bvitg-Stellungnahme
zur Verordnung zu Vertrauensdiensten (Vertrauensdiensteverordnung – VDV)

Der Bundesverband Gesundheits-IT – bvitg e. V. begrüßt den Referentenentwurf vom Bundesministerium für Wirtschaft und Energie (Stand: 02.07. 2018) zur Verordnung zu Vertrauensdiensten (Vertrauensdiensteverordnung – VDV). Mit Blick auf die Erfahrungen mit der seit dem 1. Juli 2016 geltenden 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 1993/93/EG (eIDAS-Verordnung) sowie mit dem am 29. Juli 2017 in Kraft getretenen Vertrauensdienstegesetz ist der Bedarf nach letzten Präzisierungen erkannt worden, damit Anbieter von Vertrauensdiensten und Zertifizierungsstellen ihre Anforderungen aus der eIDAS-Verordnung und dem Vertrauensdienstegesetz zuverlässig erfüllen können.

Der bvitg als Vertreter der IT-Anbieter im Gesundheitswesen, darunter auch Anbietern von Vertrauensdiensten, und mit Blick auf die kommenden Anwendungen im Rahmen der Telematikinfrastruktur begrüßt die Schaffung von Klarheit und Rechtssicherheit für die beteiligten Akteure und bedankt sich für die Gelegenheit zur Kommentierung des Entwurfes im Rahmen der Verbändebeteiligung.

Der Verband nimmt zur Vertrauensdiensteverordnung wie folgt Stellung:

§ 1 Anforderungen an die Barrierefreiheit

Redaktionelle Anpassung und inhaltliche Präzisierung:

Barrierefreie Dienste gemäß § 7 Absatz 1 des Vertrauensdienstegesetzes sollen, soweit technisch möglich, für Menschen mit Behinderungen bedienbar und robust sein. ~~und die Hinweise und Informationen zur Barrierefreiheit nach § 7 Absatz 2 des Vertrauensdienstegesetzes sollen wahrnehmbar, bedienbar, verständlich und robust sein. Dabei sollen sie sich am Stand der Technik orientieren.~~ Hinweise und Informationen zur Barrierefreiheit nach § 7 Absatz 2 des Vertrauensdienstegesetzes sollen barrierefrei wahrnehmbar und verständlich sein. Dabei sollen sich die barrierefreien Vertrauensdienste am Stand der Technik orientieren.

Begründung:

Der Referentenentwurf berücksichtigt nicht hinreichend, dass die Anforderungen an die barrierefreien Dienste iSv § 7 Abs. 1 inkl. der dazu benötigten Hardware naturgemäß nicht identisch sein können mit denen, die für Hinweise und Informationen iSv § 7 Abs. 2 Satz 3 VDG gelten. Daher ist eine Differenzierung nach Diensten und Informationen geboten. Außerdem muss für Dienste entsprechend der Einschränkung des VDG die technische Machbarkeit als restriktives Kriterium Berücksichtigung finden.

§ 3 Dokumentation der Ausgabe qualifizierter Zertifikate für Vertrauensdienste

Konkretisierung von Abs. 1:

(1) Soweit der Vertrauensdiensteanbieter bei der Ausgabe qualifizierter Zertifikate die Identität oder Attribute an Hand öffentlicher und auf Dauer zugänglicher Register oder Dokumente überprüft, genügt es, dass er vermerkt, in welches Register oder Dokument er Einsicht genommen hat und ob die verarbeiteten Daten mit denen im Register übereinstimmen. Ein Auszug des Registers oder Dokuments muss nicht zur Dokumentation genommen werden.

Es wird um Klarstellung gebeten, dass es sich bei den Registern im Sinne von § 3 Abs. 1 Satz 1 um zwei kumulativ vorliegende Voraussetzungen handelt:

- öffentlich und

- auf Dauer zugänglich.

Weiterhin wird um eine Legaldefintion bzgl. des Merkmals „auf Dauer zugänglich“ gebeten. Gemeint dürfte nicht die Information als solche sein, da diese nach entsprechendem Zeitablauf gelöscht werden, sondern die dauerhafte Zugänglichkeit der Register als solcher gemeint sein.

Begründung:

Eine Legaldefinition auf Dauer zugänglicher öffentlicher Register ist wünschenswert, um den Verwaltungsaufwand für VDA zu reduzieren.

Ergänzung von Abs. 2:

(2) Nach § 12 des Vertrauensdienstegesetzes erforderliche Vollmachten, Einwilligungen oder Bestätigungen müssen qualifiziert elektronisch signiert, qualifiziert elektronisch gesiegelt, ~~oder~~ handschriftlich unterschrieben sein oder erfolgen in einem organisatorisch-technischen Prozess, der einer eIDAS-Konformitätsbewertung unterliegt.

Begründung:

eIDAS-konforme organisatorisch-technische Prozesse stellen eine technikneutrale Öffnung dar, die es ermöglicht, auf technische Entwicklungen zu reagieren, ohne dass ein Verlust an Sicherheit einhergeht. Letzteres wird durch die Konformitätsbewertung gegen die EU-Verordnung eIDAS sichergestellt.

Grundsätzlich begrüßen wir diesen Absatz sehr, da hierbei vorstellbar ist, dass für Ärztekammern eine Vereinfachung eintritt, wenn sie Attribute von Mitgliedern (Attribut „Arzt“) mittels qualifiziertem elektronischen Siegel bestätigen dürfen. Insbesondere in der automatisierten Verarbeitung, z.B. bei der Beantragung von HBA, kann das Siegel zur technisch-organisatorischen Vereinfachungen führen.

§ 4 Vorsorge für die dauerhafte Prüfbarkeit qualifizierter Zertifikate

Ergänzung von Abs. 1:

(1) Qualifizierte Vertrauensdiensteanbieter haben Vorsorge zu treffen, dass ihre Zertifikatsdatenbank im Falle einer Betriebseinstellung im Sinne des § 16 Absatz 1 Satz 1 des Vertrauensdienstegesetzes von einem anderen qualifizierten Vertrauensdiensteanbieter oder der Bundesnetzagentur übernommen werden kann. Der qualifizierte Vertrauensdiensteanbieter ist verpflichtet hierfür den Stand der Technik zu berücksichtigen.

Begründung:

Im Markt sind verschiedene technische Lösungen verfügbar, die eine Übergabe der Zertifikatsdatenbank ermöglichen. Darüber hinaus gibt es für die langfristige Beweiswerterhaltung spezialisierte (zum

Beispiel qualifizierte) Vertrauensdienste gemäß der eIDAS, die mit der Aufgabe der Verwahrung der Zertifikatsdatenbank betraut werden können.

Streichung von Abs. 2:

~~*(2) Die Bundesnetzagentur veröffentlicht Kriterien, die eingehalten werden sollen, um eine Übernahme durch die Bundesnetzagentur zu ermöglichen.*~~

Begründung:

Es sollten keine zusätzlichen Kriterien zur Ermöglichung der Übernahme der Zertifikatsdatenbank des Vertrauensdiensteanbieter durch die Bundesnetzagentur definierbar sein, da dies einen nicht kalkulierbaren Aufwand auf Seiten des VDA darstellt. Es entsteht zusätzlicher Erfüllungsaufwand für die Wirtschaft. Die Anforderungen können beliebig oft und detailliert angepasst werden, ohne dass der VDA hierbei ein Einspruchsrecht hat. Dies stellt eine Benachteiligung deutscher VDA gegenüber europäischen VDA dar.

Ergänzung von Abs. 2:

Die Prüfbarkeit von qualifizierten Zertifikaten und qualifizierten elektronischen Zeitstempeln, die in der Datenbank nach § 16 Abs. 4 gespeichert sind, ist nach Ablauf des Gültigkeitszeitraum, wie im Zertifikat angegeben, für die Dauer von mindestens einem Monat durch den qualifizierten Vertrauensdiensteanbieter sicherzustellen.

Begründung:

Die Datenschutzgrundverordnung bedingt die Begrenzung der Speicherdauer. Unabhängig von § 16 Abs. 4 VDG sollte der VDA in der Lage sein, den Zeitraum der Veröffentlichung von Zertifikats- und Statusinformationen zu begrenzen, um den Anforderungen der Datenschutzgrundverordnung zu entsprechen.

Zudem ist üblich, dass die Widerrufsinformationen eines Zertifikats während des Zeitraums seiner Gültigkeit durch den VDA gewährleistet wird. Die unbefristete Vorhaltung der Widerrufsinformationen eines qualifizierten Zertifikats über den Zeitraum seiner Gültigkeit stellt für deutsche VDA eine Benachteiligung im europäischen Wettbewerb dar und ist allgemein unüblich (siehe hierzu RFC 5280, EN 319 412-5). Von daher ist eine Konkretisierung des Zeitraums innerhalb der Betriebszeit des VDA auf 12 Monate hinreichend. Qualifizierte Bewahrungsdienste sind darauf ausgerichtet, über diesen Zeitraum hinaus die Prüfbarkeit des Zertifikats sicherzustellen. Es sollte nicht die Verpflichtung des zertifikatsausgebenden VDA sein, die Aufgaben des qualifizierten Bewahrungsdienstes übernehmen zu müssen. Es entsteht zusätzlicher Erfüllungsaufwand für die Wirtschaft.

Konkretisierung von Abs. 4:

Ein qualifizierter Vertrauensdiensteanbieter muss ~~soll~~ die Bundesnetzagentur über eine beabsichtigte Betriebseinstellung im Sinne des § 16 Absatz 1 Satz 1 des Vertrauensdienstegesetzes unverzüglich unterrichten.

Begründung:

Das Wort „muss“ setzt in der Kommunikation die Transparenz voraus und fördert damit die Planbarkeit für alle Beteiligten.

Berlin, 26.07.2018