BETREFF:

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 (eIDAS-Durchführungsgesetz)

Beteiligung von Ländern, kommunalen Spitzenverbänden, Fachkreisen und Verbänden (§ 47 Absatz 1 der Gemeinsamen Geschäftsordnung der Bundesministerien - GGO)

HIER:
Stellungnahme der TÜV-Informationstechnik, akkreditierte Konformitätsbewertungsstelle für Qualifizierte Vertrauensdiensteanbieter und die von ihnen erbrachten Qualifizierten Vertrauensdienste im Anwendungsbereich der Verordnung (EU) Nr.910/2014

Zum o.g. Referentenentwurf vom 18.10.2016 13:02 Uhr nehmen wir wie folgt Stellung:

- Seite 2, Abschnitt E.2, erster Absatz:
  …Verordnung (EU) Nr. 1143/2014…
  Der Verweis scheint nicht zu stimmen: VO 1143 ist die „**Verordnung (EU) Nr. 1143/2014 des Europäischen Parlaments und des Rates vom 22. Oktober 2014 über die Prävention und das Management der Einbringung und Ausbreitung invasiver gebietsfremder Arten**“.

- Seite 6, § 2
  In § 2 sollte auch die Zusammenarbeit der Aufsichtsstellen geregelt werden. Sie sollen ihre Anforderungen abstimmen, so dass diese insbesondere nicht widersprüchlich sind und durch Vertrauensdiensteanbieter (und Konformitätsbewertungsstellen) gemeinsam erfüllt werden können.

- Seite 9, § 10 Absatz 2
  Sofern personenbezogene Daten (Identitätsdaten) genutzt werden, die zu einem früheren Zeitpunkt erhoben worden sind, müssen diese der im Antragsverfahren handelnden Person eindeutig zugeordnet werden können: gehören die Identitätsdaten zur handelnden Person? Dies ist insbesondere vor dem Hintergrund neuer online geführter medienbruch-freier Antragsprozesse wichtig, in deren Rahmen bereits erhobene Identitätsdaten weiter genutzt werden und der Antragsteller nicht mehr persönlich in Erscheinung tritt.
  Daher sollte der letzte Satz umformuliert werden:
  „…sofern diese Daten die zuverlässige Identitätsfeststellung des Antragstellers zum Zeitpunkt der Antragstellung gewährleisten.“

  Ferner: Meinen die Begriffe "Nutzer" im Vergleich zum "Antragsteller" weiter oben in § 10 unterschiedliche Personen? Der Unterschied sollte ggf. erläutert werden.

- Seite 9, § 12
  In § 12 wird an verschiedenen Stellen von Anbietern gesprochen. Es sollte jedoch einheitlich der Begriff "qualifizierter Vertrauensdiensteanbieter" gewählt werden.

- Seite 10, § 13, 14 & 15, Fragen des Editors
  Antwort: Ja, auch bei Website-Zertifikaten ist die Möglichkeit eines Widerrufs nicht

nur möglich, sondern unbedingt erforderlich.

- Seite 11, § 15
  In § 15(3) (und 19(1) Nr. 5) wird der Begriff „Siegel“ verwendet, wobei hier nicht ein elektronisches Siegel nach eIDAS gemeint ist. Um Verwechslungen auszuschließen, sollte „Siegel“ hier durch den Begriff Gütezeichen o. ä. ersetzt werden.

- Seite 11, § 15 Absatz 2, Letzter Satz
  Um diese Anforderung erfüllen zu können, benötigt der Vertrauensdienstanbieter technische Informationen über die Systeme der Aufsichtsstelle und deren Schnittstellen. Es sollte daher ein Satz ergänzt werden, dass die Aufsichtsstelle Informationen dazu zur Verfügung stellt.

- Seite 12, §16 (1)
  Die in § 16(1) beschriebene Aufgabe, entsprechende Kriterien festzulegen und zu veröffentlichen obliegt der Deutsche Akkreditierungsstelle GmbH (DAkkS). Daher sollte diese Aufgabe nicht (zusätzlich) dem BSI übertragen werden. Ebenso erscheint die angegebene Begründung nicht passend. Daher sollten die Sätze 2 und 3 gestrichen werden.
  Wenn Rahmenanforderungen definiert werden sollen, sollten diese als Verordnungsermächtigung in § 20 aufgenommen werden. Das Ergebnis könnte analog zu den Anforderungen aus § 16 (3) SigV lauten. In diesem Zusammenhang sollte überlegt werden, ob auch Zertifizierungsstellen und KBS, die als beliehene Prüfer für das BSI / BNetzA tätig sein können, analog § 18 SigG / 16 SigV mit aufzunehmen sind.

- Seite 12, § 18
  Die Formulierung sollte derart gewählt werden, dass daraus keine Einschränkung der Unabhängigkeit akkreditierter Konformitätsbewertungsstellen (KBS) abgeleitet werden kann. Idealerweise sollte den KBS explizit die Weiterverwendung der vorliegenden Nachweise gestattet werden (vergl. Formulierungsvorschlag unten). Ferner wäre in diesem Fall zu überlegen, in wie fern das BSI als zuständige Stelle gemäß De-Mail-Gesetz zur Unterstützung (Beantwortung und Interpretation der weiterzuverwendenden Nachweise) der betroffenen KBS verpflichtet werden müsste, sofern der Diensteanbieter zustimmt.

  Formulierungsvorschlag:
  „Bei Vorliegen einer Akkreditierung des Diensteanbieters nach Abschnitt 4 des De-Mail-Gesetztes, darf die Konformitätsbewertungsstelle bei der Konformitätsbewertung qualifizierter Dienste für die Zustellung elektronischer Einschreiben die im Rahmen der Akkreditierung nach De-Mail-Gesetz erbrachten Nachweise anerkennen. Das BSI unterstützt die Konformitätsbewertungsstelle bei der Interpretation der Nachweise.“

- Seite 14, § 20
  In § 20 sollte die Ermächtigung zur Festlegung der Algorithmengültigkeit mit aufgenommen werden. Wenn Algorithmen nicht verpflichtend definiert werden können, sollte das BSI verpflichtet sein, Empfehlungen zu veröffentlichen. (Analog Anlage 1 I Nr. 3 SigV).

- Seite 16, Artikel 4
  Es ist zu erklären, warum nach Artikel 3, Änderung des PA-Gesetz ausschließlich das BSI die Zertifizierung als QSCD durchführen darf. Eine solche Festlegung erscheint im Widerspruch zu den Vorgaben der eIDAS-VO.

- Seite 40, Begründung zu § 4, letzter Satz
  Es sollte erläutert werden, wie sich aus den Angaben der eIDAS-VO das

Kettenmodell ableitet. Die Begründung kann im Anschluss zur harmonisierten Interpretation der eIDAS-VO in Europa herangezogen werden.

- Im Teil „Begründung“ wird an einigen Stellen (z.B. „Zu § 14“ & „Zu § 15“) auf eine nach § 23 zu erlassende Rechtsverordnung verwiesen. Die zu erlassende Rechtsverordnung ist jedoch in § 20 geregelt.

- Aufgrund der vorhandenen Nachfrage im Markt sollte überlegt werden, ob nicht Bestätigungen von Signaturanwendungskomponenten einschließlich Anzeigekomponente zur Erzeugung und Prüfung von Signaturen als freiwillige Leistung definiert werden können (§§ 17(2) SigG / 15(2) SigV.)