibt sich auch, dass die vielen Folgeänderungen in Art. 10 Anlass hätten sein sollen, an dieser Stelle auch ein Normenscreening in der Weise vorzunehmen, ob nicht auch alle Fälle, in denen eine „qualifizierte elektronische Signatur nach dem Signaturgesetz“ gefordert wird, in „qualifizierte elektronische Signaturen nach Artikel 3 Nummer 12 oder qualifiziertes elektronisches Siegel nach Artikel 3 Nummer 27 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73)“ zu ändern. Darauf hatten wir in einem viel umfangreicheren Rahmen gebaut. Wenn dies nun in dem eIDAS-Durchführungsgesetz-E nicht enthalten ist, sollte das kein Grund sein, dies nicht mit erhöhtem zeitlichen Druck nachzuholen.

Auf keinen Fall darf die genannte Auflistung der vier Regelungen abschließend bleiben. Damit müsste das deutsche E-Government einen erneuten Rückschlag hinnehmen.

Zu einzelnen Regelungen nehmen wir wie folgt Stellung:

Zu § 4 VDG-E

In der Begründung zu § 4 VDG-E wird im ersten Absatz auf die alte SigG-Regelung abgestellt und in den folgenden drei Absätzen auf den Qualifikationsstatus. In § 4 VDG-E wird aber nicht zwischen qualifizierten und nichtqualifizierten Vertrauensdiensteanbietern unterschieden, sondern pauschal nur von Vertrauensdiensteanbietern gesprochen und auf Artikel 17 Absatz 4 eIDAS-VO verwiesen, was in Artikel 17 Absatz 3 eIDAS-VO der Fall ist. Gegenüber einem nichtqualifizierten Vertrauensdiensteanbieter erscheint die Ausübung der Befugnisse aus § 4 VDG-E aber als viel zu eingriffsintensiv gemessen daran, dass ein nichtqualifizierter Vertrauensdiensteanbieter ein eingerichtetes und ausgeübtes Gewerbe betreibt, ihm aber nach Antrag von der Aufsichtsstelle der Status eines qualifizierten Anbieters verliehen wurde und er im Zweifelsfalle gar nicht weiß, dass er einen Vertrauensdienst betreibt, dass außerdem die Aufsichtsstelle für ihn zuständig ist, geschweige denn, diese Eingriffsrechte besitzt. Aus diesem Grund schlagen wir eine Klarstellung vor, dass § 4 VDG-E sich nur auf qualifizierte Vertrauensdiensteanbieter gem. Art. 17 Abs. 3a eIDAS-VO bezieht.

Zu § 7 VDG-E

Wie schon im alten Signaturgesetz wird auch im Entwurf eines Vertrauensdienstegesetzes eine Regelung über den Datenschutz aufgenommen. Anders als bei der Umsetzung der Signaturrichtlinie gibt es in Art. 5 eIDAS-VO nun aber eine eigene, direktwirkende Regelung zum Datenschutz. Dies stellt zwar auf die Richtlinie 95/46/EG ab, die im deutschen Bundesdatenschutzgesetz umgesetzt wurde. Mit der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), die nach Art. 99 zwar erst ab dem 25. Mai 2018 in Kraft tritt, wird nach Art. 94 die Richtlinie 95/46/EG mit Wirkung vom 25. Mai 2018 aufgehoben, so dass Verweise auf die aufgehobene Richtlinie als Verweise auf die Datenschutz-Grundverordnung gelten. In diesem Sinne erscheint es ausreichend, den Datenschutz durch die Datenschutz-Grundverordnung geregelt zu lassen.

Wenigstens sollte in § 7 eine Beschränkung aufgenommen werden, dass mit Wirkung vom 25. Mai 2018 die Datenschutz-Grundverordnung bis dahin bestehende Regelungen ablöst.

Allerdings stellt sich auch so schon die Frage, ob die Regelungen wirklich für alle Ausprägungen von Vertrauensdiensten geeignet sind. Zum einen erscheint es in Kommunikationsszenarien von elektronischen Einschreib-Zustelldiensteanbietern kaum darstellbar, dass die Einwilligung zur Verarbeitung personenbezogener Daten unmittelbar beim Betroffenen eingeholt wird. Nachrichten, die von Teilnehmern fremder elektronischen Einschreib-Zustelldiensteanbieter in ein System des eigenen elektronischen Einschreib-Zustelldienstes gesandt werden, dürften danach nur verarbeitet werden, wenn der fremde Teilnehmer vorab in die Datenverarbeitung eingewilligt hat. Das mag in geschlossenen Benutzergruppen funktionieren, diese sind aber nach Art. 2 Abs. 2 gerade nicht durch die eIDAS-VO reguliert. Darüber hinaus gibt es für die De-Mail sektorspezifische eigene Regelungen. Zum anderen dürfte die unmittelbare Einwilli-

gung auch bei Vertrauensdiensten in der Ausprägung Bewahrungsdienst nach Art. 3 Nr. 16c i.V.m Nr. 19 bzw. Art. 34 eIDAS-VO nicht möglich sein.

Zu § 11 VDG-E

In § 11 wird ausgeführt, dass bestimmte Attribute (Vertretungsmacht, berufsbezogene und sonstige Angaben) in Zertifikaten oder in gesonderten Attributzertifikaten enthalten sein können. Dieses steht im Einklang mit Artikel 24 eIDAS-VO. Gleichzeitig gibt es in diesem Kontext aber eine Standardisierungslücke, da ETSI diese Attribute in der einschlägigen ETSI EN 319 412-2 bisher nicht profiliert hat. Dort findet sich nur der normative Hinweis auf den IETF RFC 3739, der ein qualifiziertes Zertifikatsprofil beschreibt und den IETF RFC 5280, der das grundsätzliche Zertifikatsprofil definiert. Einen Hinweis auf mögliche Attribute im oben genannten Sinne findet sich nicht in der EN.

Die Deutsche Profilierung CommonPKi hat signaturgesetzkonforme ausschließliche Attribute als private Extensions, die nicht international standardisiert sind, in Stammzertifikaten oder als Attribute in Attributzertifikaten definiert. Eine EU-weite Interoperabilität ist somit nicht gegeben. Eine Anzeige der Inhalte und automatisierte Auswertung ist in der Regel im EU-Ausland nicht möglich. Technisch gesehen sind Validierungskomponenten zunächst aber einmal generische Prüfkomponenten, d.h. es reicht im Prüfprotokoll nur die Inhalte dieser Attribute anzuzeigen und die Gültigkeit der Attributzertifikate zu prüfen. Den grenzüberschreitenden Austausch von mit Attribut-Zertifikaten signierten Objekten halten wir für problematisch. Die Anwender in den empfangenden Mitgliedstaaten könnten im Zweifelsfall diese Informationen nicht interpretieren. Ebenso wie Anwender in Deutschland nicht mit alternativen proprietären Spezifikationen aus anderen Mitgliedstaaten umgehen können, da diese Profilierungen nicht bekannt sind.

Aus kommunaler Sicht erscheint es problematisch, dass gemäß § 11 Abs. 1 in den Zertifikaten Attribute zur Vertretung aufgenommen werden. Der Nachweis dafür ist nur zu einem einzigen Zeitpunkt zu erbringen, während die Verwendung fortlaufend erfolgt. Es wäre das Risiko der öffentlichen Verwaltung, diesem Nachweis zu glauben und es kann nicht Aufgabe der Verwaltung sein, die aktuelle Pflege von Arbeitgeber-/Arbeitnehmerbeziehungen und Vertretungsbefugnissen sicherzustellen. Die zusätzlichen Attribute besitzen insoweit nicht die dauerhafte Glaubwürdigkeit und Beweiskraft wie der eigentliche Identitätsnachweis.

Zu § 13 VDG-E

Es stellt sich grundsätzlich die Frage, warum die Frage des Widerrufs qualifizierter Zertifikate in dieser Art und Weise auf gesetzlicher Ebene erfolgt. Üblicherweise sind dies Themen, die ein Zertifizierungsdiensteanbieter in seine Certification Policy bzw. in seinem Certification Practice Statement regelt bzw. auf Grundlage seiner Allgemeinen Geschäftsbedingungen mit seinen Kunden vereinbart. Es sollte dann die Aufgabe der Konformitätsbewertungsstelle sein zu prüfen, ob die Vorgaben der eIDAS-VO, insbesondere aus Art. 24 Abs. 3 hinreichend sicher umgesetzt wurden. Als dies in der Signaturrichtlinie 1999/93/EG nicht geregelt war, hatte der deutsche Gesetzgeber die Möglichkeit, aber nicht die Verpflichtung, diese Frage des Widerrufs in seinem Signaturgesetz umsetzen.

Es stellt sich nun die Frage, ob dieses Thema nicht durch die eIDAS-VO abschließend geregelt ist und es aus Sicht des europäischen Gesetzgebers eine Ermächtigungsgrundlage gibt, dies in einzelnen Mitgliedstaaten selbst und im Zweifelsfall unterschiedlich zu regeln. Im Übrigen erscheint dies wiederum als eine Regelung, die sich an Vertrauensdiensteanbieter in der Ausprä-

gung Zertifizierungsdiensteanbieter richtet, weswegen – falls die Regelung beibehalten wird – ein Hinweis erfolgen sollte, dass Vertrauensdienste anderer Ausprägung hiervon nicht betroffen sein sollen. Dann allerdings sollte sich die Vorschrift auch an Zertifizierungsdiensteanbieter richten, die qualifizierte elektronische Siegel herausgeben.

Sollte an dem § 13 VDG-E festgehalten werden, bedarf es – um auf den Kommentar zu antworten – auch einer Regelung, dass Website-Zertifikate zurückgerufen werden können sollten. Dies ist in der bisherigen Praxis sehr schwierig, da die Vertrauensprüfung über einfache Zertifikatsketten ohne weitere Onlineprüfung durchgeführt wird.

Wurde also ein Zertifikat bei einem Dienstleister im Auftrag eines Root-Zertifikatsbesitzers erstellt, ist das Root-Zertifikat vom Website-Zertifikat referenziert. Der Browser prüft nur die kryptologisch-rechnerische Korrektheit der Zertifikatskette. Wir hoffen, dass sich die europäische Regulierung der Website-Zertifikate durchsetzt. Von daher sollten Vertrauensdiensteanbieter in der Ausprägung Zertifizierungsdiensteanbieter für Website-Zertifikate wie andere Zertifizierungsdiensteanbieter auch behandelt werden.

Abschließend ist darauf hinzuweisen, dass es neben dem endgültigen Widerruf von Zertifikaten (Revocation) bei Website-Zertifikaten auch die vorübergehende Sperrung (Suspension) gibt, was ebenfalls besonders zu regeln wäre, wenn diese Verantwortung nicht den Diensteanbietern überlassen werden soll.

Zu § 15 VDG-E

Mit dem Signaturgesetz von 2001 und der Einführung der akkreditierten Zertifizierungsdiensteanbieter wurde eine Unterscheidung zwischen qualifizierten Diensteanbietern in der Form vorgenommen, dass die vorab geprüften akkreditierten Anbieter nach § 4 Abs. 2 Signaturgesetzverordnung eine Zertifikatsvorhaltepflicht von mindestens 30 weiteren Jahren nach Gültigkeitsablauf besaßen. Dagegen hatte ein Zertifizierungsdiensteanbieter ohne Anbieterakkreditierung nach § 4 Abs. 1 Signaturgesetzverordnung nur eine Pflicht, dieses fünf Jahre so zu handhaben.

Diese Unterscheidung zwischen zwei Arten von qualifizierten Zertifizierungsdiensteanbietern war ein nationaler Sonderweg, der zwar aus der Historie der Gesetzgebung vor und nach der Signaturrichtlinie 1999/93/EG zu erklären ist, der sich aber nicht in der eIDAS-VO findet. Mit Einführung der Dienste der auf Dauer prüfbaren Vertrauensdienste in § 15 VDG-E wird diese Besonderheit des akkreditierten Zertifizierungsdiensteanbieters unter Wegfall der Akkreditierung weiter fortgeführt. Die dauerhafte Überprüfbarkeit signierter oder besiegelter Objekte kann auch ohne die Vorschrift sichergestellt werden. Es stellt sich also zum einen wieder die Frage nach der europarechtlichen Zulässigkeit und zum anderen, ob eine Beschränkung auf Zertifizierungsdiensteanbieter sinnvoll ist, da es sich um eine originär signaturrechtliche Anforderung handelt.

Zu § 18 VDG-E

Dass akkreditierte De-Mail-Dienstanbieter keine zweite Prüfung durchlaufen müssen, um qualifizierter Vertrauensdiensteanbieter zu werden, halten wir für naheliegend und richtig. Dies darf aber nicht dazu führen, dass Anforderungen an die De-Mail-Diensteanbieter-Akkreditierung zum Maßstab für andere qualifizierte elektronische Einschreib-Zustelldiensteanbieter gemacht werden. Es muss klar sein, dass es neben den akkreditierten De-Mail-Diensteanbietern auch weitere qualifizierte elektronische Einschreib-Zustelldiensteanbieter geben kann, an die auch andere

Anforderungen gestellt werden. Im Zweifelsfall sind das geringere Anforderungen, nämlich die aus der eIDAS-VO selbst. Um dies sicherzustellen halten wir eine Klarstellung wie die Folgende für sinnvoll:
„Für Dienste für die Zustellung elektronischer Einschreiben, die qualifizierte Dienste erbringen, aber keine Akkreditierung nach Abschnitt 4 des De-Mail-Gesetzes besitzen, sind die Anforderungen aus dem De-Mail-Gesetz unbeachtlich. Die Qualifizierung dieser Dienste ist allein an den Vorgaben der Verordnung (EU) Nr. 910/2014 zu beurteilen."

Zu Art. 3 und 4 eIDAS-DG-E

Mit Artikel 3 und 4 werden das Personalausweisgesetz bzw. die Personalausweisverordnung geändert. Wir gehen davon aus, dass im Gesetzgebungsverfahren darauf geachtet wird, dass die Änderungen auch auf den zeitgleichen Entwurf des PAuswG und der Verordnung aus dem Bundesinnenministerium angewandt werden können.

Abschließend möchten wir noch zum Erfüllungsaufwand für die Kommunen darauf hinweisen, dass dieser Aufwand für Kommunen auch für uns schwer zu beziffern ist. Es müssen aber im Bereich der Entgegennahme von signierten oder besiegelten Dokumenten gemäß EGovG NRW bzw. § 3a VwVfG neben den signierten Dokumenten (wie bisher) zukünftig auch besiegelte Dokumente geprüft werden. Dies erfordert zumindest die Neubeschaffung von Prüfsoftware, die Schulung und Ähnliches. Wenn Kommunen für eigene Zwecke elektronische Siegel einführen wollen, ist dies ein erheblich höherer Aufwand, da nicht nur die Prüfung relevant ist, sondern auch die Erstellung in die relevanten Prozesse eingebunden werden muss. Dies soll nur kleiner Hinweis sein, wobei uns auch bewusst ist, dass die elektronischen Siegel nicht mit dem Vertrauensdienstegesetz eingeführt werden, sondern schon mit der eIDAS-VO eingeführt wurden.

Für evtl. Fragen stehen wir gern zur Verfügung. Darüber hinaus bieten wir Ihnen den Austausch mit entsprechend fachlich versierten Experten aus den Vitako-Mitgliedsunternehmen an.

Mit freundlichen Grüßen
elektronisches Dokument, daher ohne Unterschrift

Dr. Marianne Wulff
Geschäftsführerin