Elektronischer Rechtsverkehr

Wegweiser zu Behörden- und Anwaltspostfächern, DE-Mail, ersetzendem Scannen, Cloud- und IT-Sicherheit, Beweisrecht und Langzeitarchivierung

Bearbeitet von
Dr. Thomas A. Degen, Ulrich Emmert

1. Auflage 2016. Buch. XXI, 140 S. Kartoniert
ISBN 978 3 406 65844 0
Format (B x L): 16,0 x 24,0 cm
Gewicht: 343 g

Für verschiedene Branchen müssen wegen der Besonderheiten der Dokumente unterschiedliche Prozessabläufe zum Scannen und damit auch unterschiedliche Prüfkriterien zur Prüfung dieser Geschäftsprozesse erarbeitet werden. 334

Eine Zertifizierung nach TR-RESISCAN nach den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik umfasst immer auch eine komplette Prüfung des Verfahrens nach **DIN ISO/IEC 27001** (IT-Sicherheitsverfahren-Informationssicherheits-Managementsysteme-Anforderungen) mit den Zusatzanforderungen durch den IT-Grundschutz. Die Prüfkriterien für ein solches Audit hat das BSI in Ergänzung zur TR-RESISCAN als Anlage P veröffentlicht[17]. Dabei wird nur das Verfahren zertifiziert, eine Konformitätsprüfung für Hardware oder Software wird hier nicht angeboten. Die Service-GmbH des Verbandes für Organisations- und Informationssysteme bietet in Absprache mit dem BSI weitere Zertifizierungen auf Basis der TR-RESISCAN an. Zum einen eine TR-RESISCAN-ready-Zertifizierung, die die Basisanforderungen der TR-RESISCAN umfasst, aber nicht die vollständige Erfüllung der Anforderungen des IT-Grundschutzes verlangt, zum anderen die Zertifizierung von Hard- oder Softwarekomponenten als geeignet für Verfahren nach TR-RESISCAN[18]. 335

III. Revisionssichere Langzeitarchivierung

1. Aufbewahrungspflichten

Alleine nach Bundesrecht gibt es hunderte verschiedener Aufbewahrungspflichten, die von kurzen Fristen von einigen Monaten bis zu 110 Jahre für Geburtseinträge nach dem Personenstandsgesetz reichen. Die **praktisch wichtigsten Aufbewahrungspflichten sind in § 257 HGB und § 147 AO geregelt.** Danach ist jegliche textbasierte geschäftliche Kommunikation, egal ob papiergebunden oder elektronisch, archivierungspflichtig. Die Regelung bezieht sich auch auf E-Mail-Kommunikation sowie bei entsprechender Einbeziehung in geschäftliche Prozesse auch auf SMS- oder Messenger-Kommunikation. Beispiele dafür sind die Nutzung von SMS zur Authentifizierung eines Nutzers beim Homebanking per SMS-TAN-Verfahren oder Support per Messenger. 336

Um ihrer Nachweisfunktion zu genügen, müssen die aufzubewahrenden Unterlagen in unveränderbarer revisionssicherer Form vorliegen. Im Handelsgesetzbuch ist ebenso wie in der Abgabenordnung nicht ausdrücklich der Begriff der Revisionssicherheit erwähnt, die darin beschriebenen Anforderungen sind jedoch deckungsgleich. In § 239 Abs. 3 HGB heißt es: *„(3) Eine Eintragung oder eine Aufzeichnung darf nicht in einer Weise verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. Auch solche Veränderungen dürfen nicht vorgenommen werden, deren Beschaffenheit es ungewiss lässt, ob sie ursprünglich oder erst später gemacht worden sind.“* Nach § 239 Abs. 4 HGB ist dies entsprechend auf elektronische Aufzeichnungen anzuwenden. Dies gilt nach § 146 Abs. 4 und 5 der Abgabenordnung in gleicher Weise für steuerrechtlich relevante Buchungen und Aufzeichnungen. 337

Um prüfen zu können, ob eine Veränderung auch später durchgeführt worden sein kann, ist es zwingend, technisch die Nachdatierung oder Fälschung von Aufzeichnungen ausschließen zu können bzw. sicherzustellen, dass jeder Versuch der Nachdatierung oder Fälschung nicht unbemerkt bleiben, sondern durch Kontrolle und Protokollierung entdeckt werden kann. 338

[17] www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03138/TR-03138-Anlage-P_V1_1.pdf?__blob=publicationFile&v=1.

[18] www.voi-cert.de/index.php?option=com_content&view=article&id=4276&Itemid=847.

339 **Revisionssicherheit** ist daher nur dann gewährleistet, wenn die Daten nicht unbemerkt verändert werden können oder jede Änderung der Daten protokolliert wird sofern eine Umgehung der Protokollierung technisch nicht möglich ist. Dazu gehört eine vollständige Beschreibung der technischen Verfahrensabläufe, eine so genannte **Verfahrensdokumentation.** Der Begriff der revisionssicheren Archivierung wurde bereits vor über 20 Jahren vom VOI e. V., Verband für Organisations- und Informationssysteme, und dessen Gründer Dr. Ulrich Kampffmeyer, geprägt[19].

340 Der VOI hat dazu **10 Merksätze zur revisionssicheren Archivierung** veröffentlicht[20]:

1. Jedes Dokument muss nach Maßgabe der rechtlichen und organisationsinternen Anforderungen ordnungsgemäß aufbewahrt werden.
2. Die Archivierung hat vollständig zu erfolgen – kein Dokument darf auf dem Weg ins Archiv oder im Archiv selbst verloren gehen.
3. Jedes Dokument ist zum organisatorisch frühestmöglichen Zeitpunkt zu archivieren.
4. Jedes Dokument muss mit seinem Original übereinstimmen und unveränderbar archiviert werden.
5. Jedes Dokument darf nur von entsprechend berechtigten Benutzern eingesehen werden.
6. Jedes Dokument muss in angemessener Zeit wiedergefunden und reproduziert werden können.
7. Jedes Dokument darf frühestens nach Ablauf seiner Aufbewahrungsfrist vernichtet, dh aus dem Archiv gelöscht werden.
8. Jede ändernde Aktion im elektronischen Archivsystem muss für Berechtigte nachvollziehbar protokolliert werden.
9. Das gesamte organisatorische und technische Verfahren der Archivierung kann von einem sachverständigen Dritten jederzeit geprüft werden.
10. Bei allen Migrationen und Änderungen am Archivsystem muss die Einhaltung aller zuvor aufgeführten Grundsätze sichergestellt sein.

2. Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme und Grundsätze zum Datenzugriff und zur Prüfbarkeit originär digitaler Unterlagen

341 Die Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme und Grundsätze zum Datenzugriff und zur Prüfbarkeit originär digitaler Unterlagen sind als Schreiben des Bundesfinanzministeriums, als Verwaltungsanweisung zu qualifizieren. Diese haben jedoch erhebliche Auswirkungen auf die Steuerbürger und Unternehmen, da die Finanzämter dieser Verwaltungsanweisung bei der Prüfung der Steuerunterlagen unterworfen sind.

342 Die GoBD lösen zwei Verwaltungsanweisungen ab: die Grundsätze ordnungsgemäßer Buchführungssysteme (GOBs) aus dem Jahr 1995 und die Grundsätze der Prüfung digitaler Unterlagen (GDPdU) aus dem Jahr 2001, die seit 1.1.2002 in Kraft sind.

343 Seit der Einführung der GDPdU sind auch digitale Unterlagen aufzubewahren, ein Ausdruck der Unterlagen bewahrt nicht vor der Prüfung der digitalen Inhalte. Die Inhalte müssen im Nachhinein auf unveränderte Speicherung geprüft werden können, um Manipulationen ausschließen zu können.

---

[19] *Kampffmeyer/Rogalla,* Grundsätze der elektronischen Archivierung, Code of Practice Band 1, VOI Verband Organisations- und Informationssysteme e. V., 2. Aufl. 1997.

[20] VOI e. V., www.ulshoefer.de/voi_merksaetze_der_archivierung.pdf.

Dazu ist es erforderlich, dass die Daten in einer Weise gespeichert werden, die jede unbemerkbare Manipulation der Daten ausschließt. Die GoBD sind grundsätzlich technikoffen ausgestaltet, das heißt, die Art und Weise der technischen Gestaltung sind dem Unternehmen überlassen. **344**

Die GoBD enthalten Regelungen zu 4 Bereichen, die helfen sollen, die **Compliance-Vorgaben** in Bezug auf die Unveränderbarkeit von Daten nach Handelsgesetzbuch und Abgabenordnung zu erfüllen: **345**

1. Datenintegrität
2. Kontrolle und Aufzeichnungen von Beweisdaten
3. Verfahrensdokumentation
4. Erhalt der Beweiseignung bei Migration

Zur Sicherstellung der Datenintegrität sind verschiedene Möglichkeiten vorhanden: **346**

In der GoBD Rn. 59 heißt es dazu: „Veränderungen und Löschungen von und an elektronischen Buchungen oder Aufzeichnungen (vgl. Rn. → 3 bis 5) müssen daher so protokolliert werden, dass die Voraussetzungen des § 146 Abs. 4 AO bzw. § 239 Abs. 3 HGB erfüllt sind (siehe auch → Rn. 337). Für elektronische Dokumente und andere elektronische Unterlagen, die gem. § 147 AO aufbewahrungspflichtig und nicht Buchungen oder Aufzeichnungen sind, gilt dies sinngemäß."

Protokollierungen sind nur dann ausreichend vor Änderungen geschützt, wenn die nachträgliche Änderung der Protokollierung nicht auf einfache Weise möglich ist. Um dies zu verhindern, muss die Unmöglichkeit der unbemerkten Protokolländerung durch die Verfahrensdokumentation nachgewiesen werden. Es ist möglich, die Integrität der Daten durch qualifizierte Signaturverfahren zu sichern, aber nicht zwingend vorgeschrieben. Durch lückenlose und indexierte Protokollierung oder sofortige sichere Speicherung auf Datenträgern, die keine Änderung oder Löschung bis zum Ablauf der Speicherdauer mehr erlauben, ist eine Beweissicherung ebenso möglich. **347**

Die GoBD legt wesentlich mehr Wert auf die vollständige und nachvollziehbare Verfahrensdokumentation als die Vorgängerregelungen GDPdU und GOBS[21]. Unternehmen sollten darauf achten, dass spätestens bei der Prüfung der Steuererklärung 2015 alle notwendigen Voraussetzungen zur ordnungsgemäßen Prüfung der Buchführungssysteme und der aufbewahrungspflichtigen Unterlagen gegeben ist. **348**

IV. Vertrauensdienste nach der EIDAS-Verordnung

Die EIDAS-Verordnung regelt elektronische Identifikationsdienste sowie Vertrauensdienste. **349**

Die Vertrauensdienste umfassen Änderungen bei der elektronischen Signatur und die Einführung eines elektronischen Siegels sowie weitere neue Vertrauensdienste. **350**

1. eID-Verfahren

Elektronische Identifikationsdienste nach der EIDAS-Verordnung ermöglichen ab 18.9.2018 die europaweite Anerkennung dieser Dienste. Die Sicherheit der von den Mitgliedstaaten eingesetzten Verfahren muss dabei dem Durchführungsbeschluss der Kommission vom 8.9.2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen **351**

[21] Die GoBD in der Praxis, Version 1.9, 13.4.2016, Herausgeber: Peters, Schönberger & Partner mbB, www.psp.eu/media/allgemein/GoBD-Leitfaden_Version_1_9_FINAL.pdf.

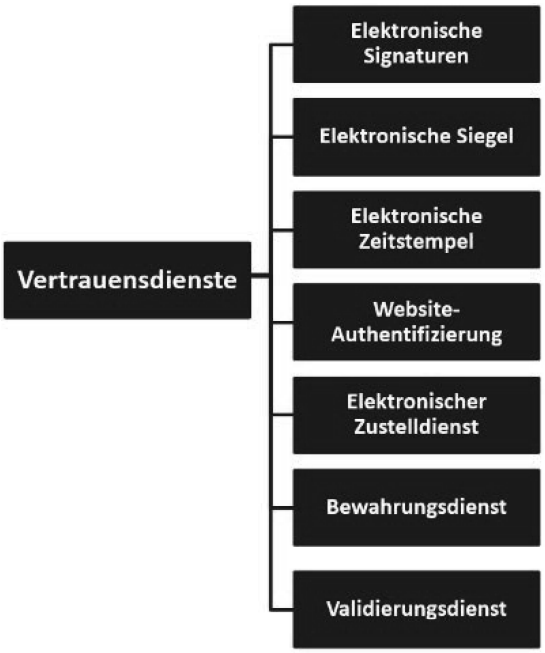
Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt[22] entsprechen.

352 Es sind hier drei Sicherheitsstufen vorgesehen, die für unterschiedliche Zwecke mit unterschiedlichem Schutzbedarf eingesetzt werden können: niedrig, substantiell und hoch.

353 Zur Identifizierung natürlicher Personen mit der Stufe „substanziell" sollen 2 unabhängige Identifizierungsverfahren eingesetzt werden, für die Stufe „hoch" unter Verwendung biometrischer Merkmale oder Fotografien[23] oder die zur Identifikation eingesetzten Mittel haben bisher in den Mitgliedstaaten entsprechende Voraussetzungen erfüllt. Für juristische Personen müssen zusätzlich mit Hilfe von verlässlichen Quelle Nachweise für die Repräsentation vorgelegt werden.

354 Es wird nach Punkt 2.4.3 bei der Absicherung der eID-Dienste ein Informationssicherheitsmanagementsystem vorgeschrieben und nach 2.4.4 die Aufbewahrung der Daten nach allgemeinen Regelungen der Aufbewahrungspflichten und des Datenschutzes verlangt.

2. Vertrauensdienste



355 Diese Vertrauensdienste können von Unternehmen ohne besondere Voraussetzungen erbracht werden, soweit sie nicht zur Bewahrung oder Validierung von qualifiziert signierten Dokumenten erbracht werden sollen und die Beweissicherheit erhalten bleiben soll.

[22] ABl. L 235 vom 9.9.2015, S. 7–20, http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015R1502&qid=1463677849104&from=DE.

[23] Anhang 2.1 zum Beschluss 2015/1502 der Kommission.

Wenn die Vertrauensdiensteanbieter jedoch die besonderen Anforderungen der EIDAS-Verordnung für qualifizierte Vertrauensdiensteanbieter erfüllen, hat dies mehrere Vorteile: **356**

- Der qualifizierte Vertrauensdiensteanbieter wird in die Trusted List der EU Kommission eingetragen.
- Die Erbringung qualifizierter Vertrauensdienste wird ab 18.9.2018 durch alle öffentlichen Stellen der Mitgliedstaaten auch dann anerkannt, wenn der Vertrauensdiensteanbieter aus einem anderen Mitgliedsstaat der europäischen Union stammt.
  Am 28.8.2014 wurde im Amtsblatt der EU die Signaturverordnung veröffentlicht. Die neue europaweit geltende EIDAS-Verordnung sieht auch die Möglichkeit von serverbasierten qualifizierten Signaturen und Signaturleistungen für Dritte in deren Namen vor[24]. Ab 1.7.2016 werden die Implementierungsvorschriften zur EIDAS-Verordnung in Kraft gesetzt, die zumeist auf der verbindlichen Festschreibung von Normen des ETSI[25] oder des CEN[26] beruhen[27]. Die Vorschriften der EIDAS-Verordnung werden dann die Vorschriften des deutschen Signaturgesetzes im Rahmen eines Anwendungsvorrangs überlagern, dh bei gleichem Regelungsgehalt gilt die EIDAS-Verordnung vor dem Signaturgesetz, von der Verordnung nicht tangierte Bereich bleiben aber durch das deutsche Signaturgesetz geregelt[28]. Das Signaturgesetz und die zugehörige Signaturverordnung sollen erst im Laufe des Jahres 2016 durch ein Vertrauensdienstegesetz abgelöst werden, das außer der qualifizierten elektronischen Signatur auch das qualifizierte elektronische Siegel nach der EIDAS-Verordnung in dem Umfang neu regelt, der den Mitgliedsstaaten durch die direkt geltende EU-Verordnung noch verblieben ist[29].

a) Elektronische Signaturen

Zur Sicherstellung der Integrität ist es möglich, fortgeschrittene oder qualifizierte Signaturverfahren einzusetzen. Eine qualifizierte Signatur nach dem Signaturgesetz ist derzeit noch mit dem Einsatz einer Chipkarte und einem Chipkartenleser Klasse 3 verbunden. **357**

Seit der Änderung des Signaturgesetzes 2001 und dem Schreiben des Bundesfinanzministeriums vom 29.1.2004 wurde die Massensignatur nach deutschem Signaturrecht ermöglicht. Vor 2001 war nach dem Signaturgesetz von 1997 eine Einzelprüfung jeder Signatur mit Sichtkontrolle erforderlich. Durch die Änderung des § 17 SigG im Zuge der Anpassung an die EU-Signaturrichtlinie von 1998 heißt es nunmehr in § 17 Abs. 2 S. 4: *„Die Signaturschlüssel-Inhaber sollen solche Signaturanwendungskomponenten einsetzen oder andere geeignete Maßnahmen zur Sicherheit qualifizierter elektronischer Signaturen treffen."* Damit ist auch die automatisierte Signatur für andere unter Verwendung **358**

[24] *Dennis Kügler,* BSI, Remote Signatures und mögliche Angriffe, www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/SmartCard_Workshop/Workshop_2015_Kuegler.pdf?__blob=publicationFile.

[25] ETSI – das Europäische Institut für Telekommunikationsnormen (englisch European Telecommunications Standards Institute),www.etsi.org/.

[26] CEN – das Europäische Komitee für Normung (französisch Comité Européen de Normalisation; englisch European Committee for Standardization), www.cen.eu.

[27] Vgl. auch http://toolbox.bearingpoint.com/ecomaXL/files/eiDAS_Paper.pdf.

[28] *Rossnagel* MMR 2015, 359; *Paul C. Johannes,* Die Novellierung des Signaturgesetzes, www.teletrust.de/fileadmin/docs/veranstaltungen/Signaturtag_2015/13–150917_TeleTrusT_Informationstag_Elektronische-Signatur_Johannes.pdf.

[29] *Sabine Maass,* Leiterin des Referats VI A 3 im BMWi, Stand der Anpassung des nationalen Rechts an die eIDAS-Verordnung, www.dihk.de/branchen/…elektronisches…/vortraege/vortrag-maas.pdf.

einer zuvor ausgestellten Vollmacht möglich. Eine echte Serversignatur des Kunden im Auftrag des Kunden, wie dies schon nach der bisherigen EU-Verordnung die Mitgliedstaaten Österreich und Italien ermöglicht haben, war damit aber noch nicht möglich.

359 Das Bundesfinanzministerium hat im Schreiben vom 29.1.2004 für Zwecke der Rechnungssignatur erklärt[30]: *„Der Rechnungsaussteller kann die Rechnungen auch in einem automatisierten Massenverfahren signieren."*

360 Bis 2005 war auch der Einsatz von fortgeschrittenen Signaturen nur mit Zertifikaten möglich. Durch die Streichung dieser Anforderung in § 2 Nr. 9 des Gesetzes wurde auch der Einsatz von biometrischen Verfahren für fortgeschrittene Signaturen möglich. Beispielsweise können Unterschriften auf Tablets bei Ermittlung von Schreibgeschwindigkeit, Druck und Schriftbild als biometrisch erzeugte fortgeschrittene Signaturen anerkannt werden.

361 Die neue Verordnung sieht keine Anforderungen mehr an Signaturanwendungskomponenten vor, wie dies bisher durch die §§ 15 und 17 des Signaturgesetzes der Fall war. Die neue Verordnung macht auch Lösungen in Deutschland möglich, wie sie bisher schon zB in Österreich mit der Handy-Signatur auf Anforderung nach Authentifizierung in einem Webformular möglich war.

362 Anbieter können zukünftig Nutzern anbieten, deren Signaturen in einem Signaturspeicher zu verwalten und auf Anforderung des Nutzers, die dieser über SMS oder Webformular dem Anbieter übermittelt, abrufen. Damit wird die Bestätigung von Dokumenten mit qualifizierten elektronischen Signaturen erheblich vereinfacht. Gerade für Zwecke, in denen es nur um die Bestätigung der Echtheit und Unveränderheit von Dokumenten geht, ist die Identifizierung des Signaturschlüsselinhabers von untergeordneter Bedeutung.

363 Bisher waren einige Beschränkungen des Signaturgesetzes für die beschränkte Verbreitung von qualifizierten elektronischen Signaturen in der Praxis verantwortlich:

1) Teure Hardware durch Notwendigkeit des Einsatzes von Chipkarte und Kartenleser sowie kompliziertes Verfahren zur Beantragung von Zertifikaten.
2) Keine zentrale und kostenneutrale Verbreitung von Lesegeräten und Zertifikaten.
3) Keine professionelle Verwaltung der Zertifikate im Kundenauftrag Praxisbedeutung.
4) Keine Organisationssignatur, sondern nur qualifizierte Signaturen für natürliche Personen.

364 Die Abschaffung des komplizierten Beschaffungsverfahrens für Smartcards und Kartenleser Gruppe 3 zur Erstellung von qualifizierten Signaturen wird aller Voraussicht nach zu einem erheblichen Schub für die Verbreitung qualifizierter elektronischer Signaturen führen. Das zeigt die Verbreitung der qualifizierten elektronischen Signatur in EU-Mitgliedstaaten, die schon auf der Basis der bisherigen EU-Richtlinie die Möglichkeit von serverbasierten Signaturen ohne Einsatz von Chipkarten auf Clientseite geschaffen haben.

365 Zudem werden die Regelungen zu Elektronischen Identifizierungsdiensten wie zB die EID-Funktion des neuen Personalausweises deshalb zu einer breiteren Nutzung führen, da diese Funktion bereits mit jedem neuen Personalausweis ausgeliefert wird. Hier ist trotzdem noch ein Kartenleser notwendig, der die ID per Kontaktleser oder RFID-Leser auslesen kann.

b) Elektronisches Siegel

366 Die Funktion des elektronischen Siegels ermöglicht eine Organisationssignatur für Behörden und Unternehmen. Damit ist es in Verbindung mit dem oben geschilderten

[30] BMF Schreiben vom 29.1.2004 – IV B 7 – S 7280 – 19/04 BStBl. 2004 I 258.

§ 371b ZPO möglich, dass unabhängig von der Person des Ausstellenden ohne eine zusätzlich notwendige Vollmacht bzw. ein entsprechendes Attribut oder Attributzertifikat direkt für eine Behörde elektronisch signiert werden kann. Der einzige Unterschied zwischen den Begriffen qualifiziertes elektronisches Siegel und qualifizierter elektronischer Signatur ist die Verwendung für eine Behörde statt für eine natürliche Person.

Ein solches Siegel kann von der Behörde auch dafür genutzt werden, nach ausreichender Authentifizierung des Bürgers für den Bürger in Stellvertretung Erklärungen abzugeben[31]*. Bisher war dies kaum möglich, derartige Bürgerdienste anzubieten, da Zertifikate nur für natürliche Personen ausgestellt werden konnten.*

c) Bewahrungsdienste

367 Für die Sicherung der Unveränderheit von Dokumenten die qualifizierte Signatur geeignet, aber keineswegs erforderlich. Die Unveränderheit von Dokumenten kann schon mit der Verknüpfung der digitalen Fingerabdrücke und einem zugehörigen Tageszeitstempel nach der TR-ESOR (TR 3125) des Bundesamts für Sicherheit in der Informationstechnik nachgewiesen werden.

368 Zukünftig kann die Beweissicherheit auch durch Anbieter von qualifizierten Bewahrungsdiensten nach Art. 34 der EIDAS-Verordnung erbracht werden. Dazu muss nach Art. 34 Abs. 1 der EIDAS-Verordnung die Vertrauenswürdigkeit qualifizierter elektronischer Signaturen erhalten bleiben. Zur Aufrechterhaltung der Sicherheit qualifizierter elektronischer Signaturen ist es nicht ausreichend, eine Protokollierung und Schreibschutzmaßnahmen vorzusehen, sondern es ist eine Aufrechterhaltung des kryptographischen Schutzes für die Dokumente erforderlich. Die Technik, die die technische Richtlinie TR-ESOR zur Langzeitsicherung des Beweiswertes kryptographisch gesicherter Dokumente einsetzt, entspricht wie unter → Rn. 317 gezeigt mit Hasherzeugung und qualifiziert signiertem Zeitstempel der Technik, die bei der Erstellung qualifizierter elektronischer Signaturen selbst eingesetzt wird. Daher ist damit zu rechnen, dass die Kommission ihre Verordnungsermächtigung in Art. 34 Abs. 2 dazu nutzen wird, um Vorgaben auf Basis von ETSI- und CEN-Normen zu machen, die den Regelungen des LTANS-Standards entsprechen, wie er in den RFC 4998 bzw. 6293 und der Technischen Richtlinie TR-ESOR geregelt ist.

369 Damit ist der Einführungszeitpunkt der Durchführungsrechtsakte zur EIDAS-Verordnung am 1.7.2016 jedoch nicht berührt, weil es sich hier um eine Kann-Bestimmung handelt und mit der Veröffentlichung des Beschlusses 2016/650[32] der letzte zwingend erforderliche Durchführungsbeschluss der Kommission erlassen worden ist.

d) Zeitstempeldienste

370 Die Erbringung von Zeitstempeldiensten war bisher in § 9 SigG geregelt. Die Technik entspricht der für fortgeschrittene bzw. qualifizierte Signaturen.

371 Der Unterschied ist jedoch, dass eigene digitale Signaturen einen Beweiswert haben, eigene Zeitstempel jedoch nicht, da nur bei Verwendung eines externen Zeitstempels das Vertrauen aller Vertragsparteien zur korrekten Ermittlung der jeweiligen Uhrzeit vorausgesetzt werden kann. Das Verstellen einer Uhrzeit vor dem Einsatz einer quali-

[31] *Theresa Vogt* IWP 2016, 61 ff.

[32] Durchführungsbeschluss (EU) 2016/650 der EU-Kommission vom 25. April 2016 zur Festlegung von Normen für die Sicherheitsbewertung qualifizierter Signatur- und Siegelerstellungseinheiten gemäß Art. 30 Abs. 3 und Art. 39 Abs. 2 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt.

fizierten Signatur ist jedem Windows-User auf einfache Weise möglich. Daher sollten für Zwecke der Beweisführung ausschließlich Zeitstempels einer vertrauenswürdigen Zertifizierungsstelle eingesetzt werden.

372 Die Erbringung von Zeitstempeln ist in der EIDAS-Verordnung als eigener Vertrauensdienst geregelt. Auch Zeitstempel, die nicht den Status der qualifizierten Zeitstempel erreichen, sind als Beweismittel in Gerichtsverfahren zuzulassen.

373 Für qualifizierte Zeitstempeldienste sind 3 Voraussetzungen erforderlich:

aa) Er verknüpft Datum und Zeit so mit Daten, dass die Möglichkeit der unbemerkten Veränderung der Daten nach vernünftigem Ermessen ausgeschlossen ist.
Dies bedeutet zwar nicht, dass jeder Manipulationsversuch ausgeschlossen sein muss, aber dass auf jeden Fall jeder Versuch durch die technische Gestaltung des Verfahrens zwingend auffallen muss.

bb) Er beruht auf einer korrekten Zeitquelle, die mit der koordinierten Weltzeit verknüpft ist.
Bisher wurde vom BSI empfohlen, zur Ermittlung der Uhrzeit mindestens zwei verschiedene Zeitquellen zu nutzen, um zB die Beeinträchtigung des DCF77-Signals der Physikalisch-Technischen Bundesanstalt durch Störsender auszuschließen.

cc) Er wird mit einer fortgeschrittenen elektronischen Signatur unterzeichnet oder einem fortgeschrittenen elektronischen Siegel des qualifizierten Vertrauensdiensteanbieters versiegelt oder es wird ein gleichwertiges Verfahren verwendet.
Zur Erfüllung der Anforderungen an qualifizierte Zeitstempeldienste sind fortgeschrittene Signaturen oder Siegel eines qualifizierten Vertrauensdiensteanbieters erforderlich, deren Sicherheit sich nach dem Beschluss 650/2016 der EU-Kommission richtet.
Die Kommission kann für qualifizierte Zeitstempeldienste Anforderungen an die Verknüpfung der Zeitangabe mit Daten und die Ermittlung der Zeitquellen vorsehen, davon hat die Kommission bisher allerdings noch keinen Gebrauch gemacht. Es ist zu erwarten, dass die Kommission die bereits bestehenden Normen des ETSI als Durchführungsrechtsakte beschließen wird:

EN 319 421:	Anforderungen an Vertrauensdiensteanbieter, wenn diese einen (qualifizierten) Zeitstempeldienst anbieten
EN 319 422:	Formate und Prozeduren verbunden mit der Anfrage, Erstellung und Auslieferung von Zeitstempeln
EN 319 423:	Anforderungen an die Richtlinien für die Überwachung und Evaluierung von (qualifizierten) Vertrauensdiensteanbietern, die einen (qualifizierten) Zeitstempeldienst anbieten

Zeitstempel sind auch für die künftigen qualifizierten Bewahrungsdienste erforderlich bzw. bisher für beweiswerterhaltende Langzeitarchivierung nach TR-ESOR und TR-RESISCAN.

e) Validierungsdienste

374 Validierungsdienste können nach Art. 33 EIDAS-VO nur von qualifizierten Vertrauensdiensteanbietern erbracht werden. Diese müssen in der Lage sein, die Gültigkeit von fortgeschrittenen elektronischen Signaturen bzw. Siegeln qualifizierter Vertrauensdiensteanbieter zu überprüfen und automatisiert eine Bestätigung abzurufen. Dies entspricht den Diensten, die bisher nach der deutschen Signaturverordnung den Anbietern von Zertifizierungsdiensten selbst als verpflichtender Verzeichnisdienst auferlegt war[33].

[33] § 4 SigVO.