EIN EUROPAWEITES NETZWERK VERTRAUENSWÜRDIGER IDENTITÄTEN?

Alexander Konzelmann

Abteilungsleiter Rechtsdatenbanken, Richard Boorberg Verlag Stuttgart
Scharrstraße 2, 70563 Stuttgart, DE
a.konzelmann@boorberg.de; http://www.boorberg.de

Schlagworte: ***elektronische Signatur, Signaturkarte, e-ID, elektronische Identifizierung, Vertrauensdienste, online-Zertifikate, eIDAS, VO (EU) Nr. 910/2014, Kommunikation und Sicherheit; Datenschutz und Datensicherheit, E-Commerce, E-Government, Telekommunikationsrecht, Internet Governance***

Abstract: *Die Signaturrichtlinie (1999/93/EG) wird nach fünfzehnjährigem Bestehen durch die 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 abgelöst, deren Regelungsgegenstand wesentlich über jenen der Richtlinie hinausgeht. Der Beitrag versucht, Gemeinsamkeiten und Unterschiede der beiden Rechtsakte und die zu erwartenden Auswirkungen in der innerstaatlichen Rechtspraxis zu benennen.*

1. Praxiswirkungen der Verordnung (EU) Nr. 910/2014

Die Verordnung (EU) Nr. 910/2014[1] wird gerne mit dem Kürzel «eIDAS» belegt. Ihr deutscher Titel ist allerdings «Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt» und im Englischen lautet er «Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market». Das geläufige Kürzel scheint auf «electronic identification, authentication and signatures» zurückzugehen.

Die 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 tritt Mitte 2016 an die Stelle ihrer Vorgänger-Richtlinie 1999/93/EG[2]; diese hatte jedoch lediglich die Qualität einer Richtlinie, war also von den Mitgliedstaaten umzusetzen, wohingegegen die neue Verordnung unmittelbare Geltung entfaltet und gegenüber abweichendem innerstaatlichen Recht Vorrang beansprucht. Sollten also bereits getroffene legislative Entscheidungen im Bereich der elektronischen Identitätsfeststellung mit Signaturkarten und ähnlichen Systemen von der neuen EU-Verordnung abweichen, dann stünde dies der gegenseitigen Anerkennung der darauf beruhenden Systeme im Wege. Im Vordergrund stehen die Interoperabilität von Systemen und das grenzüberschreitend abgeleitete Vertrauen in ausländische Identifikationssysteme, denn unterschiedliche Schutzniveaus entwickeln sich zu einem Hemmnis für den Binnenmarkt. Hinzu kommt die Vollregulierung sogenannter Vertrauensdienste. Der Beitrag versucht, grundlegende Abweichungen von der Vorgänger-Richtlinie und die daraus zu erwartenden Auswirkungen in der innerstaatlichen Rechtspraxis zu benennen. Zu diesem Zweck wurden Richtlinie und Verordnung ausgewertet und dabei insbesondere die Definitionen und Tatbe-

[1] Verordnung 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 (ABl. L 257 vom 28. August 2014 S. 73).

[2] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. L 13 vom 19. Januar 2000, S. 12).

stände im Dunstkreis um die Authentifizierungsfunktion der digitalen Signatur – jetzt: der «elektronischen Signatur» – abgeglichen. Die Reihenfolge orientiert sich lose am Aufbau der bisherigen EU-Richtlinie.

2. Im Detail ergeben sich folgende Befunde:

2.1. Anwendungsbereich

Artikel 2 Absatz 3 der Verordnung stellt zur Abgrenzung des Anwendungsbereichs klar, dass die Verordnung nicht das nationale Recht oder das Unionsrecht in Bezug auf den Abschluss und die Gültigkeit von Verträgen berührt. Das heißt, es geht nur um binnenmarktliche Gleichbehandlung von in- und ausländischen digitalen Signaturen, wobei auch weiterhin den Mitgliedstaaten zusteht, die Rechtswirkungen digitaler Signaturen innerstaatlich zu regeln. Diese Regelung ist im Wortlaut abweichend, aber inhaltlich kongruent zu Artikel 1 Absatz 2 der Richtlinie von 1999.

2.2. Elektronische Signatur

Artikel 3 Ziffer 10 der Verordnung definiert die «elektronische Signatur» als Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet. Diese Legaldefinition entspricht weitgehend derjenigen aus Artikel 2 Ziffer 1 der Richtlinie. Es wurde lediglich von einer im Nominalstil formulierten finalen Komponente («Daten [...], die zur Authentifizierung dienen») übergegangen zur Anknüpfung an eine beobachtbare Tätigkeit («Daten [...], die der Unterzeichner zum Unterzeichnen verwendet»). Dies erscheint als eine Vereinfachung, die Zweifelsfragen umgeht, jedoch nicht als eine maßgebliche Änderung des Begriffsinhalts.

2.3. Definition der fortgeschrittenen elektronischen Signatur

Die Definition der «fortgeschrittenen elektronischen Signatur» war in der Richtlinie in Artikel 2 Ziffer 2 enthalten und ist in der aktuellen Verordnung aufgespalten. Sie beginnt in Artikel 3 Ziffer 11 und wird in Artikel 26 ausgeführt. Die Voraussetzungen für die «Fortschrittlichkeit» bleiben inhaltlich unverändert. Sprachlich wurde aus der «ausschließlichen» eine «eindeutige» Zuordnung zum Unterzeichner. Die Identifizierung des Unterzeichners muss nach beiden Regelwerken möglich sein. Der Unterzeichner muss nach dem neuen Wortlaut «elektronische Signaturerstellungsdaten» verwenden, die er unter seiner alleinigen Kontrolle verwenden kann; nach dem alten Richtlinientext waren es noch «Mittel [...], die er unter seiner alleinigen Kontrolle halten kann» – auch hier ist nur eine klarstellende Umformulierung zu erkennen, aber kein Bedeutungswandel. Auch die vierte und letzte Voraussetzung bleibt gleich. Die Signatur muss so mit den unterzeichneten Daten verbunden sein, dass eine nachträgliche Veränderung der Daten erkannt werden kann, geregelt in Artikel 2 Ziffer 2 Buchstabe d) der bisherigen Richtlinie und Artikel 26 Buchstabe d) der Verordnung von 2014.

2.4. Unterzeichner

In Artikel 3 Ziffer 9 der Verordnung wird der «Unterzeichner» legal definiert als natürliche Person, die eine elektronische Signatur erstellt. Das klingt einfacher als noch die Definition in Artikel 2 Ziffer 3 der Richtlinie, die mit vielen Fallunterscheidungen befrachtet lautete: «eine Person, die eine Signaturerstellungseinheit besitzt und die entweder im eigenen Namen oder im Namen der von ihr vertretenen Stelle oder juristischen oder natürlichen Person handelt». Dennoch dürfte sich im Ergebnis nichts am gemeinten Personenkreis geändert haben.

2.5. Qualifizierte elektronische Signatur

In Artikel 3 Ziffer 12 der Verordnung ist eine Legaldefinition für die «qualifizierte elektronische Signatur» hinzugekommen, die eine fortgeschrittene elektronische Signatur ist, welche von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht. Zwar ist die Definitionsform hier neu, aber diese Art der Signatur wurde auch in der Richtlinie bereits behandelt, und zwar bei der Anerkennungsverpflichtung als unterschriftsgleiches Beweismittel nach Artikel 5.

2.6. Elektronische Signaturerstellungsdaten

In Artikel 3 Ziffer 13 der Verordnung stehen nunmehr «elektronische Signaturerstellungsdaten» im Sinne «eindeutiger» Daten; in Artikel 2 Ziffer 4 der Richtlinie ging es noch um «einmalige» Signaturerstellungsdaten ohne den Zusatz «elektronisch». Da «einmalig» aber nunmehr in der Verordnung im Anhang II Absatz 1 Buchstabe b) auftaucht, ist auch bei dieser Definition nur eine Wortlautabweichung ohne inhaltliche Relevanz zu konstatieren.

2.7. Elektronische Signaturerstellungseinheit

Die in Artikel 3 Ziffer 22 genannte «Elektronische Signaturerstellungseinheit» ist eine konfigurierte Software oder Hardware, die zum Erstellen einer elektronischen Signatur verwendet wird. Sie tritt an die Stelle der «Signaturerstellungseinheit» aus Artikel 2 Ziffer 5 und an die Stelle des «Produktes für elektronische Signaturen» aus Artikel 2 Ziffer 12 der Richtlinie. Die nächste Stufe, nämlich die «Qualifizierte elektronische Signaturerstellungseinheit» aus Artikel 3 Ziffer 23 der Verordnung, wird Rechtsnachfolgerin der «sicheren Signaturerstellungseinheit» aus Artikel 2 Ziffer 6 der Richtlinie. Die Sicherheitsanforderungen ergeben sich deckungsgleich in der Richtlinie aus Anhang III, in der Verordnung aus deren Anhang II. Es handelt sich dabei um die Vertraulichkeit und Einmaligkeit sowie die nicht-Ableitbarkeit der Erstellungsdaten, um die Fälschungssicherheit der Signatur und um die Missbrauchsresistenz des Systems. Weiterhin muss gewährleistet sein, dass der Unterzeichner das Unterzeichnete Dokument wahrnehmen kann und dass die Signaturerstellung selbst dessen Inhalt nicht verändert. In diesem sensiblen Bereich der Definitionen hat sich also durch den Übergang von Richtlinie auf Verordnung keinerlei Veränderung ergeben; nur die Begrifflichkeit ist ab Juli 2016 exakter.

2.8. Pflichtangaben für Zertifikate

Nach Artikel 3 Ziffer 14 der Verordnung ist ein «Zertifikat für elektronische Signaturen» eine elektronische Bescheinigung, die elektronische Signaturvalidierungsdaten mit einer natürlichen Person verknüpft und die mindestens den Namen oder das Pseudonym dieser Person bestätigt. Dies entspricht weitgehend der Legaldefinition von «Zertifikat» in Artikel 2 Ziffer 9 der Richtlinie, außer dass dort die Option «Pseudonym» nicht erwähnt wird. In beiden Regelwerken schließt sich unmittelbar daran die «qualifizierte» Version des Zertifikats an, welches von einem qualifizierten Vertrauensdiensteanbieter ausgestellt wird und die Anforderungen des Anhangs I der Verordnung respektive des Anhangs I der Richtlinie erfüllen muss. Der «Vertrauensdiensteanbieter» hieß in der Richtlinie noch «Zertifizierungsdiensteanbieter». Die Anforderungen der Anhänge sind zwar in weiten Teilen identisch, es gibt aber festzustellende Unterschiede: die Richtlinie forderte als Merkmale qualifizierter Zertifikate nur «Angaben»; die Verordnung verlangt auch «Daten», «Codes» und Ähnliches.

2.8.1. Pflichtangaben

Übereinstimmende Pflichtangaben sind die Angabe, dass es sich um ein qualifiziertes Zertifikat handelt, der Name und Staat des Anbieters sowie der Name oder das Pseudonym des Unterzeichners, zu den Signaturerstellungsdaten kongruente Signaturprüfdaten, die in der Verordnung «Validierungsdaten» heißen, Beginn und Ende der Gültigkeitsdauer des Zertifikats und sein Identitätscode. Zu diesem Code verlangt die Verordnung nunmehr ausdrücklich, dass er für den qualifizierten Vertrauensdiensteanbieter eindeutig sein muss.

2.8.2. Unterzeichnerattribut

Der freie Platz für ein spezifisches Unterzeichnerattribut entfällt.

2.8.3. Elektronische Siegel

Vordergründig unterscheidet sich Anhang I Buchstabe h) der Richtlinie in der Wortwahl von Anhang I Buchstabe g) der Verordnung, welche die fortgeschrittene elektronische Signatur oder das fortgeschrittene elektronische Siegel des ausstellenden qualifizierten Vertrauensdiensteanbieters verlangt. Da das «Siegel» aber funktional auch eine Signatur ist, nur eben die einer nicht natürlichen Person, und da der Zertifizierungsdiensteanbieter der Richtlinie dem qualifizierten Vertrauensdiensteanbieter der Verordnung gemäß deren Artikel 51 entspricht, sind Alt- und Neuregelung hier dennoch kongruent.

2.8.4. Beschränkungen des Geltungsbereichs

Was in der Verordnung allerdings entfallen ist, sind die «gegebenenfalls» anzugebenden Beschränkungen des Geltungsbereichs des Zertifikats oder des abgedeckten Wertes von Transaktionen nach Anhang I Buchstaben i) und j) der Richtlinie. Solche risikobegrenzenden «Angstklauseln» sind nicht mehr möglich, vermutlich weil sie nach Einschätzung der Verordnungsgeber die Akzeptanz digitaler Signaturen als Grundlage eines modernen Binnenmarktes behindert hatten.

2.8.5. Pflichtinhalte des Zertifikats

Neu hinzugekommen sind an Pflichtinhalten des Zertifikats der Ort, an dem es kostenlos zur Verfügung steht, weiterhin der Ort derjenigen Dienste, die genutzt werden können, um den Gültigkeitsstatus des qualifizierten Zertifikats zu überprüfen und gegebenenfalls eine Angabe, dass sich die Signaturerstellungsdaten in einer qualifizierten elektronischen Signaturerstellungseinheit befinden.

2.9. Anbieter qualifizierter Zertifizierungsdienste

Der bisher in Artikel 2 Ziffer 11 der Richtlinie genannte «Anbieter qualifizierter Zertifizierungsdienste» als Person oder Stelle, die Zertifikate ausstellte, oder anderweitige Dienste im Zusammenhang mit elektronischen Signaturen bereitstellte, konnte sich qualifizieren, indem er qualifizierte Zertifikate nach Anhang I ausstellte und er konnte sich freiwillig akkreditieren lassen. Gemäß Artikel 51 der Verordnung entspricht so ein qualifizierter Zertifizierungsdiensteanbieter künftig einem qualifizierten Vertrauensdiensteanbieter. Da dieser aber nicht mehr in gleicher Weise «qualifiziert» wird wie bisher, sondern durch Konformitätsbewertungsberichte, die er nach Artikel 20 der Verordnung einer akkreditierten Konformitätsbewertungsstelle vorlegt, muss ein bisheriger qualifizierter Zertifizierungsdiensteanbieter erstmalig dieses Verfahren durchlaufen, um künftig «qualifizierter Vertrauensdiensteanbieter» im Sinne der Verordnung zu heißen. Ansonsten kann er seinen Status verlieren. Seine freiwillige Akkreditierung entfällt, akkreditiert werden nur noch die aufsichtführenden Konformitätsbewertungsstellen (Artikel 3 Ziffer 18 der Verordnung).

2.10. Validierungsdaten

Die bisherigen «Signaturprüfdaten» aus Artikel 2 Ziffer 7 der Richtlinie entsprechen trotz unterschiedlicher Bezeichnung funktional den neuen «Validierungsdaten» in Artikel 3 Ziffer 40 der Verordnung.

2.11. Pseudonyme

Sowohl Artikel 8 der Richtlinie als auch Artikel 5 der Verordnung verweisen für die Datenschutzregeln auf die Richtlinie 95/46/EG und erlauben die Nutzung von Pseudonymen.

2.12. Verkehrsfähigkeit im europäischen Binnenmarkt

Einen Schritt nach vorn macht die freie Verkehrsfähigkeit im europäischen Binnenmarkt beim Inkrafttreten der Verordnung nach deren Artikel 4. Produkte und Vertrauensdienste, die der Verordnung entsprechen, dürfen dann automatisch im Binnenmarkt frei verkehren. In der Richtlinie gab es eine umzusetzende Verpflichtung der Mitgliedstaaten, für den freien Verkehr zu sorgen; dies betraf dem Wortlaut nach nur Produkte für elektronische Signaturen; für sonstige Vertrauensdienste waren nach Artikel 4 der Richtlinie diskriminierungsfreie, aber von Land zu Land unterschiedliche, innerstaatliche Regelungen zulässig. Die Verkehrsfähigkeit eröffnet im privatrechtlichen Bereich den freien grenzüberschreitenden Verkehr, insbesondere auch die Erbringung von Dienstleistungen mit Identifikationssystemen und Postdiensten.

2.13. Rechtswirkung von Signaturen

Artikel 25 der Verordnung regelt hinsichtlich der Rechtswirkung elektronischer Signaturen, dass sie als Beweismittel in Gerichtsverfahren gelten dürfen, auch in der nicht qualifizierten Version, dass einer qualifizierten elektronischen Signatur die gleiche Rechtswirkung wie einer handschriftlichen Unterschrift zukommt und dass sie grenzüberschreitend anzuerkennen ist. Dies entspricht inhaltlich der Regelung in Artikel 5 der Richtlinie, nur eben mit dem Vorteil, dass keine innerstaatlichen Umsetzungsakte mehr erforderlich sind.

2.14. Regulatorische Annexmaterien

Im Übrigen enthält die Verordnung Regeln, die in der Richtlinie noch nicht vorkamen, die aber keine Gegensätze zum alten Recht beinhalten. Es geht dabei um regulatorische Annexmaterien. Nur natürlichen Personen wird eine sogenannte Signatur zugewiesen. Das damit korrespondierende Bedürfnis für juristische Personen wird durch ein sogenanntes «Siegel» befriedigt. Somit kann klar getrennt werden, ob eine persönliche Signatur des aktuellen gesetzlichen Vertreters einer juristischen Person vorliegt oder ein unpersönliches Authentifizierungszeichen der Körperschaft selbst. Artikel 12 ist inhaltlich neu und schreibt vor, dass die nach Artikel 9 notifizierten elektronischen Identifizierungssysteme zwischen den Mitgliedstaaten interoperabel sein müssen, insbesondere sollen für die Sicherheit der Systeme, für Verfahrensregelungen und Prüfverfahren einheitliche regulatorische Rahmen definiert werden, die auch die künftigen Entwicklungen jeweils mit einbeziehen. Neu ist auch die Verpflichtung zur gegenseitigen Amtshilfe der Aufsichtsstellen und der ENISA (Europäische Agentur für Netz- und Informationssicherheit), die in Artikel 18 und 19 sehr allgemein und umfassend formuliert ist, das als einfach zu erkennendes Zertifikat verwendbare EU-Vertrauenssiegel für qualifizierte Vertrauensdiensteanbieter nach Artikel 23 und das nunmehr in Artikel 3 Ziffer 35 legal definierte «elektronische Dokument», dessen Zulässigkeit als Beweismittel in Gerichtsverfahren Artikel 46 statuiert; es ist sehr weit definiert als jeder in elektronischer Form, insbesondere als Text-, Ton-, Bild- oder audiovisuelle Aufzeichnung gespeicherte Inhalt. Neu sind überdies im Umfeld einer Signatur einige ebenfalls notwendige elektronische Produkte.

2.14.1. Zeitstempel

Der Zeitstempel für die fälschungssichere Fixierung einer Unterschrift im zeitlichen Kontext wird geregelt in Artikel 3 Ziffer 34.

2.14.2. Einschreiben

Das elektronische Einschreiben als Verknüpfung von Signatur, Zeitstempel und einem elektronisch übertragenen elektronischen Dokument mit authentifiziertem Sender und Empfänger findet sich in Artikel 3 Ziffer 36.

2.14.3. Webseiten-Zertifikat

Ein sogenanntes Webseiten-Zertifikat als digitale und weitgehend fälschungssichere Verknüpfung einer Website mit einer ebenfalls elektronisch authentifizierten natürlichen oder juristischen Person wird definiert in Artikel 3 Ziffer 38 der eIDAS-Verordnung.

3. Internationale Anerkennung gegen Haftung der Systemverantwortlichen

3.1. Anerkennungspflicht von Identifizierungssystemen

Die Verordnung forciert die Entwicklung der formellen Voraussetzungen für eine gegenseitige Anerkennungspflicht von Identifizierungssystemen durch öffentliche Stellen. Gemäß Artikel 9 Absatz 1 der Verordnung können die Mitgliedstaaten die in ihrer Zuständigkeit befindlichen elektronischen Identifizierungssysteme der Kommission notifizieren, wenn diese gewisse Mindestvoraussetzungen erfüllen. Diese Notifikation ist sehr detailliert, sie umfasst auch die Beschreibung des Systems, seine Sicherheitsstufe, die aufsichtführende Stelle, die Haftungsregeln, die Benennung der Aussteller der Zertifikate sowie der haftenden Beteiligten. Die Kommission veröffentlicht im Amtsblatt eine Liste aller notifizierten Identifizierungssysteme. Ein Jahr später müssen öffentliche Stellen eines Mitgliedstaates, die für einen Dienst eine Authentifizierung verlangen, gemäß Artikel 6 der Verordnung alle Systeme aus der Liste wie innerstaatliche Systeme anerkennen; wenn das Sicherheitsniveau «niedrig» ist, müssen sie nicht, können sie aber anerkennen.

Die Verordnung regelt die Interoperabilität der elektronischen Identifizierung in einem gesonderten Abschnitt, denn diese Materie hat zwar auch mit den Signaturen etwas zu tun (Identifizierung als Voraussetzung für qualifizierte elektronische Signaturen), ist aber technisch und logisch ein eigenständiger Regelungsbereich. Die Regulierung der internationalen Identifikation und Authentifizierung unter Abwesenden mithilfe von e-IDs und mobile-IDs als eigenständige Regelungsmaterie, also nicht nur als Voraussetzung für Signaturen, ist folglich ebenfalls eine Neuerung der Verordnung im Verhältnis zur aufgehobenen Richtlinie.

3.2. Haftungsregeln

Fühlbare Unterschiede zwischen Richtlinie und Verordnung betreffen die Haftungsregeln bei grenzüberschreitenden Transaktionen unter Nutzung notifizierter elektronischer Zertifizierungs- und Authentifizierungssysteme. Zusätzlich zu den für eine vorsätzliche oder fahrlässige Schädigung nach innerstaatlichem Recht ohnehin haftenden Subjekten haften nämlich nach Artikel 11 der Verordnung der notifizierende Mitgliedstaat, der das elektronische Identifizierungsmittel ausstellende Beteiligte sowie der das Authentifizierungsverfahren durchführende Beteiligte für Schäden, die durch die Verletzung von Pflichten aus der Verordnung bei grenzüberschreitenden Transaktionen entstehen. Sollte also die Missbrauchsvermeidung nicht greifen, ein Hard- oder Softwarefehler ein Ergebnis verfälschen, ein Zertifikat unwirksam sein, eine Verschlüsselung nicht funktionieren und dadurch adäquat kausal ein Schaden entstehen, dann wäre das Vertrauen des Gegenübers auf das

System dennoch berechtigt, denn alle Beteiligten bis hinauf zum notifizierenden Mitgliedstaat haften ihm für einen solchen Fehler nun unmittelbar, gesamtschuldnerisch und unbegrenzt nach Unionsrecht. Er kann also gleichermaßen der Technik, der Aufsicht oder einfach den Haftpflichtversicherungen der Verfahrensbeteiligten vertrauen; auf diese Weise wirbt die Verordnung sehr deutlich für eine feste Verankerung der elektronischen Signatur im europäischen Binnenmarkt. – Demgegenüber enthielt Artikel 6 der Richtlinie nur ein System von Mindestregelungen hinsichtlich der Haftung von Zertifizierungsdiensteanbietern, verwies ausdrücklich auf einen möglichen Entlastungsbeweis, statuierte keine Staatshaftung und ließ sowohl gegenständliche Beschränkungen der Haftung für Zertifikate als auch Wertgrenzen für diese Haftung zu. Offenbar erschien diese Haftungsregelung für das Vertrauen in einen offenen Binnenmarkt mit elektronischen Signaturen dem Verordnungsgeber inzwischen unzureichend oder die Lobby der künftigen Zertifizierer hat es sich anders überlegt. Gleichzeitig ist auch damit zu rechnen, dass alleine die Frage der versicherbaren Risiken angesichts dieser strengen und mehrstufigen Haftungsregeln dafür sorgen wird, dass die technisch vorgesehene «eingebaute» Missbrauchsresistenz der künftigen Signatursysteme sehr hoch sein wird.

4. Zusammenfassung und Ergebnisse

Im Großen und Ganzen eröffnet die Verordnung (EU) Nr. 910/2014 im Vergleich zur Vorläufer-Richtlinie 1999/93/EG hinsichtlich der Signaturen lediglich weitere Möglichkeiten, sie stellt aber keine neuen Verbote oder Beschränkungen auf.

4.1. Was vergleichbar geregelt bleibt

Vergleichbar bleiben die technischen Voraussetzungen der elektronischen Signatur, die Begriffskaskaden der Legaldefinitionen, die Systemoffenheit, der Zertifizierungsdiensteanbieter, der nur zum Vertrauensdiensteanbieter umbenannt – und auch in Artikel 51 der Verordnung umqualifiziert wurde. Das Stufenverhältnis von einfacher Signatur, fortgeschrittener und qualifizierter fortgeschrittener Signatur bleibt erhalten, weiterhin die Pseudonymerlaubnis, und sogar – siehe Artikel 50 der Verordnung – Bezugnahmen auf die alte Richtlinie werden legal umgedeutet in Bezugnahmen auf die neue Verordnung. Für die exakte Umdeutung solcher Bezugnahmen bei Binnenzitaten bestimmter Einzelartikel der alten Richtlinie empfiehlt sich eine Entsprechungstabelle. Signaturkarten oder -server können weiter verwendet werden, ebenso Lesegeräte und Software. Die gesondert geregelten Notifizierungen sind (lediglich) erforderlich, um EU-weite Anerkennung zu sichern; die Diensteanbieter können weitermachen, alte Signaturen und Zertifikate bleiben gültig und müssen nicht etwa wiederholt werden.

4.2. Ausnahmen: Notifizierung und Haftung

Ausnahmen hiervon sind die **Notifizierung** (Artikel 7, 9) von interoperablen Identifizierungssystemen und die Rechtswirkung der entsprechenden EU-Liste im Amtsblatt nach Artikel 9 Absatz 2 der Verordnung. Um das erhöhte Vertrauen zu rechtfertigen, werden in Artikel 11 insbesondere die **Haftungstatbestände** und die **Haftungssubjekte** im Vergleich zur bisherigen Rechtslage ausgeweitet.

4.3. Neuerungen

Neu ist hierbei, dass «Die Mitgliedstaaten tragen dafür Sorge...» entfällt, denn es sind keine Umsetzungsrechtsakte der Mitgliedstaaten mehr nötig, um die Haftung der Aussteller von Identifizierungsmitteln und der Durchführer von Authentifizierungsverfahren herbeizuführen, sowie die neu hinzugekommene Haftung der notifizierenden Mitgliedstaaten zu begründen. Damit entfällt auch die – in Artikel 5 der Richtlinie etwas systemwidrig angesiedelte – Verpflichtung, fortgeschrittene qualifizierte Signaturen Unterschriften als Beweismittel innerstaatlich gleichzustellen. Neu sind die Rechtswirkungen der Notifizierung in Form der Aner-

kennungspflicht im EU-Ausland einerseits und der grenzüberschreitenden Haftung andererseits. Ebenso neu ist die Publikation der Liste der notifizierten Identifikationssysteme im Amtsblatt der EU. Neu sind zudem die im Vergleich zur Richtlinie inzwischen hinzugekommenen regulatorischen Annexmaterien, nämlich das «Siegel» für juristische Personen, das von der Signatur ihres gesetzlichen Vertreters zu unterscheiden ist, das Interoperabilitätserfordernis (Artikel 12), die Einbeziehung der Organisation ENISA (Artikel 19), das EU-Vertrauenssiegel (Artikel 23), das nunmehr legal definierte «elektronische Dokument» (Artikel 46) sowie die abgeleiteten Produkte Zeitstempel, Einschreiben und Webseiten-Zertifikat. Dieser Block der Vertrauensdienste wird von der EU vollständig reguliert, während für die davon getrennt behandelten Identifizierungssysteme nur die Voraussetzungen für Interoperabilität und Anerkennungspflicht geregelt werden.

Rechtspolitisch ist als Neuerung hervorzuheben, dass die eIDAS-Verordnung nur die Spitze eines Eisbergs ist, denn ihre Entstehung war und ist flankiert von gezielt geförderten Pilotprojekten und Initiativen zur Definition einheitlicher Spezifikationen und zur konkreten Erprobung grenzüberschreitender Techniken, in welche öffentliche und private Institutionen verantwortlich eingebunden sind. In Gremien von STORK 2.0, e-SENS, opensignature.org etc. finden sich viele politisch und wirtschaftlich interessierte Teilnehmer, deren Beteiligung gewährleisten soll, dass sich die Verordnung und ihre nachgelagerten Spezifikationen in die technische und wirtschaftliche Realität einfügen. Für technische Spezifikationen, Normen und Verfahren verweist die Verordnung auf Durchführungsrechtsakte der Kommission; insofern sind also Umsetzungsakte erforderlich; diese hat aber – abweichend vom Ansatz der Richtlinie – nunmehr die EU an sich gezogen.

Abschlussthese: Die Verordnung geht mit der strengen grenzüberschreitenden Haftung und der damit korrelierenden Pflicht zum gegenseitigen Vertrauen einen klaren Schritt in Richtung eines europaweiten, aber dezentralen Netzwerks von Vertrauensdiensten, ohne hierbei in die Richtung eines zentralistischen oder gar monopolistischen regulatorischen Molochs zu geraten.