Stellungnahme zum Referentenentwurf „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“

(Bearbeitungsstand: 18.10.2016 13:02 Uhr)

Ernst G. Giessmann*
Institut für Informatik – Humboldt-Universität zu Berlin

31. Oktober 2016

Anmerkung

Der besseren Lesbarkeit halber werden die Zitate farblich hervorgehoben. Die Reihenfolge der Kommentare wird durch das Dokument bestimmt und ist keine inhaltliche Wertung. Ergänzende Vorschläge stellen nur meine eigene und nicht die Meinung des Instituts oder der Humboldt-Universität zu Berlin dar.

Seite 1

Um dem Ziel der eIDAS-Verordnung nach effektiveren elektronischen Transaktionen gerecht zu werden, sind die Anwendungsmöglichkeiten für elektronische Vertrauensdienste zu erweitern. Dies gilt insbesondere für das in der eIDAS-Verordnung erstmals geregelte elektronische Siegel.

Editorische Anmerkung: An dieser Stelle und auch später in der Begründung wird darauf hingewiesen, dass durch die Verordnung erstmals elektronische Siegel geregelt werden. Damit wird auch ein Vorschlag aus dem Signaturbündnis umgesetzt, als seinerzeit gefordert wurde, sogenannte *Organisationszertifikate* zu spezifizieren. Ergänzend könnte man auch erwähnen, dass auch die *qualifizierten Zeitstempel*, die ja bereits auch schon im Signaturgesetz definiert wurden, nun auf europäischer Ebene erstmals geregelt werden.

Seite 9

§ 11 Attribute in qualifizierten Zertifikaten für elektronische Signaturen
(3) Attribute können auch in ein gesondertes qualifiziertes Zertifikat (qualifiziertes Attribut-Zertifikat) aufgenommen werden. Bei einem qualifizierten Attribut-Zertifikat können die Angaben nach Anhang I der Verordnung (EU) Nr. 910/2014 durch eindeutige Referenzdaten des qualifizierten Zertifikates, auf das sie Bezug nehmen, ersetzt werden, soweit sie nicht für die Nutzung des qualifizierten Attribut-Zertifikates benötigt werden.

Technische Ergänzung: Für qualifizierte Attribut-Zertifikate wird es wahrscheinlich keine technische Spezifikation (beispielsweise ein Zertifikatsprofil) geben. Zu unterschiedlich waren die Vorstellungen innerhalb des Technischen Komitees „Elektronische Signaturen und Infrastrukturen“ bei ETSI. Im Interesse der Interoperabilität sollte deshalb im Gesetz auf eine

*mailto:*giessman@informatik.hu-berlin.de*

Regelung zu Attribut-Zertifikaten verzichtet werden (sie werden ja auch gar nicht in der Überschrift erwähnt). Statt zusätzlich ein Attribut-Zertifikat zu erstellen, besteht die in jedem Fall technisch leichter umzusetzende Möglichkeit, Attribute in ein qualifiziertes Zertifikat zu übernehmen. Statt optionaler Attribut-Zertifikate hat man dann die Auswahl zwischen zwei (oder mehreren) qualifizierten Zertifikaten mit jeweils unterschiedlichen zusätzlichen Attributen.

Textvorschlag: Absatz 3 streichen.

§ 12 Unterrichtung über Sicherheitsmaßnahmen und Rechtswirkungen
(1) 2. darauf hinzuweisen, dass qualifiziert elektronisch signierte, gesiegelte oder zeitgestempelte Daten bei Bedarf neu zu sichern sind, bevor der Sicherheitswert der vorhandenen Signaturen, Siegel oder Zeitstempel durch Zeitablauf geringer wird,

Technische Ergänzung: Bevor der Sicherheitswert erstellter Signaturen, Siegel oder Zeitstempel verblasst, sind immer entsprechende Maßnahmen zu ergreifen. Die aktuelle Formulierung „sind neu zu sichern“ trägt dem jedoch nicht ausreichend Rechnung. Möglich ist auch die Nutzung eines qualifizierten Bewahrungsdienstes, der nicht die Daten „neu“ sichern muss, sondern die Bindung der Daten und Signaturen an den ursprünglichen Erstellungszeitpunkt fixieren muss.

Textvorschlag: 2. darauf hinzuweisen, dass qualifiziert elektronisch signierte, gesiegelte oder zeitgestempelte Daten durch geeignete Maßnahmen zu schützen sind, bevor der Sicherheitswert der vorhandenen Signaturen, Siegel oder Zeitstempel durch Zeitablauf geringer wird

Seite 10

§ 13 Widerruf qualifizierter Zertifikate

Nachfrage: Das Signaturgesetz hat bisher statt dem *Widerruf* den Begriff der *Sperrung* verwendet. Auch für die so genannte *certificate revocation list* hat sich im deutschen Sprachgebiet die Bezeichnung *Sperrliste* durchgesetzt. Warum wurde hier auf die Kontinuität in den Bezeichnungen verzichtet?

Weitere Widerrufsgründe können vertraglich vereinbart werden.

Editorische Anmerkung: Die Verordnung benennt in den Erwägungsgründen auch die *Aussetzung von Zertifikaten* (Recital 53) und stellt es den Mitgliedsstaaten frei, das zu regeln. Eine Beschreibung der Regelungen zur Aussetzung muss auch bei der Notifizierung angegeben werden. Da sich bei der Aussetzung von Zertifikaten technische Probleme bei der Gültigkeitsprüfung ergeben könnten, wäre eine gesetzliche Regelung, die die Aussetzung für in Deutschland zugelassene Vertrauensdiensteanbieter nicht erlaubt, sinnvoll.

Seite 40

Eine Regelung zur Gültigkeit der qualifizierten Zertifikate entsprechend § 19 Absatz 5 SigG ist nicht erforderlich. Eine solche Regelung zum Gültigkeitsmodell enthält Artikel 32 Absatz 1 Buchstabe a der eIDAS-Verordnung im Sinne des Kettenmodells.

Technische Ergänzung: Auch die durch das Signaturgesetz erzwungene Regelung des Kettenmodells, dass gesperrte ZDA-Zertifikate keine Auswirkungen auf die Gültigkeit der Nutzerzertifikate haben, ist zukünftig nicht mehr erforderlich. Mit der Einstellung des Betriebs können die Zertifikate eines Vertrauensdiensteanbieters übernommen werden und müssen nicht, wie seinerzeit in SigG § 16 (1) vorgeschrieben, in jedem Fall gesperrt werden.

Textvorschlag: Regelungen zur Sperrung von ZDA-Zertifikaten, die sich bisher aus dem Kettenmodell ergaben, sind ebenfalls nicht mehr erforderlich, da mit der Einstellung des Betriebs die Zertifikate durch einen anderen Vertrauensdiensteanbieter übernommen werden können.

Seite 44

Die langfristige Sicherung qualifiziert signierter Daten erfolgt derzeit durch Neusignieren der signierten Daten, bevor die verwendeten Algorithmen und Parameter ihre Sicherheitseignung verlieren.

Editorische Anmerkung: Neben der Neusignierung konnte man bisher auch einen qualifizierten Zeitstempel verwenden.

Textvorschlag: Die langfristige Sicherung qualifiziert signierter Daten erfolgt derzeit durch Neusignieren oder erneutes Zeitstempeln der signierten Daten, bevor die verwendeten Algorithmen und Parameter ihre Sicherheitseignung verlieren.

Seite 47

Die Abnahme von Bewertungen auf Korrektheit der Implementierung kryptografischer Algorithmen und von Zufallszahlengeneratoren wird vom BSI durchgeführt.

Technische Ergänzung: Die Veröffentlichung der Festlegungen zu den geeigneten Algorithmen und Parametern (Algorithmen-Katalog) sollte jedoch wie bisher durch die Aufsichtsbehörde nach einer Anhörung von Experten aus Wirtschaft und Wissenschaft erfolgen (SigV Anlage 1, I.2).

Textvorschlag: Die Veröffentlichung der Festlegungen zu den geeigneten Algorithmen und Parametern durch die Aufsichtsstelle wird in der Rechtsverordnung nach § 20 geregelt. Bei den jährlichen Anhörungen sind Experten aus Wirtschaft und Wissenschaft zu beteiligen.