Bundesnetzagentur

Überblick über das Vertrauensdienstegesetz: Dauerhaft prüfbare Vertrauensdienste

Konstantin Götze, Referent elektronische Vertrauensdienste

eIDAS-Symposium Deutscher EDV Gerichtstag

Berlin, 22.06.2017

Was ist das VDG?

Unter Federführung des BMWi wurde ein Entwurf eines eIDAS-Durchführungsgesetzes abgestimmt.

Das VDG ist der wesentliche Teil dieses Artikelgesetzes. Es soll zwei Aufgaben erfüllen:

1. Die eIDAS-VO hat Regelungslücken, die für ihre Durchführbarkeit geschlossen werden müssen.

2. Ein Übergang vom dt. Signaturrecht zur eIDAS-VO unter Wahrung der Kontinuität der existenten Dienste sollte ermöglicht werden.

Was ist das VDG?

Die Entscheidung hinsichtlich des Übergangs fiel zugunsten einer kompletten, zeitgleichen Ablösung des SigG durch ein VDG und gegen eine weitergehende parallele Geltung von SigG (wo noch anwendbar) und eIDAS aus.

Durch die Entscheidung für eine Stichtagsablösung müssen die Verweise auf das SigG in Fachgesetzen zeitgleich angepasst werden und es sind Übergangsregelungen für Anbieter erforderlich.

Anpassung von Verweisen

Beispiele für Verweisänderungen:
(Löschung des Bezugs zum SigG)

- § 126a BGB
- §§ 130a, 174, 371a ZPO
- § 3a VwVfG
- §§ 55a, 100 VwGO
- § 41a StPO
- §110a-d OWIG
- § 42 BeurkG

Schließen von Regelungslücken

Beispiele für Regelungslücken:

- Zuständigkeiten für die Aufsicht über Anbieter / für die Zertifizierung von QSEE / für das Führen und Veröffentlichen der deutschen Vertrauensliste

- Barrierefreiheit (stärkere Berücksichtigung der Bedürfnisse von Menschen mit Behinderungen)

Schließen von Regelungslücken

- Datenschutz – es widerstreiten das Interesse am Schutz persönlicher Daten und der Sicherheit bei der Erbringung und dem Komfort bei der Nutzung von Vertrauensdiensten
  (Anpassung an EU-Datenschutz-Grundverordnung erfolgt am 25. Mai 2018)

- Deckungsvorsorge für Anbieter – die Höhe orientiert sich am SigG/der SigV

- Bußgelder/Gebühren – Erforderlich für die Arbeit von BSI/BNetzA

Schließen von Regelungslücken

Bei den Deckungsvorsorgesummen für Anbieter, Bußgeldern und Gebühren bestehen somit Unterschiede zwischen den Mitgliedsstaaten, die sich in unterschiedlichen Marktchancen für die Anbieter manifestieren können.

Sicherheit und Kosten stehen faktisch im Wettstreit!

Diesbezügliche Harmonisierung ist ein angestrebtes Ziel der Aufsichtsstellen (FESA).

Altlasten aus dem SigG

Beispiele für Altlasten:

- Attribute in qualifizierten Zertifikaten – Klarstellung der weiteren Verwendbarkeit ausdrücklich von Berufsattributs-Trägern gewünscht

- Haftung: Exkulpationsausschluss für Verrichtungsgehilfen wird beibehalten

- Unterrichtungspflichten und Informationsmöglichkeiten über Produkte und Algorithmen (statt Herstellererklärungen)

Altlasten aus dem SigG

- Identitätsprüfung mittels „sonstiger geeigneter Verfahren“ – BNetzA veröffentlicht periodisch Anforderungen an solche Verfahren und beurteilt kurzfristig neue, innovative Identifizierungsverfahren im Einvernehmen mit dem BSI.

- Akkreditierung nach dem SigG und auf Dauer prüfbare Vertrauensdienste eingebettet in den „Beendigungsplan“ nach eIDAS (§ 16 VDG)

Quo vadis Akkreditierung?

Signaturgesetz	eIDAS
Bestätigung der „technischen und administrativen Sicherheit“ durch Prüf- und Bestätigungsstelle	Bestätigung der Konformität zu den Vorgaben der eIDAS durch Konformitätsbewertungsstelle
Gütezeichen der BNetzA	Vertrauenssiegel der EU
Technische Prüfbarkeit der Zertifikate der Anbieter gegen die „Wurzel“ der BNetzA	Technische Prüfbarkeit der Zertifikate der Anbieter gegen die Vertrauensliste (TL) der BNetzA
Sperrung der Zertifikate als technischer „Showstopper“	Statusentzug in der TL als technischer „Showstopper“
„Ewigkeitsgarantie“ für Zertifikate	???

Langfristige Verfügbarkeit nach eIDAS?

Pflichten qualifizierter Anbieter nach eIDAS:

- Art. 24 (2) lit. h) eIDAS: Einschlägige Informationen über ausgegebene und empfangene Daten sind so aufzubewahren, dass sie über den Zeitpunkt der Einstellung der Tätigkeit hinaus verfügbar sind.

Zweck: Beweise liefern zu können und die Kontinuität des Dienstes sicherzustellen.

Langfristige Verfügbarkeit nach eIDAS?

Nähere Ausgestaltung der Norm z.B. durch Standard ETSI EN 319 411-1

The TSP shall retain [log(s) of all events relating to the life cycle of keys managed by the CA…] for at least seven years after any certificate based on these records ceases to be valid.

Damit ist nichts über Art und Dauer des Vorhaltens der Informationen nach der Einstellung des Betriebs des Zertifikatsausstellers ausgesagt!

Langfristige Verfügbarkeit nach eIDAS?

- Art. 24 (4) eIDAS: Informationen über den Gültigkeits- oder Widerrufsstatus sind jederzeit und über die Gültigkeitsdauer des Zertifikats hinaus automatisch auf zuverlässige, kostenlose und effiziente Weise bereitzustellen.

  Damit ist erneut nichts über Art und Dauer des Vorhaltens der Informationen nach der Einstellung des Betriebs des Zertifikatsausstellers ausgesagt!

Langfristige Verfügbarkeit nach eIDAS?

- Bewahrungsdienste für qualifizierte e. Signaturen als eIDAS-Pendant zum Verzeichnis der BNetzA?

Bewahrungsdienste beziehen sich immer nur auf signierte oder gesiegelte Dokumente (einschließlich der entsprechenden Zertifikate), für die jemand aktiv eine Sicherung durch den Bewahrungsdienst in Auftrag geben muss. Spontanes Entstehen eines Bedarfs - i.d.R. beim zufällig Prüfenden - ist so nicht abzufangen.

Langfristige Verfügbarkeit nach eIDAS?

Das Ausfallrisiko dieser Anbieter besteht ebenso wie bei Zertifikatsausstellern. Es sind keine 30+ Jahre Aufbewahrung gewährleistet.

Fazit:

Abschwächung der Verfügbarkeit gegenüber der „Ewigkeitsgarantie“ nach SigG!

Regelungsspielräume der eIDAS?

Art. 17 (5) eIDAS gibt Regelungsspielraum für eine Vertrauensinfrastruktur der Aufsichtsstelle

- Möglichkeit der Regelung im VDG
- Nutzungen z.B. im eGovernment, für DE-Mail, im BeurkG, Gesundheitswesen, Verteidigung etc. mit Bezug auf „langfristig prüfbare Zertifikate“

Fazit: Möglichkeit und Notwendigkeit der Angleichung an SigG besteht!

Zusammenfassung

- Aufbewahrungspflicht für Zertifikate akkreditierter Anbieter nach SigG besteht für mindestens 30 Jahre
- Fachverfahren und Gesetze setzen auf diese langfristige Verfügbarkeit
- Die eIDAS selbst bietet keine gleichwertige Regelung
- Sie sieht jedoch den Aufbau einer Vertrauensinfrastruktur nach nationalem Recht vor
- Das VDG soll diese etablieren und das SigG ablösen

Technische Ausgestaltung

SigG:

- ~~Produktion (Root-CA)~~
- Verzeichnisdienst
- ~~Sperrung~~

eIDAS:

- Vertrauensliste
- Algorithmen

„Friedhofsverwaltung“ für

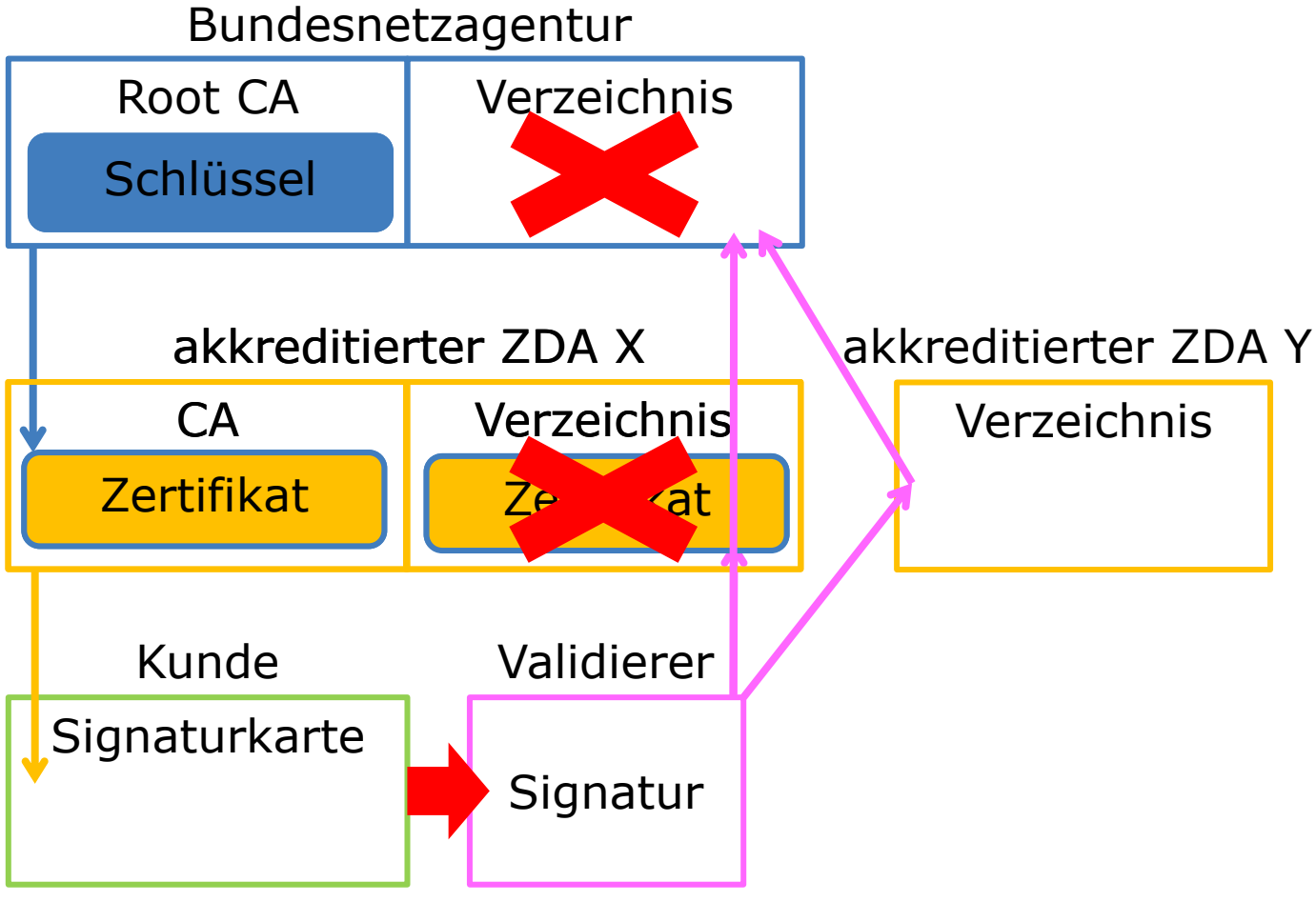
- bisherigen Datenbestand der BNetzA nach SigG
- Dienste-/Endnutzerzertifikate von Signatur-/Siegel-Anbietern nach VDG

Keine Root-CA mehr

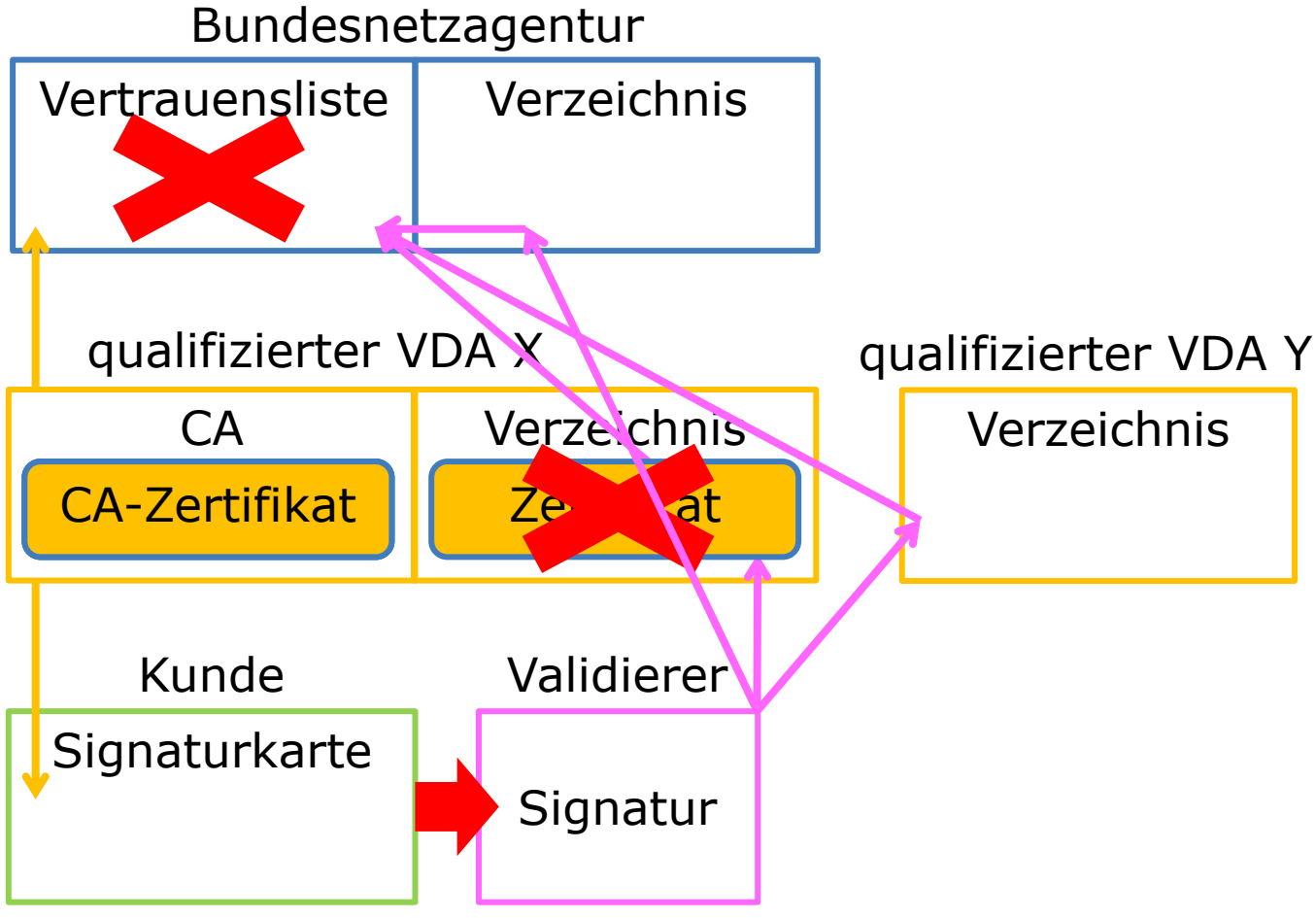
- neue Vertrauensinfrastruktur
- keine Produktion/Sperrung von Dienstezertifikaten

Einbindung eines elektronischen Algorithmenkatalogs für langfristige Sicherheit

Betriebseinstellung nach SigG Variante 2



Betriebseinstellung nach VDG Var. 1



Übergang für akkreditierte Anbieter

- Akkreditierung entfällt mit Ende SigG
- Dienstezertifikate der BNetzA können für eine Übergangszeit weitergenutzt werden
- Kundenzertifikate können weiter genutzt und vom qualifizierten Anbieter beauskunftet werden
- Der Kunde merkt von der Umstellung nichts!

Bei Betriebseinstellung erfolgt eine Überführung in die Vertrauensinfrastruktur der BNetzA, die „Ewigkeitsgarantie“ als SigG-Erbe bleibt gewahrt.

Aktueller Sachstand und Ausblick

Das eIDAS-DurchführungsG wurde am 16. März der EU-Kommission notifiziert, die Stillhaltefrist lief bis diesen Montag (19.06.).

Heute gegen 12:20 findet die abschließende Beratung und Beschlussempfehlung des Bundestages statt.

Anfang Juli soll der Bundesrat zustimmen.

Damit findet der Übergang vom SigG zum VDG voraussichtlich Anfang August statt.

Bundesnetzagentur

Vielen Dank!

Konstantin Götze
Referent elektronische Vertrauensdienste

+49 6131 18 - 0
konstantin.goetze@bnetza.de