



Stellungnahme der Bundesärztekammer

zum Referentenentwurf 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, Vertrauensdienstegesetz-Entwurf (VDG-E), vom 18.10.2016

Berlin, 01.11.2016

Korrespondenzadresse:

Bundesärztekammer
Herbert-Lewin-Platz 1
10623 Berlin

1. Grundlegende Bewertung des Gesetzesentwurfs

Die seit dem 1. Juli 2016 geltende eIDAS-VO statuiert EU-weit einheitliche Anforderungen an elektronische Vertrauensdienste wie elektronische Signaturen, Siegel, Zeitstempel, Zustelldienste und Webseitenauthentifizierungen.

Das Vertrauensdienstegesetz konkretisiert als nationales Durchführungsgesetz die eIDAS-Verordnung der EU (Nr. 910/2014) und ersetzt die EU-Signaturrechtlinie (1999/93/EG).

Die Bundesärztekammer begrüßt den vorliegenden Referentenentwurf des Vertrauensdienstegesetzes, insbesondere da in weiten Teilen auch das hohe Sicherheitsniveau des bisherigen Signaturgesetzes wieder Berücksichtigung findet.

Aktuell existiert noch weiterer Regelungsbedarf, der im Gesetzesentwurf nicht berücksichtigt wurde.

2. Vorbemerkung

Die Bundesärztekammer wird im Kap. 3 Stellung beziehen zu den Paragraphen 10, 11, 14 und 15. Dies sind die Paragraphen, die für die Ärztekammern als Herausgeber der Heilberufsausweise für Ärzte im Gesundheitswesen sowie für die Zulassung der Vertrauensdiensteanbieter durch die Ärztekammern von besonderem Interesse sind.

In Kap. 4 werden wir weiteren Regelungsbedarf adressieren, der aber ggf. auch in untergeordneten Verordnungen, gemäß § 20 VDG-E, geregelt werden kann.

3. Stellungnahme im Einzelnen

Zu dem Referentenentwurf 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 (eIDAS-VO) nimmt die Bundesärztekammer wie folgt Stellung:

Anforderungen an qualifizierte Vertrauensdiensteanbieter

§ 10 Identitätsprüfung

A) Beabsichtigte Regelung

Gemäß Artikel 24 Abs. 1 Satz 2 Buchstabe c der eIDAS-VO (Anforderungen an qualifizierte Vertrauensdiensteanbieter) überprüft der Anbieter die Identität des Antragstellers „*durch ein Zertifikat einer qualifizierten elektronischen Signatur [...]*“.

In §10 des VDG-E wird festgelegt, dass die Bundesnetzagentur die vorgesehene Festlegung der Identifizierungsmethoden und der dafür geltenden Mindestanforderungen definiert.

B) Stellungnahme der Bundesärztekammer

Diese Regelung wird begrüßt, da sie aus Sicht der Bundesärztekammer ermöglichen soll, dass auf Basis eines einmal ausgestellten qualifizierten Zertifikates auch weitere qualifizierte Zertifikate online bei anderen Anbietern ausgestellt werden könnten.

Die Bundesärztekammer begrüßt die durch § 10 des Entwurfs eines Vertrauensdienstegesetzes (VDG-E) vorgesehene und an Art. 24 eIDAS-VO anknüpfende Festlegung der Identifizierungsmethoden und der dafür geltenden Mindestanforderungen durch die Bundesnetzagentur.

In diesem Zusammenhang bleibt jedoch unklar, welche Anforderungen und Möglichkeiten hinsichtlich der Dokumentation und Archivierung der Antragsunterlagen (Aufzeichnungen) auf die möglichen anderen Anbieter zukommen und wie sichergestellt ist, dass die ursprünglichen Antragsunterlagen – auf deren Basis das Zertifikat ausgestellt wurde und dessen Signatur für die weiteren Zertifikate anderer Anbieter verwendet wird -, noch für etwaige Streitfälle zur Verfügung stehen.

Anforderungen an qualifizierte Vertrauensdiensteanbieter

§11 Attribute in qualifizierten Zertifikaten für elektronische Signaturen

A) Beabsichtigte Regelung

§11 Abs. 1 Satz 3 VDG-E definiert, dass Attribute in qualifizierte Zertifikate für elektronische Signaturen aufgenommen werden können, „*wenn der Antragsteller eine Bestätigung der Angaben durch die jeweils zuständige Stelle vorlegt.*“

B) Stellungnahme der Bundesärztekammer

Die Bundesärztekammer begrüßt die Möglichkeit zur Aufnahme von Berufsgruppenattributen in qualifizierten Zertifikaten.

Aus Sicht der Bundesärztekammer deckt diese Regelung jedoch nicht die Möglichkeit ab, dass die zuständige Stelle, bspw. wie im Fall der Heilberufsausweise im Gesundheitswesen, in einem Vertragsverhältnis mit dem (zugelassenen) Anbieter steht und die zuständige Stelle im Rahmen des Antragsprozesses direkt dem Anbieter die Bestätigung der Angaben übermittelt.

C) Änderungsvorschlag der Bundesärztekammer

Vorgeschlagene Neufassung §11 Abs. 1 Satz 3 VDG-E:

Amts-, berufsbezogene oder sonstige Angaben zur Person dürfen nur dann in das qualifizierte Zertifikat aufgenommen werden, wenn der Antragsteller eine Bestätigung der Angaben durch die jeweils zuständige Stelle vorlegt oder diese von der zuständigen Stelle vorgelegt wird.

Anforderungen an qualifizierte Vertrauensdiensteanbieter

§11 Attribute in qualifizierten Zertifikaten für elektronische Signaturen

A) Beabsichtigte Regelung

Mit § 11 Abs. 3 VDG-E wird ausdrücklich geregelt, dass Attribute auch in ein gesondertes qualifiziertes Zertifikat (qualifiziertes Attribut-Zertifikat) aufgenommen werden können.

B) Stellungnahme der Bundesärztekammer

Im Sinne einer europäischen Interoperabilität wird durch die Bundesärztekammer angeregt, zuvorderst die Standardisierung und Festlegung einer einheitlichen ASN.1-Struktur für die Aufnahme der Berufsgruppeninformation (*professionItem*) in einem Zertifikat festzulegen. Bislang fehlen hierzu europaweit standardisierte und interoperable Vorgaben.

Anforderungen an qualifizierte Vertrauensdiensteanbieter

§14 Aufzeichnungen

A) Beabsichtigte Regelung

Gemäß Art. 24 Abs. 2 Buchstabe h eIDAS-VO (Anforderungen an qualifizierte Vertrauensdiensteanbieter) sind die qualifizierten Vertrauensdiensteanbieter verpflichtet, alle einschlägigen Informationen über die von dem qualifizierten Vertrauensdiensteanbieter aus-gegebenen und empfangenen Daten aufzubewahren und haben sie so aufzubewahren, dass sie über einen angemessenen Zeitraum, auch über den Zeitpunkt der Einstellung der Tätigkeit des qualifizierten Vertrauensdiensteanbieters hinaus, verfügbar sind, um insbesondere bei Gerichtsverfahren entsprechende Beweise liefern zu können und die Kontinuität des Dienstes sicherzustellen. Die Aufzeichnung kann in elektronischer Form erfolgen.

§ 14 Abs. 1 VDG-E konkretisiert Art. 24 Abs. 2 eIDAS-VO dahingehend, dass die entsprechenden Informationen so aufzuzeichnen sind, dass sie nachträglich nicht unbemerkt verändert werden können und so aufzubewahren sind, dass die Daten und ihre Unverfälschtheit jederzeit nachprüfbar bleiben. Weiter wird in § 14 Abs. 2 VDG-E geregelt, dass – wenn kein anderer qualifizierter Vertrauensdiensteanbieter die Aufzeichnungen entsprechend dem Beendigungsplan nach § 15 Abs. 1 VDG-E übernimmt – die Aufsichtsstelle diese Aufgabe zu übernehmen hat.

B) Stellungnahme der Bundesärztekammer

Die Bundesärztekammer begrüßt diese Regelung ausdrücklich, da auf diese Weise ein ähnliches Sicherheitsniveau wie dem akkreditierten Niveau des Signaturgesetzes möglich ist.

Anforderungen an qualifizierte Vertrauensdiensteanbieter

§15 Beendigungsplan; auf Dauer prüfbare Vertrauensdienste

A) Beabsichtigte Regelung

Gemäß Art. 24 Abs. 2 Buchstabe i eIDAS-VO (Anforderungen an qualifizierte Vertrauensdiensteanbieter) müssen qualifizierte Vertrauensdiensteanbieter über einen fortlaufend aktualisierten Beendigungsplan verfügen, der für den Fall der Einstellung des Betriebs definiert, ob Aufzeichnungen und Zertifikate durch andere Anbieter übernommen werden oder die ausgestellten Zertifikate widerrufen werden.

§ 15 Abs. 2 VDG-E konkretisiert dahingehend, dass der Anbieter im Beendigungsplan vor-sehen kann, dass – sofern kein anderer qualifizierter Anbieter Zertifikate und Aufzeichnungen übernimmt – die Aufsichtsstelle diese Aufgabe übernimmt und die qualifizierten Zertifikate für jedermann jederzeit und dauerhaft in einem Zertifikatsverzeichnis öffentlich verfügbar macht.

§ 15 Abs. 3 VDG-E bestimmt ein Siegel der Aufsichtsstelle, das die Garantie der Aufsichtsstelle zur Übernahme der Zertifikate zum Ausdruck bringt.

§15 Abs. 4 VDG-E regelt, dass der Anbieter von auf Dauer prüfbaren Vertrauensdiensten die Zertifikate nach § 15 Abs. Satz 1 VDG-E zusammen mit den zugehörigen Widerrufsinformationen für die in einer Rechtsverordnung nach § 20 VDG-E festgelegte Dauer für jedermann in einem Zertifikatsverzeichnis öffentlich verfügbar zu machen.

B) Stellungnahme der Bundesärztekammer

Die Bundesärztekammer begrüßt die Konkretisierung in § 15 Abs. 2 VDG-E ausdrücklich, insbesondere in Kombination mit §14 Abs. 2 VDG-E, wonach die Bundesnetzagentur auch die Aufzeichnungen der qualifizierten Anbieter bei Betriebseinstellung übernimmt.

Die Bundesärztekammer begrüßt die Regelung in § 15 Abs. 3 VDG-E und schlägt vor, dass die Bundesnetzagentur – als unabhängiger und zentraler Dritter – die ausgestellten Siegel veröffentlicht.

Die Bundesärztekammer weist darauf hin, dass im Gesundheitswesen unter anderem 30-jährige Archivierungsanforderungen aufgestellt werden, die auf Dauer prüfbare Vertrauensdienste erfordern. Sie geht davon aus, dass gemäß der Regelung in § 15 Abs. 4 VDG-E „auf Dauer prüfbare Vertrauensdienste“ vergleichbar zum heutigen akkreditierten Niveau des Signaturgesetzes prüfbar sind.

4. Ergänzender Änderungsbedarf

- Schaffung eines europäischen Algorithmenkatalogs
Im Rahmen des Signaturgesetzes hatte das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Aufgabe mit dem Algorithmenkatalog die Vertrauenswürdigkeit der verschiedenen kryptographischen Algorithmen und Schlüssellängen einzuordnen. Unklar ist aus Sicht der Bundesärztekammer, wie diese Festlegung zukünftig unter dem Regime der eIDAS-VO – und insbesondere europaweit gleichartig – getroffen wird.
- Formerfordernis für die Bestätigung von Attributen
Die Bundesärztekammer geht davon aus, dass mit der in § 20 VDG-E angestrebten Vertrauensdiensteverordnung geregelt wird, dass die Bestätigung der Angaben im Sinne des § 11 VDG-E durch die jeweils zuständige Stelle mit einer qualifizierten elektronischen Signatur (QES) oder zusätzlich zu einer QES mit einem elektronischen Siegel oder schriftlich vorliegen muss. Aus Sicht der Bundesärztekammer stellt sich schon jetzt die Frage, ob das elektronische Siegel auch allein, d.h. ohne eine QES, dafür nutzbar wäre.