Stellungnahme zum Referentenentwurf des Bundesministeriums für Wirtschaft und Energie

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

Die Kommentierung erfolgt im Namen der akkreditierten Zertifizierungsdiensteanbieter resp. qualifizierten Vertrauensdiensteanbieter DGN Deutsches Gesundheitsnetz Service GmbH und medisign GmbH.

Düsseldorf, 31.10.2016

Allgemeines

Grundsätzlich begrüßen wir den vorliegenden Referentenentwurf mit dem Ansatz, die erprobten Regelungen des Signaturgesetzes und der Signaturverordnung soweit sinnvoll und möglich als nationale Vorgaben bzw. Auslegung der eIDAS-Verordnung in ein Vertrauensdienstegesetz einfließen zu lassen.
Um dem Umfang und der Relevanz dieses Gesetzesvorhabens gerecht zu werden, wäre eine längere Kommentierungsfrist für die beteiligten Fachkreise und Verbände angemessen. Die eingeräumten 2 Wochen sind kaum ausreichend, alle relevanten Punkte beachten und angemessen bewerten und kommentieren zu können.
Aus diesem Grund konzentrieren wir uns bei unserer Stellungnahme vornehmlich auf die Kommentierung des VDG für die elektronischen Vertrauensdienste elektronische Signaturen, Siegel und Zeitstempel aus Sicht der Vertrauensdiensteanbieter. Dies scheint auch die Basis des Referentenentwurf selbst zu sein, der in der Hauptsache als Überführung des Signaturgesetzes wirkt und vergleichsweise wenig Augenmerk auf die in Bezug zum SigG „neuen“ Vertrauensdienste legt.
Einige Punkte sind aus unserer Sicht für die von uns betrachteten Vertrauensdienste in der aktuellen Ausprägung nicht sinnvoll oder ggfs. missverständlich formuliert, so dass wir diese mit dem vorliegenden Dokument entsprechend kommentieren und mögliche Anpassungen oder Alternativformulierungen vorschlagen möchten.

Wir würden uns sehr freuen, wenn Sie unsere Kommentare aus der Sicht akkreditierter Zertifizierungsdiensteanbieter als hilfreich erachten und diese, soweit möglich, auch berücksichtigen können.

Kommentierung der einzelnen Paragraphen

§1 Anwendungsbereich

Absatz 2

Der Sinn und die Folgen des Vorschlags des BMI sind trotz der enthaltenen Erläuterung unklar, so dass wir empfehlen, hier entweder komplett auf Absatz 2 zu verzichten oder die Formulierung klarer zu fassen.

§2 Aufsichtsstelle; zuständige Stelle für die Informationssicherheit

Absatz 1

Der letzte Satz: " Die Aufgaben des Bundesamtes für Sicherheit in der Informationstechnik nach dem BSI- Gesetz und weiterer Fachgesetze bleiben hiervon unberührt." enthält keine neue Regelung und sollte daher hier zu Gunsten der Lesbarkeit und Kürze entfallen.

§4 Untersagung des Betriebs

Gemäß Artikel 17 Absatz 3 Unterabsatz g der eIDAS ist die zu vorgesehene Sanktion der Entzug des Qualifikationsstatus. Eine darüber hinausgehende Sanktion in Form einer Untersagung des Betriebs erscheint unbillig und unnötig, da der Entzug des Qualifikationsstatus ausreichende Sicherheit vor Missbrauch bietet.

§6 Haftung

In Artikel 24 Absatz 2 Punkt (b) der eIDAS wird der Begriff "Unterauftragnehmer" anstelle der im SigG-Umfeld genutzten Begrifflichkeit "Dritte" verwendet. Daher sollten an dieser Stelle zur Klarstellung beide Begriffe verwendet werden:
„Ein Vertrauensdiensteanbieter haftet für Unterauftragnehmer und Dritte, die er mit Aufgaben ...".

§7 Datenschutz

Absatz 1 Satz 2 fordert eine Einwilligung betroffener Personen bei Datenverarbeitung "bei Dritten". Der Zweck dieser Forderung ist insbesondere aufgrund der Formulierung durch die Verwendung des in eIDAS nicht verwendeten Begriffs des "Dritten" nicht ersichtlich.
§4 Absatz 5 SigG hat die Einbeziehung sog. "beauftragter Dritter" explizit vorgesehen, so dass diese beauftragte Dritte als Auftragsdatenverarbeiter gemäß §11 BDSG zu werten waren und somit die Notwendigkeit einer expliziten Einwilligung gerade nicht gegeben war. Artikel 24 Absatz 2 Punkt (b) der eIDAS enthält ebenfalls einen Verweis auf "Dritte", hier jedoch unter der Bezeichnung "Unterauftragnehmer". Auch diese sollten daher unter die Privilegierung des §11 BDSG fallen. Aus datenschutzrechtlicher Sicht wäre jedoch hilfreich, die Beauftragung Dritter ähnlich explizit wie in §4 Absatz 5 SigG in das VDG aufzunehmen, um u.a. die höheren Anforderungen an einen Auftragsverarbeiter (vgl. Art. 4 Nr. 8 DSGVO) gemäß Art. 28 DSGVO zu erfüllen.
Ist die hier verwendete Bezeichnung "Dritte" weiterhin in diesem Verständnis zu sehen (als Auftrags(daten)verarbeiter), gibt es keinen Anlass, erweiterte Anforderungen an die Informationspflicht zu stellen. Aus diesem Grund empfehlen wir, diesen Satz (Absatz 1 Satz 2) ersatzlos zu streichen. Die jeweils geltenden Datenschutzregelungen (BDSG und anschließend DSGVO und ggfs. nationale Zusatzregelungen) können somit ihre Wirkung entfalten und das VDG bleibt unabhängig von deren Änderungen.

Absatz 2 Unterabsatz 1 geht insbesondere für ein "Vertrauensdienstegesetz", dass diesem Namen gerecht werden soll, in seiner Offenbarungspflicht an nicht deutlich abgegrenzte "zuständige Stellen" und den zu allgemein und sehr weit gefassten Berechtigungsgründen deutlich zu weit und ist dadurch geeignet, das Vertrauen in die angebotenen Vertrauensdienste stark einzuschränken.
Die Empfehlung ist daher, wenn möglich komplett auf Unterabsatz 1 zu verzichten und damit die Übermittlung ausschließlich unter richterlicher Kontrolle zu stellen. Sollte dies nicht umsetzbar sein, kann hier auf eine im Sinne des Datenschutzes sinnvollere und zur Strafverfolgung entsprechender Delikte ausreichende und an §14 TMG angelehnte bewährte Formulierung zurückgegriffen werden. Die empfohlene Formulierung für Absatz 2 lautet in diesem Fall:
"*Auf Anordnung der zuständigen Stellen darf der Vertrauensdiensteanbieter diesen im Einzelfall personenbezogene Daten einer Person, die Vertrauensdienste nutzt, übermitteln,*

1. *soweit dies für Zwecke der Strafverfolgung, zur Gefahrenabwehr durch die Polizeibehörden der Länder, zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes oder des Bundeskriminalamtes im Rahmen seiner Aufgabe zur Abwehr von Gefahren des internationalen Terrorismus oder*
2. *soweit Gerichte die Übermittlung im Rahmen anhängiger Verfahren nach Maßgabe der hierfür geltenden Bestimmungen anordnen.*"

§10 Identitätsprüfung

Insbesondere aus der Begründung zu diesem Artikel lässt sich erkennen, dass an dieser Stelle leider die Identitätsprüfung juristischer Personen für die Ausstellung qualifizierter elektronischer Siegel nicht berücksichtigt wurde. Gerade für diesen Bereich existieren derzeit jedoch noch keine praktischen Erfahrungen, so dass hier durch eine gesetzliche Klarstellung die Einführung dieses neuen Vertrauensdienstes und entsprechender Dienste gefördert werden könnte und sollte. Wir empfehlen daher, dass die Bundesnetzagentur als zuständige Aufsichtsstelle einheitliche Vorgaben für die Identifizierung juristischer Personen erstellt und Absatz 1 dahingehend ergänzt wird.

Grundsätzlich wäre es sinnvoll, die Anforderungen an die Identifizierung natürlicher und juristischer Personen über die verschiedenen Gesetze, die entsprechende Vorgaben enthalten (SigG/VDG, De-Mail-G, GWG, TMG…), zumindest im Sinne einer nationalen Interoperabilität zu vereinheitlichen. Auf dieser Basis könnten entsprechende Dienstleister vergleichbar zu bisherigen, im SigG-Umfeld etablierten „Modul-Bestätigungen“ bzw. „Bestätigung der Eignung und praktischen Umsetzung eines Teilsicherheitskonzeptes“, mit eigenständigen Konformitätsbewertungen zugelassen werden, die anschließend in den verschiedenen Einsatzfeldern (Vertrauensdiensteanbieter, Banken, Mobiltelefonie …) anerkannt würden.

Ungeachtet dieser allgemeinen Anmerkungen gelten folgende Kommentare zu §10:

Absatz 1 legt in Verbindung mit dessen Begründung die Annahme nahe, dass hier eben nicht nur Methoden („Video-Ident-Verfahren“), sondern auch konkrete Ausprägungen von Verfahren im Sinne von Produkten („Post-Ident-Verfahren“) festgelegt werden können. In

diesem Fall ergäbe sich ein Widerspruch zu der ebenfalls in der Begründung aufgeführten Forderung, dass die Konformitätsbewertungsstellen die "gleichwertige Sicherheit" bestätigen sollen. Dies wird ja gerade durch die hier beschriebene Veröffentlichung im Amtsblatt vorweg genommen und würde bei abweichender Bewertung durch eine Konformitätsbewertungsstelle zur Rechtsunsicherheit beitragen.

Wir gehen daher davon aus, dass die Bundesnetzagentur ausschließlich entsprechende Methoden ohne deren konkrete Umsetzung als geeignet festlegt und veröffentlicht, die dementsprechend nach Bestätigung einer geeigneten und korrekten Umsetzung der von der Bundesnetzagentur festgelegten Mindestanforderungen durch eine Konformitätsbewertungsstelle als solche mit "gleichwertiger Sicherheit" gelten.

Absatz 2 sollte dahingehend an die derzeitige Auslegung dieser auch schon in § 5 Absatz 1 Satz 2 SigG enthaltenen Regelung angepasst werden, dass nicht die verantwortliche Stelle der ursprünglichen Datenerhebung auf den VDA selbst eingeschränkt wird, sondern ausschließlich deren korrekte und gesetzeskonforme Erhebung von einer geeigneten Stelle (z.B. Banken, die gemäß eigener gesetzlichen Vorgaben eine gleichwertige Sicherheit der Identitätsprüfung resp. der daraus resultierenden Datenerhebung bieten) und der notwendigen Zustimmung zur Übermittlung an und Weiternutzung durch den VDA abhängig gemacht wird. Ein mögliche Alternativformulierung für Absatz 2 lautet

"... mit Einwilligung des Antragstellers personenbezogene Daten nutzen, die zu einem früheren Zeitpunkt durch eine berechtigte Stelle erhoben wurden, sofern diese Daten die zuverlässige Identitätsfeststellung des Nutzers gewährleisten.".

§11 Attribute in qualifizierten Zertifikaten für elektronische Signaturen

Kommentar JZ6: Aus unserer Sicht sind Attribute durchaus auch bei e-Siegeln sinnvoll einzusetzen, wenn auch nicht unbedingt in Verbindung mit Vertretungsregeln, da der Einsatz von Siegeln gerade dazu geeignet ist, qualifizierte Zertifikate mit Vertretungsregelungen zu ersetzen. Attribute könnten jedoch insbesondere dann sinnvoll sein, wenn es hierzu in bestimmten Bereichen fest definierte Vorgaben geben würde. Beispielsweise könnte man die Funktion einer Firma in einem Attribut festlegen, u.a. könnten Konformitätsbewertungsstellen genau diese Bezeichnung als Attribut "Konformitätsbewertungsstelle" aufnehmen und sich damit als solche direkt im Siegel des elektronischen Konformitätsbewertungsberichts ausweisen, gleiches gilt für Identitätsdiensteanbieter, Vertrauensdiensteanbieter oder im EANV-Umfeld Transportunternehmen, Entsorger usw..

Die Absätze 1 und 2 sind sinnvolle Ergänzungen zu den Vorgaben der eIDAS, die auch zur Weiternutzung bereits ausgegebener qualifizierter Zertifikate hilfreich sind.

Absatz 1 enthält jedoch in **Satz 3** die Formulierung *"... dürfen nur dann in das qualifizierte Zertifikat aufgenommen werden, wenn der Antragsteller eine Bestätigung der Angaben durch die jeweils zuständige Stelle vorlegt.*", die eine unnötige Beschränkung dadurch erzeugt, dass der Weg dieser Bestätigung vorgegeben wird. Es kommt unseres Erachtens nicht darauf an, wer diese Bestätigung vorliegt, sondern ausschließlich darauf, dass diese bei der Ausstellung des Zertifikats, spätestens jedoch zum Zeitpunkt der Aktivierung des

betreffenden Zertifikats beim ausgebenden VDA vorliegen muss. Eine entsprechende alternative Formulierung lautet:

"... dürfen nur dann in das qualifizierte Zertifikat aufgenommen werden, wenn eine Bestätigung der Angaben durch die jeweils zuständige Stelle nachgewiesen werden kann."

Eine durch die Möglichkeit zur Verkürzung der Produktionszeiten kundenfreundlichere Alternative wäre:

"*Amts-, berufsbezogene oder sonstige Angaben zur Person dürfen nur dann in das qualifizierte Zertifikat aufgenommen werden, wenn eine Bestätigung der Angaben durch die jeweils zuständige Stelle vor der Aktivierung des Zertifikats nachgewiesen werden kann. Kann der Nachweis nicht erbracht werden, dürfen entsprechende Zertifikate in der Zertifikatsdatenbank nicht als gültig gekennzeichnet und vorgehalten werden. Wird eine Bestätigung nachträglich entzogen, muss das betreffende Zertifikat durch die zuständige Stelle gesperrt werden.*"

Mit **Absatz 3** werden Attributzertifikate eingeführt. Dies führt zu einer ausschließlich auf nationaler Ebene verbindlichen technischen Vorgabe für qualifizierte Zertifikate, die von den Vorgaben an qualifizierte Zertifikate für elektronische Signaturen Anhang I der eIDAS abweichen und somit Artikel 28 Absatz 2 widersprechen. Dies führt zu einem Konflikt zu einem der Hauptbeweggründe der eIDAS, der Interoperabilität, und sollte daher vermieden werden.

Überdies haben praktische Erfahrungen in Deutschland gezeigt, dass

(1) ZDAs/VDAs die Verwendung von Attributzertifikaten bis auf wenige Ausnahmen nicht genutzt bzw. deren Verwendung weitestgehend eingestellt haben,
(2) SAK und andere Softwarekomponenten damit nicht umgehen können und
(3) den Anwendern die Verwendung und der Nutzen nicht vermittelt werden konnte.

Aus diesen Gründen ist die Einbindung der Attribute in Basiszertifikate wesentlich sinnvoller und für Zertifikatsinhaber und Nutzer einfacher handzuhaben und zu verstehen und im Rahmen der eIDAS unter Beibehaltung der Interoperabilitätsanforderungen umsetzbar.

Unsere Empfehlung lautet daher, Absatz 3 ersatzlos zu streichen.

§12 Unterrichtung über Sicherheitsmaßnahmen und Rechtswirkungen

Absatz 1 Punkt 3

Die zu berücksichtigen Rechtswirkungen sind sehr umfangreich, dabei jedoch nicht abhängig vom einzelnen VDA. Wir empfehlen daher, einen allgemeingültigen bzw. einheitlichen Textvorschlag von den zuständigen Aufsichtsstellen erarbeiten zu lassen, diesen an geeigneter Stelle zu veröffentlichen und aktuell zu halten.

Der VDA sollte darauf verweisen können oder den Text in seine eigene Unterrichtung übernehmen.

§13 Widerruf qualifizierter Zertifikate

Absatz 1 Punkt 4

Die hier verwendeten Formulierungen sind ungenau und sollten daher wie folgt präzisiert werden.

„4. Tatsachen die Annahme rechtfertigen, dass

- *a) dieses qualifizierte Zertifikat gefälscht oder nicht hinreichend fälschungssicher sind,*
- *b) die verwendeten qualifizierten elektronischen Signaturerstellungseinheiten oder qualifizierten elektronischen Siegelerstellungseinheiten Sicherheitsmängel aufweisen, die die Integrität des Zertifikats oder die Vertraulichkeit oder Integrität der elektronischen Signaturerstellungsdaten gefährden."*

§14 Aufzeichnungen

Absatz 2 Punkt 2

Die Aufsichtsstelle unterliegt in Bezug auf die Beauskunftung im Sinne einer Offenbarung personenbezogener Daten den gleichen datenschutzrechtlichen Anforderungen wie der ursprüngliche VDA. Dies sollte an dieser Stelle verdeutlicht werden, mindestens durch einen entsprechenden Zusatz in Satz 2:

„Die Aufsichtsstelle erteilt bei Vorliegen eines berechtigten Interesses unter Berücksichtigung von §7 Absatz 2 und den allgemeinen datenschutzrechtlichen Vorgaben Auskunft zu den Aufzeichnungen, soweit dies technisch ohne unverhältnismäßig großen Aufwand möglich ist."

Die in eIDAS Artikel 24 Absatz 2 Unterabsatz h geforderte Aufbewahrung der Aufzeichnungen über einen „… angemessenen Zeitraum, auch über den Zeitpunkt der Einstellung der Tätigkeit des qualifizierten Vertrauensdiensteanbieters hinaus …" sollte an dieser Stelle allgemeinverbindlich, also auch für die Aufsichtsstelle im Falle der Übernahme der Daten gemäß §14 Absatz 2 VDG, ggfs. durch Verweis auf die zugehörige Rechtsverordnung nach §20, da dies in der derzeitigen Version nur für die VDAs selbst in §15 Absatz 2 Nummer 4 für die im VDG neu eingeführte Formulierung „auf Dauer prüfbar" bzw. „dauerhaft", die wahrscheinlich einen längeren Zeitraum als der in eIDAS vorgegebene „angemessene Zeitraum" umfassen soll, definiert wird.

Eine dedizierte Festlegung dieser Zeiträume ist auch aus Sicht der datenschutzrechtlichen Vorgaben gemäß BDSG/DSGVO hilfreich, um die jeweiligen Lösch- und/oder Sperrfristen für alle VDAs und ggfs. die Aufsichtsbehörden einheitlich vorzugeben.

§15 Beendigungsplan; auf Dauer prüfbare Vertrauensdienste

Absatz 1 Punkt 2 müsste korrekt *„2. alle ausgestellten und noch gültigen Zertifikate zu widerrufen."* lauten.

Zur Erstellung eines geeigneten Beendigungsplans gemäß Absatz 2 Satz 2 fehlen die entsprechenden technischen und organisatorischen Beschreibungen der Aufsichtsstelle.

Frage: Gibt es dazu schon Vorstellungen, wie dies umgesetzt werden soll bzw. wann, in welcher Form und an welcher Stelle entsprechende Informationen verfügbar gemacht werden?

Die Bestätigung der Umsetzbarkeit eines geeigneten Beendigungsplans wird gemäß Absatz 2 Punkt 3 gefordert. Handelt es sich dabei um eine explizite zusätzliche Bestätigung oder soll dies Teil der gesamten eIDAS-Konformitätsbewertung sein? Dies ist insbesondere im Hinblick auf die Übergangsvorschriften gemäß § 21 zu betrachten.

Absatz 3 Punkt 4 enthält den oben geforderten Verweis auf einen definierten Zeitraum, allerdings ausschließlich für die VDAs und nur für die „auf Dauer prüfbaren“ Vertrauensdienste. Es fehlen somit die im Kommentar zu §14 Absatz 2 Punkt 2 ebenfalls geforderten Angaben für den „angemessenen Zeitraum“ laut eIDAS und der Hinweis, dass diese Zeiten auch für die Aufsichtsstelle gelten.

§16 Benannte Stellen nach Artikel 30 Absatz 1 der Verordnung (EU) Nr. 910/2014

Absatz 2 legt das BSI ohne weitere Angaben als entsprechende öffentliche Stelle fest. Es wäre konsequent, die Vorgaben an private Stellen gemäß Absatz 1 auch für die öffentliche Stelle als bindend zu definieren.

§ 17 Verweis auf Regelungen zu qualifizierten elektronischen Signaturen

Die Benennung dieses Paragraphen ist nicht sinnvoll, vielmehr sollte hier der eigentliche Regelungsinhalt benannt werden:
„§17 Zertifizierung qualifizierter elektronischer Siegelerstellungseinheiten"
oder (zwar formal korrekt aber leider nicht allgemeinverständlich)
„§17 Benannte Stellen nach Artikel 39 Absatz 2 der Verordnung (EU) Nr. 910/2014“

§21 Übergangsvorschriften

Absatz 2 Satz 2 definiert Übergangsvorschriften für Bedingungen, die allein aus der gewählten Formulierung nicht direkt ersichtlich sind.
Aus jetziger Sicht „gilt“ eine bereits vorliegende Akkreditierung bis zur Einführung des VDG, da erst damit SigG und SigV formal ungültig werden. Insofern wäre es konsequenter, die Regelungen gemäß Satz 1 nicht mit dem 01.07.2017 enden zu lassen, sondern mit der Einführung des VDG resp. Ablösung des SigG.
Wenn jedoch der Akkreditierungsstatus mit Ende der Übergangszeit nach eIDAS zum 01.07.2017 verloren geht, würde auch der Qualifikationsstatus entfallen, wenn noch keine eIDAS-Konformitätsbestätigung vorgelegt wurde. Der bestätigte Beendigungsplan muss daher Teil eines kompletten eIDAS-Konformitätsbewertungsberichts sein, um die notwendigen Vorgaben gemäß eIDAS Artikel 51 Absatz 3 einzuhalten und kann nicht unabhängig davon existieren, wie es nach der aktuellen Formulierung dieses Absatzes zu vermuten wäre.
Alternativer Formulierungsvorschlag:
„(2) Nach § 15 des Signaturgesetzes akkreditierte Zertifizierungsdiensteanbieter gelten bis zum 1. Juli 2017 und darüber hinaus bis zur Ablösung des Signaturgesetzes als Anbieter von auf Dauer prüfbaren Vertrauensdiensten gemäß § 15 Absatz 3 dieses Gesetzes, sofern sie gemäß Artikel 51 Absatz 3 der Verordnung (EU) Nr. 910/2014 bis zum 1. Juli 2017 einen Konformitätsbewertungsbericht mit bestätigten Beendigungsplan mit dem Inhalt des § 15 Absatz 2 vorgelegt haben. Dieser Status bleibt bis zum Abschluss der Bewertung des Berichts durch die Aufsichtsstelle erhalten. Die Sätze 1 und 2 gelten nicht, wenn und sobald der akkreditierte Zertifizierungsdiensteanbieter den Qualifikationsstatus beantragt hat und dabei keinen Beendigungsplan mit dem Inhalt des § 15 Absatz 2 vorgelegt hat.“