Tomasz Kusber, Steffen Schwalm, Ulrike Korte, Mario Engel

Langfristige Beweissicherheit und Vertrauenswürdigkeit digitaler Unterlagen

(qualifizierte) Bewahrungsdienste nach eIDAS, ETSI und TR-ESOR

Tomasz Kusber

arbeitet seit 2017 als wissenschaftliche Mitarbeiter beim Fraunhofer Institut für offene Kommunikationssysteme (FOKUS). Er ist ist (Co-)Autor der Technischen Richtlinie 03125 (TR-ESOR) des BSI sowie zahlreicher themenbezogener Publikationen.
E-Mail: thomas.kusber@bearingpoint.com

Steffen Schwalm

berät seit langen Jahren hochregulierte Industrien in der Beweissicherheit digitaler Aufzeichnungen. Er ist (Co-) Autor der Technischen Richtlinie 03125 (TR-ESOR) des BSI sowie zahlreichen Publikationen und an der internationalen Standards in diesem Thema.
E-Mail: Steffen.Schwalm@msg.group

Ulrike Korte

arbeitet seit 2004 beim Bundesamt für Sicherheit in der Informationstechnik. Sie ist Projektleiterin der Technischen Richtlinie 03125 (TR-ESOR) des BSI (sowie Co-)Autor zahlreicher wissenschaftlicher Publikationen und ist Mitglied internationaler Standardisierungsgruppen zu diesem Thema.
E-Mail: ulrike.korte@bsi.bund.de

Mario Engel

arbeitet beim Bundesamt für Sicherheit in der Informationstechnik. Er ist u.a. Projektmitarbeiter der Technischen Richtlinie 03125 (TR-ESOR) des BSI sowie (Co-)Autor zahlreicher Fachartikel und in der Standardisierung beteiligt
E-Mail: mario.engel@bsi.bund.de

Die Nutzung der Informationstechnologie zur Abbildung elektronischer Geschäftsprozesse ist in Wirtschaft und Verwaltung etabliert. Der Fokus liegt dabei zunehmend auf der Umsetzung vollständig digitaler Transaktionen. Beschleunigt wird diese Entwicklung durch gesetzliche Vorgaben wie z.B. die Pflicht zur Einführung der elektronischen Akte und dem Onlineangebot aller digitale abbildbaren Behördenleistungen für die öffentliche Verwaltung oder die Zahlungsverkehrsrichtlinie PSD2 in der Finanzwirtschaft. Gleichzeitig sind umfassende Dokumentations- und Nachweispflichten teilweise über Jahrzehnte einzuhalten. Die eIDAS-Verordnung schuf einen einheitlichen regulatorischen wie technischen Rahmen vertrauenswürdiger Digitalisierung in Europa. Mit den Bewahrungsdiensten wird die langfristige Nachweisfähigkeit elektronischer Transaktionen gewährleistet. Der Beitrag stellt basierend auf den regulatorischen Vorgaben den aktuellen Stand der Technik sowie konkrete Lösungen vor.

1 Einführung

Die Nutzung der Informationstechnologie zur Abbildung elektronischer Geschäftsprozesse ist Unternehmen, Behörden sowie im Gesundheitswesen etabliert. Der Fokus liegt dabei zunehmend auf der Umsetzung vollständig digitaler Transaktionen, Ende zu Ende, also vom Kunden zum Unter-nehmen/Behörde/Krankenkasse etc. und zurück. Beschleunigt wird diese Entwicklung durch gesetzliche Vorgaben wie z.B. die Pflicht zur Einführung

elektronischer Akten im Allgemeinen oder der Patientenakte im Besonderen, der Vorgabe zur Annahme digitaler Identitäten oder qualifizierter elektronischer Signaturen für öffentliche Institutionen bis hin zum elektronischen Rezept oder digitalen Impfpass.

In der Folge liegen geschäftsrelevante Aufzeichnungen ausschließlich elektronisch vor. Gleichzeitig sind gesetzliche Vorgaben bzgl. Zeitpunkt sowie Art und Weise der vollständigen Umsetzung, Dokumentation und Nachweis digitaler Transaktionen einzuhalten. Eine wesentliche Kernanforderung bildet hierbei der Aufbau und Etablierung vertrauenswürdiger digitaler Transaktionen und Aufzeichnungen. Dies erfordert zum einen die eindeutige Identifizierung der beteiligten natürlichen wie juristischen Personen oder auch Verfahren (Maschine-Maschine-Kommunikation) inklusive der eindeutigen Zuweisbarkeit und Nichtabstreitbarkeit von Transaktionen und Dokumenten, die Unveränderheit geschäftsrelevanter Aufzeichnungen, zum anderen deren Verfügbarkeit in der notwendigen Form, was auch die Verkehrsfähigkeit bedingt und die Wahrung der Vertraulichkeit gegenüber Nutzern und Betroffenen. Die Maßgaben sind bis zum Ablauf der geltenden Aufbewahrungsfristen gegenüber Prüfbehörden, Gerichten, Dritten entsprechend nachzuweisen. [Ko13], [KuSc16], [Ro07], [Fi06], [We18].

Digitale Daten sind aus sich selbst heraus jedoch weder wahrnehmbar und lesbar, noch liefern sie Hinweise für ihre Integrität, Authentizität oder Ordnungsmäßigkeit im elektronischen Rechts- und Geschäftsverkehr. Vor dem Hintergrund der erwähnten Dokumentations- und Nachweispflichten, die zum einen für Fristen zwischen zwei und 110 Jahren zu erfüllen sind, die teilweise erst Jahrzehnte nach dem Abschluss des zugrundeliegenden Geschäftsvorfalls beginnen, gilt es, organisatorische und technische Maßnahmen nach dem Stand der Technik zu treffen, um die Vertrauenswürdigkeit von Prozessen und Aufzeichnungen nicht nur langfristig zu gewährleisten, sondern auch nachweisen zu können. Eine langfristig vertrauenswürdige Digitalisierung kann als elementare Grundlage nachhaltiger elektronischer Prozesse, Dienstleistungen und Aufzeichnungen bezeichnet werden.

Die Verwendung kryptographischer Sicherungsmittel wie mindestens fortgeschrittener elektronischer Signaturen, Siegel, Zeitstempel und Beweisdaten (Evidence Records) ermöglicht nach geltendem Recht nicht nur die Wahrung von Authentizität und Integrität von Transaktionen und Aufzeichnungen, sondern vor allem die Erhaltung des zur Nachweisführung notwendigen Beweiswerts direkt an den aufzubewahrenden Aufzeichnungen, ohne deren Verkehrsfähigkeit einzuschränken (Beweiswerterhaltung). Darüber hinaus ist es notwendig, die Interpretierbarkeit der Aufzeichnungen zu gewährleisten, sie also entsprechend dem Aufbewahrungszweck und –vorgaben verfügbar zu halten (Informationserhaltung) [Ko13] [Ro07], [KoKuSc18].

Die Umsetzung erfolgt in der Praxis auf Basis geltender Standards und Normen zum Records Management sowie zur beweissicheren Langzeitspeicherung resp. Bewahrung, die es ermöglichen, zum einen die organisatorische wie technischen Rahmenbedingungen zum Umgang mit geschäftsrelevanten Aufzeichnungen zu etablieren und zum anderen die zur Beweiswert- und Informationserhaltung notwendigen Information, gemeinsam mit den aufzubewahrenden Aufzeichnungen in selbst-tragenden Archivinformationspaketen (AIP) in einem digitalen Langzeitarchiv auf Basis ISO 15489, ISO 14721, DIN 31647 oder BSI TR-03125 TR-ESOR. Als Stand der Technik gelten Standards und Normen anerkannter wie unabhängiger Standardisierungsorganisationen wie z.B. DIN, ISO, ETSI/CEN oder BSI.

Der vorliegende Aufsatz beschreibt auf Basis der wesentlichen regulatorischen Rahmenbedingungen (Kap. 2.1) sowie fachlich-technischen Anforderungen (Kap. 2.2) einer vertrauenswürdigen Digitalisierung den aktuellen Stand der relevanten Standards und Normen (Kap. 3). Der Fokus liegt dabei, im Sinne der Nachweisfähigkeit, auf den Maßgaben zur langfristigen wie beweissicheren Aufbewahrung geschäftsrelevanter Aufzeichnungen. Darüber hinaus wird ein Ausblick auf aktuelle Anwendungsfälle sowie künftige Weiterentwicklungen im Kontext disruptiver Technologien gegeben (Kap. 4).

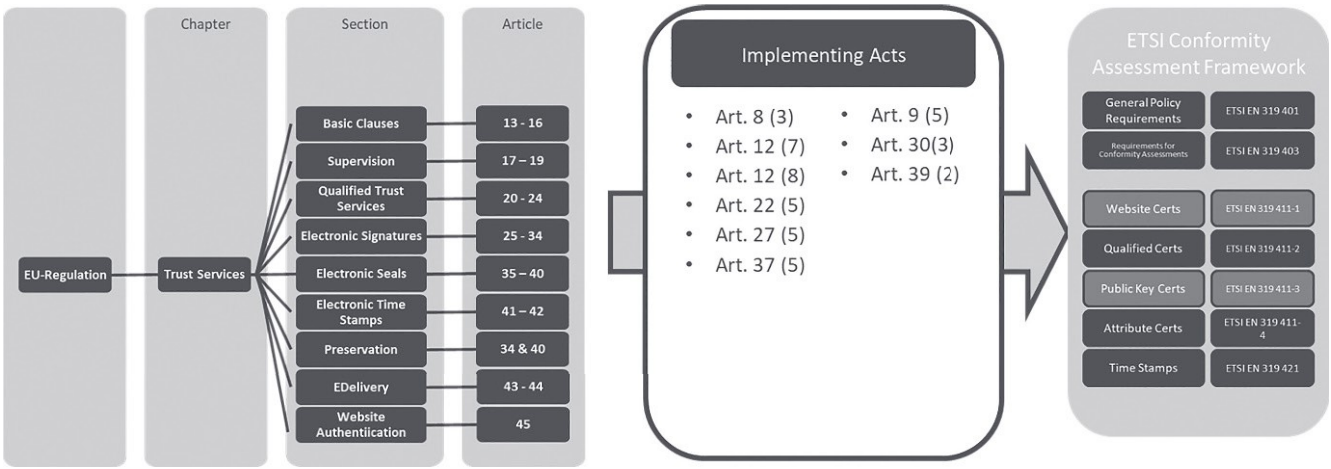
2 Regulatorischer Rahmen und Vertrauenswürdigkeit in der Digitalisierung

2.1 Regulatorischer Rahmen in Deutschland und Europa

Die eIDAS-Verordnung schuf im EWR einheitliche Vorgaben für vertrauenswürdige digitale Transaktionen auf Basis elektronischer Identifizierungsmittel sowie elektronischer Vertrauensdienste im Binnenmarkt. Als Identifizierungsmittel gilt hierbei z.B. der neue Personalausweis in Deutschland sowie dessen europäische Pendant. Die Vertrauensdienste umfassen Erzeugung sowie Prüfung elektronischer Signaturen, Siegel, Zeitstempel, Verifikationsdienste, Bewahrungsdienste (Beweiswerterhaltung), Einschreib- und Zustelldienste (z.B. De-Mail) sowie Websitezertifikate. Durch die Zulassung z.B. von Server- und Fernsignaturen ohne Signaturkarte sowie von Siegeln (Signaturen für Organisationen) ebenso wie die Pflicht zur Anerkennung jeder mindestens fortgeschrittenen elektronischen Signatur bzw. Siegel bzw. Zeitstempel (Art. 25, 35, 41 eIDAS) jedes qualifizierten europäischen Vertrauensdienstes durch öffentliche Stellen ist ein deutlicher Anstieg signierter Dokumente in Deutschland bereits im Gang, wie dies auch in den europäischen Nachbarstaaten bereits seit langen Jahren der Fall ist [BIT19], [KSDV15] [KoScKu18]. Die eIDAS definiert für die Bewahrungsdienste gemäß Artikel 34 eIDAS auch spezielle Anforderungen für die beweiswerterhaltende Aufbewahrung

Im Zuge der Umsetzung der eIDAS werden „beim Erlass von delegierten Rechtsakten bzw. Durchführungsrechtsakten, die von europäischen und internationalen Normungs-organisationen und -einrichtungen, insbesondere dem Europäischen Komitee für Normung (CEN), dem Europäischen Institut für Telekommunikationsnormen (ETSI), der Internationalen Normungsorganisation (ISO) und der Internationalen Fernmeldeunion (ITU), festgelegten Normen und technischen Spezifikationen berücksichtigt“ gem. eIDAS. Die genannten Standardisierungsgremien haben mit Mandat M416 der Europäischen Kommission die explizite Aufgabe, die rechtlichen Regelungen der eIDAS durch konkrete technische Standards zu untersetzen und so die Umsetzung durch Interoperabilität und Harmonisierung von Vertrauensdiensten (engl. Trust Services) und elektronischen Identifizierungsmitteln zu erleichtern [Ko17]. Diese technischen Standards werden zudem zunehmend weltweit angewandt, was deren Bedeutung hervorhebt [KSDV15]. Die nachstehende Grafik zeigt das Zusammenwirken von Rechtsrahmen [eIDAS] und den technischen Normen durch ETSI/CEN im Überblick.

Abbildung 1 | Zusammenwirken Rechtsrahmen, Implementing Acts und Standardisierung in eIDAS



In Deutschland wird die wirksame Durchführung von [eIDAS] durch das Vertrauensdienstegesetz [VDG] geregelt. Dieses sieht die Beweiswerterhaltung signierter Dokumente in § 15 [VDG] vor.

Die Umsetzung vertrauenswürdige digitaler Transaktionen sowie deren Nachweis wird durch weitere EU-Vorgaben wie der EU-Dienstleistungsrichtlinie oder der EU-Datenschutzgrundverordnung einerseits sowie durch branchenspezifische Vorgaben anderseits, so z.B. Patientenrechtegesetz, SGB V, eHealth-Gesetz im Gesundheitswesenbis hin zum Haftungsrecht nach BGB sowie im Bereich klinischer Forschung (GxP) oder im Gesundheitswesen resp. EASA Part 21, FDA in Luftfahrt und Pharma, EuroSOX oder PSD2 in der Finanzindustrie, untersetzt [KoKuSc19], [We18].

Eine weitergehende Digitalisierung hochregulierter Industrien im Allgemeinen ist bspw. durch elektronische Patientenakte und elektronischem Rezept im Gesundheitswesen, Tokenisierung und elektronische Identifizierung in der Finanzwirtschaft oder Vorgaben für öffentliche Stellen in Ländern und Kommunen im Zuge der länderweiten E-Government-Gesetze z.B. Einführung E-Akte, Umsetzung vom rechtssicheren ersetzenden Scannen, Annahme qualifiziert elektronisch signierter Dokumente oder die Verpflichtung zum Onlineangebot aller Verwaltungsleistungen nach OZG absehbar. Für die Justiz gilt, dass bis 2022 alle Gerichte die notwendigen Schriftsätze elektronisch annehmen müssen gemäß eJustice-Gesetz.

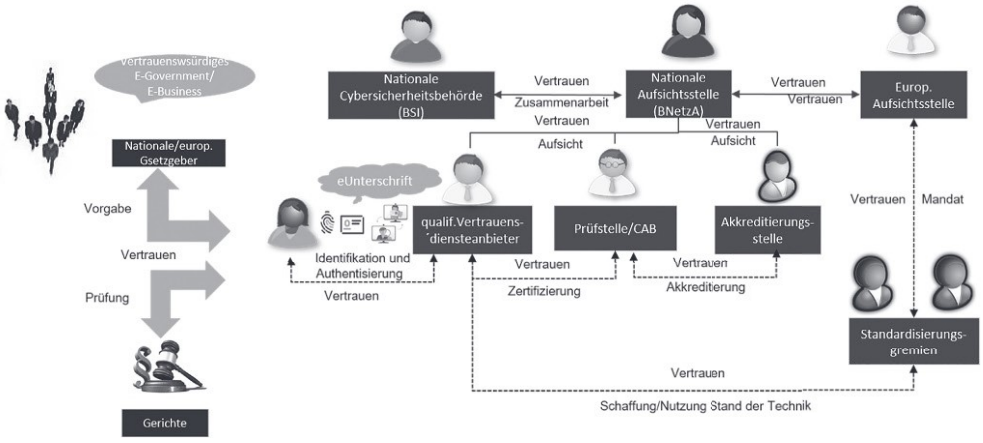
Untersetzt wird der regulatorische Rahmen durch verbindliche Standards und Normen, die als sog. Stand der Technik gelten. Um der Verpflichtung nachzukommen, behördliche Entscheidungen bis zum Ablauf der geltenden Aufbewahrungsfristen nachweisbar und damit gerichtsfest zu halten, sind insbesondere die Maßgaben zum Records Management sowie die Technischen Richtlinien RESISCAN (rechtssicheres ersetzendes Scannen TR03138) und BSI Technische Richtlinie TR-ESOR] hervorzuheben. Sowohl die TR-RESISCAN als auch die TR-ESOR sind zudem regulatorisch als Stand der Technik u.a. in den -Government-Gesetzen von Bund und Ländern, dem Vertrauensdienstegesetz oder der ZPO verankert [We18], [Ko16], so auch für Gesetzliche Krankenkassen im Leitfaden des Bundesversicherungsamts [LeitfBVA]. Die Bedeutung eines solch ordnungsgemäßen Records Management sowie der Umsetzung der genannten Technischen Richtlinien des BSI unter Nutzung der Vertrauensdienste der eIDAS zeigt sich zudem in einigen aktuellen Gerichtsurteilen, welche die Umsetzung des Stands der Technik faktisch einfordern [Az. 6 K 691/14.WI.A; Az. 6 K 808/17.WI.A].

2.2 Vertrauenswürdigkeit digitaler Aufzeichnungen

Vertrauenswürdigkeit geschäftsrelevanter Aufzeichnungen und Transaktionen erfordert in Deutschland und Europa vertrauenswürdige Dritten, die auf Basis gesetzlicher Vorgaben sowie geltender Standard und Normen agieren und wiederum durch vertrauenswürdige Dritte in einer Vertrauenskette transparent überprüft wie ermächtigt werden. Die nachstehende Grafik zeigt diese Vertrauensketten am Beispiel der [eIDAS].

Wesentliches Merkmal einer vertrauenswürdigen Digitalisierung ist Gewährleistung und Nachweis der zentralen Schutzziele:

Abbildung 2 | Vertrauensketten in eIDAS



- Integrität beinhaltet
  - Authentizität
  - Nachvollziehbarkeit
- Verfügbarkeit beinhaltet
  - Lesbarkeit/Nutzbarkeit
  - Verkehrsfähigkeit
- Vertraulichkeit

der elektronischen Prozesse anhand der geschäftsrelevanten Aufzeichnungen auf Basis der durch vertrauenswürdige Dritte definierten regulatorischen wie fachlich-technischen Anforderungen [KoKuSc19], [We18], [Ko21].

Nach derzeitiger Rechtslage ist kein IT-Verfahren, Organisation oder System aus sich selbst heraus vertrauenswürdig. In jedem Fall ist der Nachweis gegenüber Gerichten, Prüfbehörden etc. zu führen. [KoScKu18], [KoBeScKu18], [Ro07], [We18].

3 Wesentlicher Stand der Technik im Überblick

3.1 Grundsatz

Wie in den vorherigen Kapiteln dargestellt, bilden Standards und Normen anerkannter Standardisierungsorganisationen den sog. Stand der Technik. Hierunter werden also die fachlich-technischen Rahmenbedingungen zur Umsetzung und Nachweis einer vertrauenswürdigen Digitalisierung entsprechend den regulatorischen Vorgaben verstanden. Welcher Standard anzuwenden ist, ergibt sich demgemäß aus der Branche und konkreten Anwendungsfall der jeweiligen Institution. Die nachstehende Grafik gibt einen Überblick wesentlicher Standards und Normen zum langfristigen Nachweis digitaler Transaktionen und Aufzeichnungen.

Eine beweissichere Langzeitspeicherung gewährleistet dementsprechend sowohl die Erhaltung und Nachweis der Integrität, Authentizität und Vertraulichkeit geschäftsrelevanter Aufzeichnungen als auch deren Nachvollziehbarkeit, Verfügbarkeit und Verkehrsfähigkeit. Sie umfasst also:

- Informationserhaltung
  und
- Beweiswerterhaltung [Ko13] [KoScDH14] [KoScKu18].

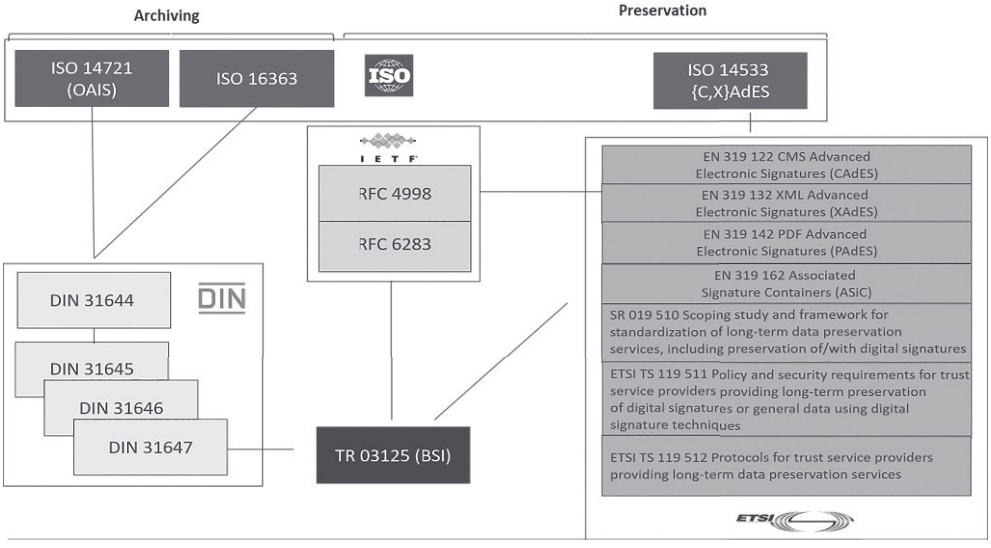
Elementare Basis bildet ein ordnungsgemäßes Records Management. Dieses stellt zum einen die Umsetzung der regulatorischen Vorgaben an elektronische Prozesse sicher und ermöglicht durch klare Regelungen, Prozesse sowie Rollen und Verantwortlichkeiten die Erfüllung geltender Dokumentationserfordernisse sowie die Strukturierung, Speicherung, Wiederauffindung und Bewahrung der hierfür notwendigen (geschäftsrelevanten) Unterlagen. Diese können dabei sowohl gescannte als auch digitale entstandene Dokumente, jedoch auch Daten aus Fachsystemen, bis hin zu Rechnungs- oder Forschungsdaten umfassen [We18], [KoKuSc20].

Das in ISO14721 normierte OAIS-Modell sowie die hierauf aufbauenden DIN31644 etc. definieren die notwendigen Prozesse und Informationspakete eines vertrauenswürdigen digitalen Langzeitarchivs. Die DIN31647 wiederum beschreibt die grundlegenden Funktionen zur Beweiswerterhaltung in einem OAIS-konformen vertrauenswürdigen digitalen Langzeitarchiv (dLZA). Um Authentizität und Integrität langfristig zu erhalten und nachzuweisen, gilt es, das dLZA um die notwendigen technischen Maßnahmen der digitalen Signaturtechniken, also Signaturen, Siegel, Zeitstempel oder Evidence Records, auf Basis der im Zuge der [eIDAS] entstandenen ETSI- Standards, vor allem hinsichtlich der Bewahrungsdienste gem. Art. 34 und 40 eIDAS zu ergänzen. Hierzu gehören vor allem die ETSI-Standards ETSI TS119511 und ETSI TS119512. Die TR-ESOR des BSI führt die Vorgaben zur Informations- und Beweiswerterhaltung logisch zusammen und definiert im Kern eine Middleware als Produkt zur Beweiswerterhaltung einschließlich der notwendigen Informationspakete, der äußeren Austauschschnittstellen sowie der Maßgaben zur Integration in ein vollständiges OAIS-konformes dLZA [KoScKu18], [KoKuSc19], [KuSc16]. Im Folgenden wird auf den Stand der Standardisierung insbesondere im Records Management sowie zur Beweiswerterhaltung näher eingegangen.

3.2 Records Management

Im Jahr 2016 wurde die ISO-15489 als zentrale Norm zum Records Management neugefasst. Der Fokus liegt nunmehr vorrangig auf elektronischen Aufzeichnungen. Die Norm reiht sich ein in den mit der ISO30300 (Terminologie), ISO30301](Basisanforderungen) und ISO30302 (Guidelines zur Implementierung) geschaffenen fachlichen Rahmen zum Records Management. Die 303xx-Familie richtet sich dabei an Management von Organisationen und beschreibt grundlegende Anforderungen an den Umgang mit geschäftsrelevanten Aufzeichnungen. Diese Vorgaben bilden die Basis für spezifische Standards zur fachlich-technischen Untersetzung.

Abbildung 3 | Wesentliche Standards und Normen



Die ISO-15489 selbst fordert zum einen die Definition klarer wie verbindlicher Regelungen, Prozesse, Rollen und Verantwortlichkeiten für die Erzeugung/Empfang, Ordnung, Speicher, Nutzung und Aufbewahrung – kurz das Management geschäftsrelevanter Aufzeichnungen auf Basis der jeweils geltenden regulatorischen Vorgaben. Ziel sind die Wahrung und langfristiger Nachweis der Authentizität, Zuverlässigkeit (inkl. Nachvollziehbarkeit und Vertraulichkeit), Integrität und Nutzbarkeit (inkl. Verkehrsfähigkeit) der geschäftsrelevanten Aufzeichnungen. Speziell im Kontext der Zuverlässigkeit wird die eindeutige Zuweisbarkeit explizit hervorgehoben. Hierauf basierend beschreibt ISO-15489 Anforderungen an die Identifikation geschäftsrelevanter Aufzeichnungen, die Systematisierung wie Indexierung von Aufzeichnungen sowie deren berechtigter Nutzung im Geschäftsprozess. Hervorzuheben ist zudem der Vorgehensvorschlag zur organisationsinternen Konzeption und Implementierung eines ordnungsgemäßen Records Management einschließlich der IT-Verfahren, die in geschäftsrelevanten Aufzeichnungen entstehen, empfangen, verwaltet und aufbewahrt werden einschließlich Ansätzen für eine spätere Migration im Sinne des Langzeiterhalts der Unterlagen. Im Kern fordern ISO-30301 und 15489, dass geschäftsrelevante Aufzeichnungen als Nachweis geschäftlicher Transaktionen gegenüber Prüfbehörden, Gerichten, Dritten dienen. Um dies zu erreichen, sind neben dem regulatorischen Rahmen die Maßgaben dieser Normen sowie der hierauf aufbauenden technischen Standardisierung entsprechend zu berücksichtigen [To07] [We18]. Untersetzt werden die ISO-/DIN-Normen durch themen- und branchenspezifische Standards wie insbesondere z.B. die TR-RESISCAN des BSI zum rechtssicheren ersetzenden Scannen sowie die TR-ESOR des BSI zur beweissicheren Aufbewahrung, auch als Produktkomponente im Rahmen (qualifizierter) Vertrauensdienste insbesondere auf Basis der ETSI-Vorgaben ETSI TS119511 und ETSI TS119512.

3.3 Beweissichere Aufbewahrung

3.3.1 Bewahrungsdienste gem. eIDAS (Service-Provider)

Die Standardisierung zur beweissicheren Aufbewahrung fokussierte bislang vorrangig auf die technischen Produkte sowie die aufzubewahrenden Aufzeichnungen selbst. Hinsichtlich der Betreiber entsprechender digitaler Langzeitspeicher- bzw. Langzeitarchiv-Dienste lagen bisher wenige Standards und keine regulatorisch determinierten Zertifizierungsverfahren vor.

Im Zuge der eIDAS wurden in Art. 34 und 40 eIDAS Anforderungen an die Bewahrung kryptographisch signierter, gesiegelter oder zeitgestempelter Dokumente mittels qualifizierter Bewahrungsdienste definiert. Unter Bewahrungsdienste sind im Kern (qualifizierte) Vertrauensdienste, also IT-Services zur beweiswerterhaltenden Aufbewahrung geschäftsrelevanter Aufzeichnungen zu verstehen. Bereitgestellt und betrieben werden diese durch (qualifizierte) Vertrauensdienste, die auf Basis der durch ETSI definierten Standards ETSI EN319401 und ETSI TS119511 von nationalen Konformitätsbewertungs- bzw. Prüfstellen zertifiziert werden und ihre Dienste in der Folge im EWR anbieten können. Soll die Beweiswerterhaltung als Dienst gegenüber Dritten angeboten werden, so muss der Betreiber sich als (qualifizierter) Bewahrungsdienst zertifizieren lassen [LeitlBNetzA]. Die Zertifizierung erfolgt national. Die Anerkennung, wie auch bei den übrigen Vertrauensdiensten (z.B. Erzeugung qualifizierter elektronische Signaturen/Siegel/Zeitstempel oder Einschreib-/Zustelldienste), gilt im gesamten Europäischen Wirtschaftsraum. Die Aufsicht obliegt in Deutschland der Bundesnetzagentur. Als Prüfstellen fungieren aktuell der TÜVIT Informationstechnik GmbH, datenschutz cert GmbH, SRC Security Research & Consulting GmbH und T-Systems International GmbH. An der technischen Standardisierung ist das BSI umfänglich beteiligt. Die im Zuge von Mandat 460 bei ETSI entstehenden Standards ETSI TS119511 und ETSITS119512 für (qualifizierte) Bewahrungsdienste ergänzen die allgemeinen Anforderungen gemäß ETSI EN319401 für (qualifizierte) Vertrauensdiensteanbieter (engl. Trust Service Provider (TSP)). Dabei fordern die europäischen Bewahrungs-Standards ETSI TS119511 und ETSI TS119512 von den Bewahrungsdiensten, dass die Integrität und Authentizität sowohl signierter als auch unsignierter Aufzeichnungen langfristig durch kryptographische Signaturtechniken basierend auf elektronischen Signaturen, Siegeln oder qualifizierten Zeitstempeln oder technische Beweisdaten (Evidence Records gemäß RFC4998, RFC6283, TR-ESOR) zu sichern und zu erhalten sind. Die konkreten Verfahren basieren dabei im Wesentlichen auf den auch in Deutschland angewendeten Hashbaumverfahren gemäß [Merk] und TR-ESOR.

Die nachfolgende Tabelle zeigt im Überblick die Kerninhalte der für (qualifizierte) Bewahrungsdienste wesentlichen Standards, nach denen diese Bewahrungsdienste sich zertifizieren lassen müssen. Im Zertifizierungsprozess sind vom möglichen (qualifizierten) Vertrauensdiensteanbieter für die Bewahrung kryptographischer elektronischer Signaturen, Siegel und Zeitstempel und Daten sowohl die Vorgaben nach ETSI EN319401 als auch ETSI TS119511 zu erfüllen. Dabei sind stets eine Stage1-Prüfung (Dokumentenprüfung) und eine Stage-2-Prüfung (technischer Vor-Ort-Tests) zu durchlaufen, wobei die erfolgreiche Stage-1-Prüfung Voraussetzung für die Stage-2-Prüfung ist. Bietet der angehende Bewahrungs-Vertrauensdienst (eng. Preservation Trust Service Provider (PSP)) bereits einen (qualifizierten) Vertrauensdienst an z.B. Erzeugung qualifizierter elektronischer Signaturen oder Siegel, so ist nur die Erfüllung der ETSI TS119511 nachzuweisen, da die Zertifizierung gegen ETSI EN319401 bereits für die übrigen Vertrauensdienste erfolgt ist [LeitLBNetzA].

(Qualifizierte) Bewahrungsanbieter müssen die vollständige Kontrolle über alle Prozesse und Aufzeichnungen seines Bewahrungsdienstes besitzen. Bypässe, durch die Aufzeichnungen am Bewahrungsdienst vorbei abgelegt werden können, sind untersagt. In die Standardisierung auf europäischer Ebene sind die fundierten Erfahrungen des BSI sowie der Praxis in Unternehmen und Behörden bei der beweiswerterhaltenden Aufbewahrung mit der TR-ESOR in Deutschland unmittelbar eingeflossen. So wird angehenden (qualifizierten) Bewahrungsdiensten das Zertifizierungsverfahren erleichtert, sofern diese ein gem. TR-ESOR v1.2.1 oder höher zertifiziertes Bewahrungsprodukt einsetzen. In diesem Fall entfällt nämlich ein Großteil der in ETSI TS119511 für (qualifizierte) Bewahrungsdienste vorgesehene Tests des Bewahrungsdiensts [ASS119511]. Es empfiehlt sich also, Produkte nach dem Stand der Technik, in Deutschland TR-ESOR, einzusetzen. Die Prüfung selbst erfolgt durch die nationale Konformitätsbewertungsstelle anhand dezidierter Prüfkataloge, welche die europäischen Standards weiter untersetzen. Diese nationalen Prüfkataloge wurden von der Bundesnetzagentur sowie dem Bundesamt für Sicherheit in der Informationstechnik als Empfehlungen für die Prüfstellen entwickelt [ASS319401], [ASS119511]. Die neu-

Tabelle 1 | Wesentliche Inhalte Standards für (qualifizierte) Bewahrungsdienste

Standard	Geltungsbereich	Kerninhalte
ETSI EN 319 401	Alle Vertrauensdienste	Grundlegende Vertrauensdienste-Prüfkriterien für ▪ das Risikomanagement ▪ „Policies" and Practices" ▪ das Management und den Betrieb eines Vertrauensdienstes
ETSI TS 119 511	Nur Bewahrungsdienste	Erweiterung der allgemeinen Anforderungen von ETSI EN319401 für (Langzeit-)Bewahrungs-Dienst, um Prüfprozesse bzgl. ▪ der Dokumentation und ▪ der Richtlinien (z.B.„Preservation Service Practice Statement", „Preservation Evidence Policy", etc.) sowie der darin enthaltenen betrieblichen und technischen Anforderungen (Preservation Profile, Preservation Protocol, etc.) Ziel: Gewährleistung der langfristigen ▪ Prüfbarkeit kryptographischer Signatur-Techniken (Signaturen/ Siegel/Zeitstempel/Evidence Records) und ▪ Bewahrung des Gültigkeitsstatus ▪ Erhalt eines„Proof of Existence" der beweisrelevanten Daten und Beweisdaten sowie ▪ Erhalt eines Proof of Existence der jeweils aufbewahrten signierten oder unsignierten Daten Speichermodelle: ▪ Mit Speicher (z.B. TR-ESOR) ▪ Mit temporärem Speicher ▪ Ohne Speicher
ETSI TS 119 512	Nur Bewahrungsdienste	Definition einer generischen Referenzarchitektur für Bewahrungsdienste ▪ Definition der Bewahrungs-Schnittstellen und Protokolle RFC4998, RFC6283 die unmittelbar auf diejenigen der TR-ESOR des BSI abbildbar sind s. TR-ESOR-TRANS ▪ Integration des Hashbaumverfahren nach RFC4998 RFC6283 bzw. TR-ESOR sowie ▪ Integration der AIP-Formate XAIP nach TR-ESOR-F resp. ASiC ETSI EN319162

esten Versionen der TR-ESOR, so v1.2.2 und v1.3, integrieren die Maßgaben der ETSI-Standards und legen mit den überarbeiteten Zertifizierungsvorgaben für Bewahrungsprodukte die Brücke zur Nutzung der o.g. Zertifizierungserleichterungen für (qualifizierte) Bewahrungsdiensteanbieter beim Einsatz von TR-ESOR-Produkten [ASS119511]. So wird eine [eIDAS] konforme beweissichere Langzeitspeicherung spürbar erleichtert.

3.3.2 BSI Technische Richtlinie TR-ESOR

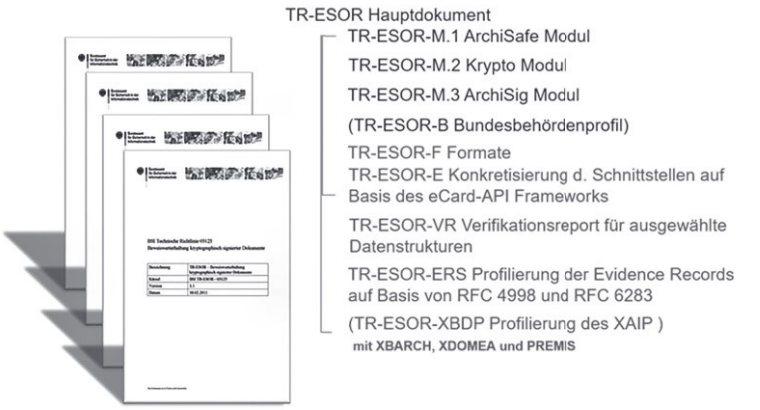
Die technische Richtlinie TR-ESOR des BSI, aktuell Version 1.2.2, gilt branchenübergreifend als verbindlicher Stand der Technik zur beweiswerterhaltenden Aufbewahrung in Deutschland. Sie beschreibt zum einen eine generische, modulare wie skalierbare Referenzarchitektur einer Middleware zur Beweiswerterhaltung, zum anderen die notwendigen verpflichtenden sowie optionalen Prozesse, ArchivInformationsPakete und Schnittstellen sowie Formate für technische Beweisdaten (Evidence Records). Die Zertifizierung konkreter Produkte auf Basis dieser TR-ESOR ermöglicht es zum einen dem Anwender, die Konformität von Marktlösungen gegenüber der TR transparent zu erkennen, zum anderen den Produktanbietern den Nachweis des Stands der Technik und angehenden (qualifizierten) Bewahrungsdiensteanbietern die Nutzung der in Kap. 3.3.1 beschriebenen Zertifizierungserleichterungen. Darüber hinaus wurden vom BSI Open-Source-Testwerkzeuge entwickelt, die auf Basis der definierten Schnittstellen und Formate der TR-ESOR die technische Interoperabilität der Schnittstellen, AIPs und Beweisdaten (Evidence Records) zwischen den Herstellern erleichtern [Ko13], [KoKuSc18], [Ko14], [KuSc16]. Die TR-ESOR selbst beruht resp. integriert nationale wie internationale Standards, so insbesondere ISO14721, ISO14533, RFC4998 RFC6283, ISO13527. ETSI TS119511, ETSI TS119512. Die TR-ESOR ist branchenübergreifend zur beweissicheren Langzeitspeicherung etabliert. Umfassende Anwendungsbeispiele finden sich u.a. im Public Sector, Gesundheitswesen, Luft- und Raumfahrt, Finanzindustrie oder dem Energiesektor. Aufbau und Dokumente sowie die Referenzarchitektur der TR-ESOR zeigen die folgenden Grafiken.

Mit der Version 1.2.1 wurde die TR-ESOR auf die wesentlichen Anforderungen der [eIDAS] angepasst.

Seit der TR-ESOR v1.2.2 ermöglicht ein optionales Upload-/Downloadmodul sowie ein Logisches XAIP die beweiswerterhaltende Aufbewahrung von Daten mit umfangreicher Dateigröße (> 2 GB) in selbsttragenden, jedoch logischen Containern. Damit wird z.B. die Bewahrung von Röntgenbildern, umfassenden Patientenakten oder Labordaten erheblich erleichtert.

Daneben wurde mit dem Transformator vom BSI nach TR-ESOR-TRANS eine Open-Source.Referenzimplementierung bereitgestellt, die eine Übersetzung der europäischen Schnittstelle aus ETSI TS119512 nach der zentralen Eingangsschnittstelle S.4 der TR-ESOR bereitgestellt, ohne dass eigentliche TR-ESOR-Produkt ändern zu müssen, so dass eine einfache Interoperabilität mit europäischen Lösungen ermöglicht wird. Darüber hinaus kann auch anstelle der Eingangsschnittstelle S.4 die ETSI-Preservation-API gemäß ETSI TS119512 in TR-ESOR eingesetzt werden.

Abbildung 4 | Dokumente der TR-ESOR



Die nachstehende Tabelle zeigt die wesentlichen Inhalte der verschiedenen TR-ESOR Versionen im Überblick

Hinsichtlich der Produktzertifizierung gegen TR-ESOR bestehen folgende Optionen:

- Stufe 1: logisch-funktionale Konformität
- Stufe 2: technische Interoperabilität

Bis einschließlich Version 1.2.1 besteht also ein stufenweises Zertifizierungsverfahren, wobei nicht jede Stufe zwingend durchzuführen, jedoch Stufe 1 Voraussetzung für Stufe 2 ist. In Ver-

Abbildung 5 | Referenzarchitektur der TR-ESOR

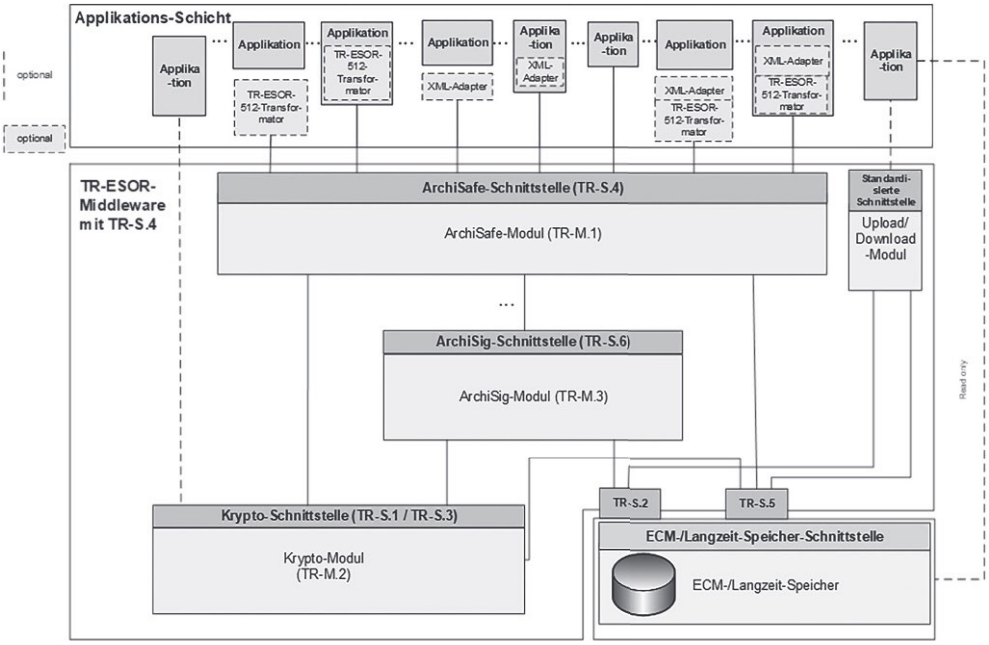


Tabelle 2 | Wesentliche Inhalte TR-ESOR v1.2.1, v1.2.2 und v1.3

Version	Kerninhalt	Erscheinungsdatum
v1.2.1	Editorielle Anpassung auf [eIDAS] Änderungen an Funktionen des Krypto-Moduls zur Signaturprüfung und Einholung der beweisrelevanten Daten gemäß [eIDAS] ▪ Schalenmodell und ▪ Kettenmodell ▪ Anforderung qualifizierter Zeitstempel und optional elektronischer Signaturen/Siegel bei qualifizierten Vertrauensdiensteanbieter	2018
v1.2.2	AIP für große Datenmengen ▪ Einführung eines logischen XAIP-Containers (LXAIP) ▪ Einführung des ASiC-AIP-Containers als Profilierung von ASiC-E [EN319162] Ergänzung der Referenzarchitektur bzgl. logischer LAIPs Ergänzung der zentralen Eingangsschnittstelle S.4 zur Verwendung von MTOM, Protokoll nach [ETSI TS119512] als weitere Eingangsschnittstelle neben der bestehenden S.4, auch auf Basis XML mit dem Binding SOAP oder auf Basis JSON mit dem Binding REST Bereitstellung des Testwerkzeugs zur Interoperabilität technischer Beweisdaten (Evidence Records) Open-Source-Modul zur Transformation der PreservationAPI ETSI TS119512 auf S.4 Konformitätstest-Spezifikation für Level 1 – Funktionale Konformität Appendix für TR-ESOR V1.2.1 und TR-ESOR V1.2.2 – Profilierung einiger TR-ESOR-Assessment-Kriterien zur ETSI TS 119 511 Prüferleichterung Leitlinie für die beweiswerterhaltende Aufbewahrung gemäß BSI TR-03125 TR-ESOR – Eine Handlungshilfe für Behörden und Unternehmen	2019 2020 2021
v1.3	Anpassung des Zertifizierungsschemas mit Fokus auf die technische Interoperabilität Bereitstellung des Testwerkzeugs zur Interoperabilität der Archivdaten-Container XAIP bzw. LXAIP und Schnittstellen Editorielle Anpassungen an den Dokumenten der TR	2021/22

Tabelle 3 | Unterschiede Zertifizierungsverfahren nach TR-ESOR in Versionen v1.2.1 bis v1.3

Version	Zertifizierungsoptionen	Ab Zeitpunkt
v1.2.1	Stufe 1: logisch-funktionale Konformität Stufe 2: technische Interoperabilität	2018 2018
V1.2.2	Nur Stufe 1: logisch-funktionale Konformität	2021
V1.3	Stufe 1 logisch-funktionale Konformität und Stufe 2: technische Interoperabilität zwingend notwendig zur Zertifizierung	2021/22

sion 1.2.2 ist nur eine Zertifizierung gegen Stufe 1 möglich. Hintergrund ist die Einführung eines neuen, an die Zertifizierung für die (qualifizierten) Bewahrungsdienste angelehntes Zertifizierungsverfahren für TR-ESOR-Produkte in v1.3. Mit den in TR-ESOR Appendix TR-ESOR-APP enthaltenen zusätzlichen Prüffällen wird die Nutzung der Zertifizierungserleichterungen für angehende (qualifizierte) Bewahrungsdienste gemäß [ASS119511] vereinfacht. Ab TR-ESOR v1.3 wird es nur noch ein Zertifizierungsverfahren geben. In diesem ist zunächst Stufe 1 logisch-funktionale Konformität erfolgreich zu absolvieren, danach wird Stufe 2 technische Interoperabilität durchgeführt. Es sind Stufe 1 und Stufe 2 zwingend zu bestehen, damit ein Zertifikat für ein TR-ESOR-Produkt erteilt werden kann.

Das Zertifizierungsverfahren liegt in der Verantwortung des BSI, als Prüfstelle fungiert derzeit datenschutzCert. Nachstehende Tabelle zeigt die wesentlichen Unterschiede im Produktzertifizierungsverfahren der einzelnen Versionen der TR-ESOR.

3.3.3 Zusammenwirken Bewahrungsdiensten und Produktstandards

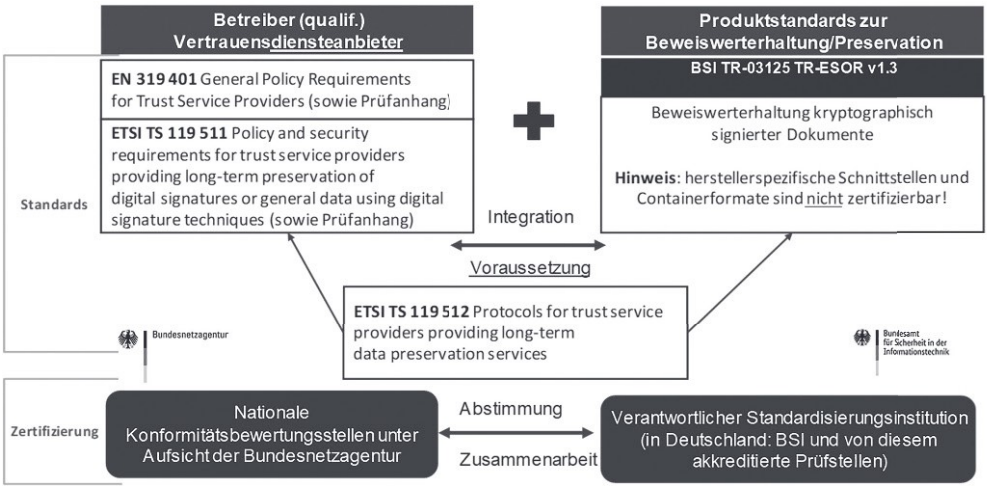
Die Standardisierung hinsichtlich Bewahrungsdiensten sowie den von diesen eingesetzten Produkten und Systemen ist komplementär. Die europäischen Maßgaben seitens ETSI EN319401 und ETSI TS119511 setzen die organisatorischen, prozessualen sowie technischen Vorgaben an den (qualifizierten) Vertrauensdienst, also den Service-Provider oder Betreiber. ETSI TS119511 definiert zudem grundlegende Anforderungen ans eingesetzte Bewahrungs-Produkt durch Verweis auf die [ETSI TS119512], die national durch die jeweiligen Bewahrungs-Produkts-Standards wie die TR-ESOR in Deutschland integriert wird. Die nachstehende Abbildung zeigt das Zusammenwirken im Detail

4 Fazit und Ausblick

Sowohl die Regelungen der [eIDAS]-Verordnung als auch die hierauf basierenden ETSI-

Normen schaffen die regulatorische wie technische Basis für einen digitalen Vertrauensraum im europäischen Binnenmarkt [BuDru18]. Untersetzt durch fachspezifische Regularien und Standardisierungen in Records Management und beweissicherer Langzeitspeicherung liegt ein rechtlich-organisatorisch wie valides fachlich-technisches Framework vor, um elektronische Prozesse in allen Geschäftsbereichen (öffentliche Verwaltung, Wirtschaft und Wissenschaft) vollständig sicher, nachweisbar und damit vertrauenswürdig bis zum Ablauf der geltenden Aufbewahrungsfristen zu etablieren

Abbildung 6 | Zusammenspiel (qualifizierter) Bewahrungsdienst und Bewahrungsprodukt



Qualifizierte Bewahrungsdienste, die Produkte gemäß TR-ESOR umsetzen, ermöglichen langfristige Sicherheit von elektronischen Daten und Dokumente und schaffen durch eine beweissichere Langzeitspeicherung eine nachhaltige und vertrauenswürdige Digitalisierung

Literatur

[1], [2] [ASS319401] BSI, Criteria for Assessing: Criteria for Assessing Trust Service Providers against ETSI Policy Requirements, Part 1: Assessment Criteria for all TSP – ETSI EN 319 401, 2020.

[3] [ASS119511] BSI, Criteria for Assessing: Criteria for Assessing Trust Service Providers against ETSI Policy Requirements, Part 2: Assessment Criteria providing long-term preservation of digital signatures or general data using digital signature techniques – ETSI TS 119 511, 2020.

[2] [BIT19]eIDAS und der ECM-Markt. Elektronische Identifizierung und Vertrauensdienste als Chance für die Digitalisierung. BITKOM e.V. (Hrsg.), Berlin 2019

[3] [BuDru18] Vertrauensraum in der Digitalisierung. Bundesdruckerei (Hrsg.). Berlin 2018

[4] [BSIGS] BSI-Grundschutzkompendium. Bundesamt für Sicherheit in der Informationstechnik. Bonn 2021

[5] [Fi06] S. Fischer-Dieskau: Das elektronisch signierte Dokument als Mittel zur Beweissicherung, Baden-Baden, 2006

[6] [Ko13] U. Korte, S. Schwalm, D. Hühnlein: Vertrauenswürdige und beweiswerterhaltende Langzeit-speicherung auf Basis von DIN 31647 und BSI TR-03125, Informatik 2013, GI-LNI, P220, ISBN 978-3-88579-614-5, S. 550-566, 2013

[7] [KoScDH14] U. Korte, S. Schwalm, D. Hühnlein: Standards for the preservation of evidence and trust. Proceedings Archiving 2014, Springfield 2014, S. 9-14

[8] [Ko14] U. Korte, S. Schwalm, D. Hühnlein: Standards und Lösungen zur langfristigen Beweiswert-erhaltung, DACH-Security 2014, S. 46-58, Frechen 2014

[9] [Ko16] U. Korte. S.Schwalm. T. Kusber. D. Hühnlein: Beweiswerterhaltung im Kontext eIDAS – eine Case Study. DACH-Security 2016, Frechen 2016 S. 379-392

[10] [Ko17] U. Korte. S. Schwalm. T. Kusber. D. Hühnlein, M. Prechtl, B. Wild: Datenpakete zur Informations- und Beweiswerterhaltung. Ein Vergleich. DACH-Security 2017. Frechen 2017 S. 291-303

[11] [Ko21] U. Korte., T. Kusber, K. Shamburger, S. Schwalm: Records Management and Long-Term Preservation of Evidence in DLT. in: OpenIdentitySummit 2020. Proceedings, Lyngby 2021

[12] [KSDV15] T. Kusber, S. Schwalm, A. Dörner, T. Vogt, Die Bedeutung der eIDAS-Verordnung für Unternehmen und Behörden. Neue Chancen und Herausforderungen für vertrauenswürdige elektronische Geschäftsprozesse in Europa, Berlin, 2015

[13] [KuSc16] T. Kusber, S. Schwalm: Elektronische Langzeitspeicherung als SOA-Dienst – Kernelement eines vertrauenswürdigen Informationsmanagements. INFORMATIK 2016 S. 869-882

[14] [KoScKu18] U. Korte, S. Schwalm, T. Kusber: Vertrauenswürdiges E-Government – Anforderungen und Lösungen zur beweiswerterhaltenden Langzeitspeicherung. 23. Archivwissenschaftliches Kolloqium. Marburg 2018

[15] [KoBeScKu18] U. Korte, Christian Berghoff, Steffen Schwalm, Tomasz Kusber: Langfristige Beweiswerterhaltung und Datenschutz in der Blockchain, DACH-Security 2018, S. 177-192, Gelsenkirchen, 2018

[16] [KoKuSc19] U. Korte, T. Kusber, S. Schwalm: Aktuelle Standards und Normen in Records Management und beweissicherer Langzeitspeicherung. in: 23. Tagung des Arbeitskreises „Archivierung von Unterlagen aus digitalen Systemen. Prag 2019

[17] [LeitLBNetzA] Leitlinie für digitale Signatur-/ Siegel-, Zeitstempel- und Beweisdaten (Evidence Record) – formate. Bundesamt für Sicherheit in der Informationstechnik/Bundesnetzagentur. 2019

[18] [LeitfBVA] Leitfaden Elektronische Kommunikation und Langzeitspeicherung elektronischer Daten. Bundesversicherungsamt 2018

[53] [Merk] R. Merkle: Protocols for Public Key Cryptosystems, Proceedings of the 1980 IEEE Symposium on Security and Privacy (Oakland, CA, USA), SS. 122-134, 1980

[60] [Ro07] A. Rossnagel: Langfristige Aufbewahrung elektronischer Dokumente, Anforderungen und Trends, Baden-Baden, 2007

[61] [SR019510] ETSI SR 019 510, Electronic Signatures and Infrastructures (ESI); Scoping Study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures, ETSI V1.1.1 (2017-05)

[19] [To07] Peter M. Toebak: Records Management. Ein Handbuch. Baden 2007

[20] [VS18] T. Vogt, S. Schwalm: eIDAS-ready?. Status Quo und Roadmap zur Umsetzung elektronischer Vertrauensdienste in Behörden und Unternehmen. Berlin 2018

[21] [We18] M. Weber, T Vogt, W. Krogel, S. Schwalm: Records Management nach ISO 15489. Einführung und Anleitung. Berlin 2018