Koordinierungsstelle
für IT-Standards

Freie Hansestadt Bremen

Die Senatorin für Finanzen

02 – Zentrales IT-Management und E-Government

Koordinierungsstelle für IT-Standards (KoSIT)

Rudolf-Hilferding-Platz 1

28195 Bremen

Bremen, den 1.11.2016

Stellungnahme zum Referentenentwurf eines eIDAS-Durchführungsgesetzes

Wir bedanken uns für die Zusendung des Entwurfs 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. Hierzu möchten wir wie folgt Stellung nehmen.

1. Zur Attributzertifikaten gem. § 11 VDG-E

In § 11 wird ausgeführt, dass bestimmte Attribute (Vertretungsmacht, berufsbezogene und sonstige Angaben) in Zertifikaten oder in gesonderten Attributzertifikaten enthalten sein können. Dieses steht im Einklang mit Artikel 24 eIDAS-VO. Gleichzeitig gibt es in diesem Kontext aber eine Standardisierungslücke, da ETSI diese Attribute in der einschlägigen ETSI EN 319 412-2 bisher nicht profiliert hat. Dort findet sich nur der normative Hinweis auf den IETF RFC 3739, der ein qualifiziertes Zertifikatsprofil beschreibt und den IETF RFC 5280, der das grundsätzliche Zertifikatsprofil definiert. Einen Hinweis auf mögliche Attribute im oben genannten Sinne findet sich nicht in der EN.

Die Deutsche Profilierung CommonPKi hat signaturgesetzkonforme ausschließliche Attribute als private Extensions, die nicht international standardisiert sind, in Stammzertifikaten oder als Attribute in Attributzertifikaten definiert. Eine EU-weite Interoperabilität ist somit nicht gegeben. Eine Anzeige der Inhalte und automatisierte Auswertung ist in der Regel im EU-Ausland nicht möglich. Technisch gesehen sind Validierungskomponenten zunächst aber einmal generische Prüfkomponenten, d.h. es reicht im Prüfprotokoll nur die Inhalte dieser Attribute anzuzeigen und die Gültigkeit der Attributzertifikate zu prüfen. Den grenzüberschreitenden Austausch von mit Attribut-Zertifikaten signierten Objekten halten wir für problematisch. Die Anwender in den empfangenden Mitgliedstaaten könnten im Zweifelsfall diese Informationen nicht interpretieren. Ebenso wie Anwender in Deutschland nicht mit alternativen proprietären Spezifikationen aus anderen Mitgliedstaaten umgehen können, da diese Profilierungen nicht bekannt sind.

Aus kommunaler Sicht erscheint es problematisch, dass gemäß § 11 Abs. 1 in den Zertifikaten Attribute zur Vertretung aufgenommen werden. Der Nachweis dafür ist nur zu einem einzigen Zeitpunkt zu erbringen, während die Verwendung fortlaufend erfolgt. Es wäre das Risiko der öffentlichen Verwaltung, diesem Nachweis zu glauben und es kann nicht Aufgabe der Verwaltung sein, die aktuelle Pflege von Arbeitgeber - /Arbeitnehmerbeziehungen und Vertretungsbefugnissen sicherzustellen. Die zusätzlichen Attribute besitzen insoweit nicht die dauerhafte Glaubwürdigkeit und Beweiskraft wie der eigentliche Identitätsnachweis.

2. Zum Widerruf vom Zertifikaten gem. § 13 VDG-E

Es stellt sich grundsätzlich die Frage, warum die Frage des Widerrufs qualifizierter Zertifikate in dieser Art und Weise auf gesetzlicher Ebene erfolgt. Üblicherweise sind dies Themen, die ein Zertifizierungsdiensteanbieter in seine Certification Policy bzw. in seinem Certification Practice Statement regelt bzw. auf Grundlage seiner Allgemeinen Geschäftsbedingungen mit seinen Kunden vereinbart. Es sollte dann die Aufgabe der Konformitätsbewertungsstelle sein, zu prüfen, ob die Vorgaben der eIDAS-VO, insbesondere aus Art. 24 Abs. 3 hinreichend sicher umgesetzt wurden. Als dies in der Signaturrichtlinie 1999/93/EG nicht geregelt war, hatte der deutsche Gesetzgeber die Möglichkeit, aber nicht die Verpflichtung, diese Frage des Widerrufs in seinem Signaturgesetz umsetzen. Es stellt sich nun die Frage, ob dieses Thema nicht durch die eIDAS-VO abschließend geregelt ist und es aus Sicht des europäischen Gesetzgebers eine Ermächtigungsgrundlage gibt, dies in einzelnen Mitgliedstaaten selbst und im Zweifelsfall unterschiedlich zu regeln. Im Übrigen erscheint dies wiederum als eine Regelung, die sich an Vertrauensdiensteanbieter in der Ausprägung Zertifizierungsdiensteanbieter, weswegen – falls die Regelung beibehalten wird – ein Hinweis erfolgen sollte, dass Vertrauensdienste anderer Ausprägung hiervon nicht betroffen sein sollen. Dann allerdings sollte sich die Vorschrift auch an Zertifizierungsdiensteanbieter richten, die qualifizierte elektronische Siegel herausgeben.

3. Zum Fehlen eines deutschen Algorithmenkataloges

Mit Erstaunen haben wir zur Kenntnis genommen, dass in dem Entwurf eines Vertrauensdienstegesetzes keine Ermächtigung zum Erlass einer Verordnung enthalten ist, wie sie sich derzeit aus Abschnitt I Nr. 1.2 der Anlage 1 zur Signaturverordnung ergibt. Wir möchten darauf aufmerksam machen, dass wir einen deutschen Algorithmenkatalog nach wie vor für notwendig halten. Die von der KoSIT betreuten Standards für den elektronischen Datenaustausch XÖV (XML in der öffentlichen Verwaltung (XÖV) verweisen jeweils auf die gültige OSCI-Spezifikation, die auf die Verwendung sicherer, geeigneter Algorithmen abstellt. Grundlage hierfür bildet bislang der genannte deutsche Algorithmenkatalog, der durch die Bundesnetzagentur als aufsichtsführender Stelle nach SigG/SigV veröffentlicht wird. Letztlich ist es für öffentliche Verwaltung egal, welche Bundesbehörde den Algorithmenkatalog veröffentlicht. Wichtig für das deutsche eGovernment mit seinen XÖV-Einsatzszenarien ist, dass mit dem Außerkrafttreten der Signaturverordnung nicht auch beiläufig die genannten Regelung, namentlich der deutsche Algorithmenkatalog, abgeschafft wird. Wir schlagen deshalb vor, in § 20 Abs. 1 des Vertrauensdienstegesetzes auch eine Regelung aufzunehmen, die die Aufnahme der genannten Vorschrift in eine künftige Vertrauensdiensteverordnung zulässt. In diesem Zusammenhang ist es auch wichtig, auf den zeitlichen Rahmen zu achten. Es darf aus unserer Sicht nicht dazu kommen, dass die Verpflichtung einen solchen Algorithmenkatalog zu erlassen, bis zum möglichen Erlass einer Vertrauensdiensteverordnung zwischenzeitlich nicht besteht.

4. Zur Nennung des Kettenmodells

In der Begründung zu § 4 VDG wird ausgeführt: „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.“ Dort wird ausgeführt „(1) Mit dem Verfahren für die Validierung einer qualifizierten elektronischen Signatur wird die Gültigkeit einer qualifizierten elektronischen Signatur bestätigt, wenn a) das der Signatur zugrunde liegende Zertifikat zum Zeitpunkt des Signierens ein qualifiziertes Zertifikat für elektronische Signaturen war, das die Anforderungen des Anhangs I erfüllt ….“.

Die ETSI Standards und insbesondere der ETSI-Standard EN 319 102-1 V1.1.1 2016, lassen sowohl das Schalen- wie auch das Kettenmodell zu, so dass sowohl ein Prüfung nach dem Kettenmodell, aber eben auch nach dem Schalenmodell möglich ist. Es hängt immer von dem Signierenden oder dem Prüfenden ab, welches Modell zur Anwendung kommt. Daher empfehlen wir zur Vermeidung von Fehlinterpretationen, auf eine Nennung des Kettenmodells in der Begründung zu verzichten. Es wird vorgeschlagen, die Festlegung auf Kettenmodell zu streichen, da ETSI-Norm kein der genannten Ansätze favorisiert.

i.A. Schulte