Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Handreichung „Digitale Zeugnisse“

Eine Hilfestellung zur Digitalisierung von Zeugnissen und Bildungsnachweisen basierend auf den Technischen Richtlinien des BSI und europäischen Standards

Version: 1.0

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn

E-Mail: digitale-bildung@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Einleitung

1.1 Zweck und Rahmen des Dokuments

Ein **Zeugnis** im Sinne dieses Dokuments ist eine urkundliche Bescheinigung bzw. ein öffentliches Dokument – ein Schulzeugnis etwa enthält eine meist in Noten ausgedrückte Bewertung der Leistungen von Schülerinnen und Schülern, eine besonders hervorzuhebende Form ist das Abschlusszeugnis. Ein Prüfungszeugnis ist eine (öffentliche) Urkunde, die eine bestandene Prüfung dokumentiert, etwa eine bestandene Gesellen- oder Abschlussprüfung. Zeugnisse sind **Bildungsnachweise**, es gibt jedoch auch Bildungsnachweise die keine Zeugnisse im eigentlichen Sinne sind – sie können feingranularer gestaltet sein, sie können auch von nichtöffentlichen Stellen stammen und damit weniger oder anders reguliert sein. Viele der im Folgenden für digitale Zeugnisse getroffenen Aussagen lassen sich auch auf digitale Bildungsnachweise anwenden.

Im Zuge der fortschreitenden Digitalisierung finden zunehmend auch öffentliche elektronische Dokumente Verbreitung[1], klassische Schul- oder auch Hochschulzeugnisse dagegen werden in der Regel noch in Papierform erstellt, meist auch noch ohne jede begleitende digitale Form. Einschreibungen an weiterführenden Bildungseinrichtungen dagegen werden zunehmend digitalisiert, Bewerbungen bei Firmen sind bereits in den allermeisten Fällen nur noch digital erwünscht oder auch nur noch digital möglich[2]. Das weitverbreitete eigenhändig eingescannte Zeugnis verliert durch den Scanvorgang allerdings Sicherheitsmerkmale – die Verwendung geeigneten Papiers und dokumentenechter Tinte ist einem gescannten Dokument nicht mehr anzusehen, und durch den Verlust der Stofflichkeit geht auch der Integritätsschutz verloren und nachträglich vorgenommene Änderungen wären kaum noch feststellbar.

Diese Handreichung betrachtet den Fall von digitalen Zeugnissen und Bildungsnachweise als Ergänzung zu papiernen Zeugnissen (und Bildungsnachweisen) wie auch den Fall ausschließlich digitaler Zeugnisse ohne papierbasierte Entsprechung. Es wird dabei die Annahme zugrunde gelegt, dass diese digitalen Zeugnisse innerhalb des Geltungsbereichs der eIDAS-Verordnung verwendet werden sollen, und es wird ein inhaltlicher Schwerpunkt auf solche Zeugnisse gelegt, die von öffentlichen Stellen ausgestellt werden.

1.2 Zielsetzung und Zielgruppen

Zielgruppe dieser Handreichung sind all jene öffentlichen Einrichtungen, Firmen und Personen, die sich mit der Digitalisierung von Zeugnissen befassen. Die in den folgenden Kapiteln getroffenen Aussagen sind grundsätzlich als Empfehlungen zu verstehen. Das Ziel ist, aufzuzeigen, welche Vorarbeiten bereits geleistet wurden in der Erwartung, dass eine Verwendung existierender Arbeiten die Digitalisierung von Zeugnissen einerseits beschleunigen, vor allem aber auch sicherer gestalten kann.

Die Handreichung hat nicht das Ziel, juristische Fragestellungen zu beantworten, sondern beschränkt sich auf technische Empfehlungen – die rechtlichen Abschnitte dienen ausschließlich der Auswahlhilfe. Ebenfalls ist es nicht das Ziel dieser Handreichung, eine Aussage darüber zu treffen, ob und wann eine Digitalisierung von Zeugnissen sinnvoll ist – aber, wenn sie erfolgt, sollte sie stets gemäß aktuellem Stand der Technik erfolgen.

[1] Siehe auch Zivilprozessordnung (ZPO) § 371a (3)
[2] https://www.bitkom.org/Presse/Presseinformation/Die-Bewerbungsmappe-ist-tot.html

1.3 Struktur des Dokuments

Diese Handreichung stellt zunächst den „Lebenszyklus“ eines digitalen Zeugnisses dar und bietet damit einen Einstieg in die Thematik. Es folgen ausgewählte aktuelle Initiativen und Projekte, die sich ebenfalls mit dieser Thematik befassen und es werden einige wesentliche rechtliche Rahmenbedingungen dargestellt, gefolgt von fachlichen Anforderungen an digitale Zeugnisse. Daraus ableitend wird in den folgenden Kapiteln versucht, geeignete Technologien zur Digitalisierung von Zeugnissen zu benennen und - soweit vorhanden - passende, bereits existierende technische Richtlinien des BSI als auch deutsche, europäische und internationale technische Standards aufzuführen. Die Handreichung schließt mit Empfehlungen und einer Zusammenfassung sowie einem Ausblick.

2 Lebenszyklus eines Digitalen Zeugnisses

Bevor überhaupt digitale Zeugnisse ausgestellt werden können, ist es erforderlich, berechtigte von unberechtigten Zeugnisausstellern zu unterscheiden. Dieses Dokument geht vereinfachend davon aus, dass die Menge an Bildungseinrichtungen, die zur Ausstellung digitaler Zeugnisse berechtigt ist („Schulen“, „Hochschulen“, „Industrie- und Handelskammern“, usw.) vorab bekannt ist – auch wenn dies ganz besonders im internationalen Kontext eine größere Herausforderung darstellen wird. Über die technische Repräsentation der Menge der berechtigten Bildungseinrichtungen – Liste, Verzeichnis, Register, andere Datenstruktur, on- oder offline – wird hier keine Annahme getroffen.

Ein digitales Zeugnis oder allgemeiner formuliert ein digitaler Bildungsnachweis durchläuft eine Abfolge von Phasen:

1. Beantragung des digitalen Zeugnisses (optional)
2. Erstellung des digitalen Zeugnisses
3. Übergabe an den Zeugnisempfänger
4. Verwendung des Zeugnisses und Validierung der Zeugnisgültigkeit
5. Bewahrung und Löschung des Zeugnisses

Abbildung 1 veranschaulicht diese Phasen:

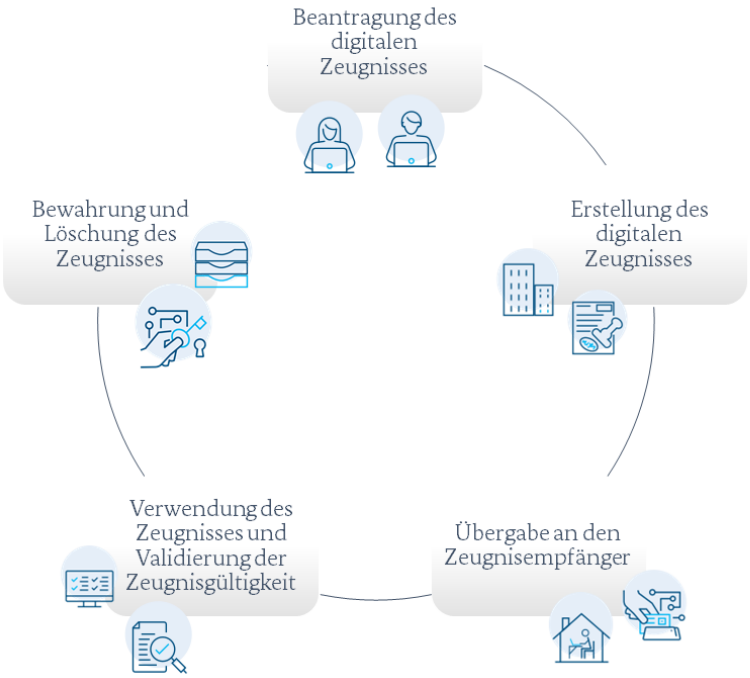

Abbildung 1: Lebenszyklus eines digitalen Zeugnisses

Phase 1. „Beantragung“ würde dann optional, wenn jeder Zeugnisempfänger ein digitales Zeugnis ohne Antrag erhalten würde. Eine zusätzliche Phase „Rückruf“ wäre ebenfalls denkbar. In den folgenden Abschnitten wird auf alle fünf genannten Phasen eingegangen.

2.1 Beantragung des digitalen Zeugnisses

Der Zeugnisempfänger oder die Zeugnisempfängerin stellt einen Antrag auf Ausstellung eines digitalen Zeugnisses. Hierbei kommen dieselben Wege in Betracht wie bei anderen Online-Antragsverfahren auch. Die zum Empfang des Zeugnisses berechtigte Person (oder eine jeweils erziehungsberechtigte Person) verwendet ein vorhandenes **Authentisierungsmittel**, um ihre Identität gegenüber dem Online-Dienst nachzuweisen. Im einfachsten Fall ist ein Authentisierungsmittel ein Passwort. Empfohlen wird grundsätzlich die Verwendung einer Zwei-Faktor-Authentisierung[3] - das bedeutet, es wird ein Passwort und zusätzlich ein zweiter Faktor wie bspw. ein Bestätigungscode auf einem weiteren Gerät, ein Fingerabdruck oder ein USB-Token verwendet. Für ein hohes Vertrauensniveau steht allen Bürgerinnen und Bürgern ab 16 Jahren die **Online-Ausweisfunktion**[4] zur Verfügung – das Authentisierungsmittel besteht hierbei aus einer sechsstelligen PIN und dem Personalausweis. Nach erfolgreicher Authentisierung stellt der Zeugnisempfänger einen Antrag auf ein digitales Zeugnis und der Online-Dienst übermittelt die Antragsdaten auf sicherem Weg an die Bildungseinrichtung.

Weitere Detailinformationen zur Identifizierung und Authentisierung finden sich im Folgenden in Kapitel 8.

2.2 Erstellung des digitalen Zeugnisses

Ein digitales Zeugnis wird anhand der vorliegenden Daten im IT-System der Bildungseinrichtung erstellt. Es kann eine menschen- oder eine maschinenlesbare Form haben. Oder es kann beide Formen haben, entweder unabhängig voneinander (als zwei separate Zeugnis-Objekte) oder eingebettet ineinander (ein Zeugnis-Objekt in einem anderen). Empfehlenswert für die menschenlesbare Form ist für Dokumente mit Text und Tabellen die Verwendung des Portable Document Format 2.0 (PDF), für eine Langzeitspeicherung empfiehlt sich das Format PDF/A. Empfehlenswerte maschinenlesbare Formate für strukturierte Zeugnisdaten sind Extensible Markup Language (XML) und JavaScript Object Notation (JSON). Diese und weitere empfohlene Dateiformate sind aufgelistet in der Architekturrichtlinie für die IT des Bundes - Technische Spezifikationen zur Architekturrichtlinie[5]. Der für den Anwendungsfall Zeugnis besonders relevante Standard XBildung[6] und die drei Spezifikationen XSchule, XHochschule und XBerufsbildung basieren auf XML. Für den internationalen Transfer von Studierendendaten ist EMREX ein relevanter Standard.

Ein herkömmliches Zeugnis in Papierform beinhaltet Elemente um die Echtheit (Authentizität) erkennen zu können und um feststellen zu können, ob es in unmodifiziertem Zustand vorliegt (Integrität). Die Anwendung **digitaler Signaturverfahren** erlaubt die Prüfung auf Echtheit und die Erkennung von eventuellen Modifikationen bei digitalen Dokumenten. Hierbei kommen asymmetrische kryptographische Verfahren zum Einsatz. Wird eine digitale Signatur im Auftrag einer juristischen Person (wie einer Bildungseinrichtung) aufgebracht, spricht man von einem **elektronischen Siegel**. Zu allen vorgenannten Dateiformaten existieren passende, auf europäischer Ebene standardisierte Signaturformate.

Einen zusätzlichen Weg zur Erstellung digitaler Versionen von existierenden papiernen Zeugnissen bietet das **ersetzende Scannen**, siehe hierzu Kapitel 7.

[3] https://www.bsi.bund.de/dok/11693908
[4] https://www.personalausweisportal.de/Webs/PA/DE/buergerinnen-und-buerger/online-ausweisen/online-ausweisen-node.html
[5] https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitaler-wandel/architekturen-standard/Architekturrichtlinie_techn_Anhang.pdf?__blob=publicationFile&v=7
[6] https://xbildung.de/web/

2.3 Übergabe an den Zeugnisempfänger

Wie auch bei der Zustellung von allen weiteren öffentlichen digitalen Dokumenten stehen für die Zustellung und Übergabe von digitalen Zeugnissen mehrere Alternativen zur Verfügung:

- Es existiert ein Webportal an einer bekannten Adresse, und nach erfolgreicher Authentisierung hat der Zeugnisempfänger die Möglichkeit des Downloads
- Ein digitales Zeugnis wird an das Postfach des **Nutzerkontos**[7] des Zeugnisempfängers übermittelt
- Der Zeugnisempfänger lädt sein digitales Zeugnis in eine Wallet (zum Beispiel auf seinem Smartphone)

In jedem Fall wird sich der Zeugnisempfänger vor Erhalt des Zeugnisses authentisieren, mit einem Authentisierungsmittel, welches dem erforderlichen **Vertrauensniveau** entspricht (oder darüber liegt). Das mindestens erforderliche Vertrauensniveau kann je nach Zeugnis oder Bildungsnachweis variieren – so wird ein Schulabschlusszeugnis möglicherweise ein höheres Vertrauensniveau erfordern als der Nachweis, dass ein einzelner Kurs erfolgreich besucht wurde, so kann ein substantielles oder auch ein hohes Vertrauensniveau erforderlich sein (weitere Detail-Informationen siehe Kapitel 8).

2.4 Verwendung des Zeugnisses und Validierung der Gültigkeit

Liegt ein digitales Zeugnis im Format eines signierten oder gesiegelten PDFs vor, kann es bereits ohne weitere spezifische IT-Systeme allein mit verbreiteter Standardsoftware dargestellt werden und seine Integrität kann geprüft werden. Für die Prüfung ob die Signatur bzw. das Siegel von einer berechtigten Bildungseinrichtung stammt, ist ein weiterer Schritt erforderlich. Liegt (auch) eine maschinenlesbare Form vor, kann ein entsprechend gestaltetes IT-System (etwa zur Entgegennahme von Bewerbungen) eine weitere Automatisierung ermöglichen. Eine vollständige Validierung besteht aus den Schritten

1. Prüfung der Syntax – sind die einzelnen inhaltlichen Elemente an der Stelle und von der Art, wie erwartet?
2. Mathematische Gültigkeit – der kryptographische Teil der digitalen Signatur wird geprüft, damit können Änderungen nach der Signierung erkannt werden?
3. Gültigkeit der für die Signatur / das Siegel verwendeten Zertifikate gemäß Gültigkeitsmodell[8] (ist das Zertifikat abgelaufen, wurde es zurückgerufen?)
4. Prüfung der Zertifikatskette und des Vertrauensankers – ist das verwendete Zertifikat tatsächlich das einer berechtigten Bildungseinrichtung?

Diese Prüfungen können prinzipiell alle mit handelsüblichen Softwareprogrammen durchgeführt werden (sofern die nötigen Informationen etwa für 4. an einer vertrauenswürdigen Stelle öffentlich verfügbar sind). Insbesondere für die Schritte 2 und 3 – die **Prüfung der Integrität** und der Signatur/des Siegels – stehen eine Reihe von Anwendungen zur Verfügung. Einfacher und nutzerfreundlicher ist die Verwendung eines spezifischen Tools zur lokalen Installation oder die Nutzung eines entsprechenden Online-Dienstes zur Validierung digitaler Zeugnisse. Spezifische Tools oder Dienste könnten auch auf einen eventuellen Rückruf einzelner Zeugnisse hin prüfen.

[7] https://www.digitale-verwaltung.de/Webs/DV/DE/onlinezugangsgesetz/rahmenarchitektur/basisdienste-basiskomponenten/nutzerkonten/nutzerkonten-node.html

[8] Siehe Kap. 9.2

2.5 Beweiswerterhaltende Langzeitspeicherung und Archivierung oder Löschung des Zeugnisses

Für viele (digitale) Dokumente existieren gesetzliche Vorgaben, wie lange sie aufbewahrt werden müssen – im Fall von Abschlusszeugnissen können es mehrere Jahrzehnte verpflichtende Aufbewahrungsdauer sein. Folgende Aspekte sollten berücksichtigt werden:

- Datenformat – kann es in 10 / 20 / 30 Jahren noch mit den dann verfügbaren IT-Systemen gelesen und verarbeitet werden?[9]
- Datensicherung – ist sichergestellt, dass die Daten sowohl bei technischen Defekten als auch bei unerwünschter physikalischer Einwirkung (z.B. Wetterereignissen) wiederhergestellt werden können?
- Datenschutz – kann auch langfristig der Zugriff von nicht berechtigten Personen ausgeschlossen werden?
- **Beweiswerterhalt** (Bewahrung) – sind Mechanismen implementiert, welche die ständige Weiterentwicklung der kryptographischen Verfahren berücksichtigen und den Integritätsschutz auch in Zukunft (bei neuen Angriffsmöglichkeiten auf die Kryptographie) sicherstellen?

Archivierung oder Löschung (nach Aufbewahrungsfrist) – sind die digitalen Zeugnisse an das zuständige Archiv anzubieten, bevor eine Löschung erfolgen würde? Es existieren bereits digitale Archive und entsprechende Technologien, und auch für den Beweiswerterhalt bei der Langzeitspeicherung existieren BSI-zertifizierte Softwarelösungen[10]. Digitale Langzeitarchive gewährleisten auch nach Ablauf der Aufbewahrungsfrist die Beweiswerterhaltung. Werden neue Strukturen bei der Bereitstellung von Zeugnissen aufgesetzt, sollte auch das Ende bzw. das Nachleben der Unterlagen in den gesetzlich zuständigen Archiven berücksichtigt werden, damit die Überlieferungsbildung gesichert wird.

[9] Siehe auch Kap 10.1
[10] https://www.bsi.bund.de/dok/6618080

3 Projekte und Initiativen

3.1 Ansätze basierend auf Self-sovereign Identities oder Distributed-Ledger-Technologie

Politik und Wirtschaft in Deutschland und der EU haben das Potenzial von digitalen Identitäten und digital verifizierbaren Nachweisen erkannt. Dies zeigt sich an verschiedenen strategischen Initiativen und den derzeitigen Entwicklungen auf Länder-; Bundes- und europäischer Ebene. Einige Ansätze beruhen auf Blockchain bzw. der Distributed-Ledger-Technologie (DLT) und manche davon (zusätzlich) auf dem Konzept der selbstverwalteten Identitäten (Self-sovereign Identities – SSI). Grundlegende Empfehlungen zu Blockchain finden sich in der Veröffentlichung „Blockchain sicher gestalten“[11] und spezifischer für SSI in Kombination mit DLT im „Eckpunktepapier für Self-sovereign Identities (SSI)“[12] [BSI SSI].

Mit dem „**Schaufenster Sichere Digitale Identitäten**“[13] sollen digitale Identitätslösungen, die gleichermaßen nutzerfreundlich, vertrauenswürdig und wirtschaftlich sind, der öffentlichen Verwaltung, Wirtschaft und natürlich der Bevölkerung in Deutschland nähergebracht werden. Ziel der Schaufensterprojekte ist es, die technischen, organisatorischen und rechtlichen Grundlagen für digitale Identitätslösungen zu schaffen. Nutzer und Nutzerinnen sollen in naher Zukunft ihre digitalen Identitäten und unterschiedliche Dokumente, wie etwa Personalausweis, Führerschein oder auch Zeugnisse, in Form von digitalen Zertifikaten selbst auf ihren mobilen Endgeräten verwalten und bei Bedarf Teile davon in digitalen Transaktionen vorweisen können.

Mit **Cert4Trust** haben die Industrie- und Handelskammer für München und Oberbayern und das Bayerische Staatsministerium für Digitales gemeinsam mit anderen Partnern eine Lösung entwickelt, die es ermöglicht digitale Dokumente durch ihren in der Cert4Trust Blockchain abgelegten Hashwert zweifelsfrei zu identifizieren und eine Aussage über die Gültigkeit zu treffen. Die Identifizierung der Einsteller wird dabei über Smart Contracts abgebildet. Seit Sommer 2020 ist das System in der IHK München im produktiven Einsatz, 2023 sind bereits sieben IHKs Nutzer. Absolventen der beruflichen Ausbildung erhalten zusätzlich zu ihrem Papier-Zeugnis ein elektronisches Abbild, das sie im Azubi-Portal der IHK herunterladen können. Das mit einem Salt versehene elektronische Zeugnis wird als PDF-A archiviert und der Hashwert des Dokuments über einen Smart Contract gemeinsam mit dem Dokumentenstatus in der Cert4Trust Blockchain abgelegt. Cert4Trust stellt neben der Blockchain Infrastruktur eine Webanwendung[14] bereit – hier können die elektronischen Zeugnisse z.B. durch Personaler überprüft werden, indem wiederum der Hashwert berechnet und mit den Einträgen in der Blockchain verglichen wird. Die Anwendung gibt als Ergebnis direkt eine Auskunft über Gültigkeit und Echtheit des Dokuments.

Das 2020 von Partnern aus verschiedenen Bildungssektoren, Wirtschaft- und Forschungsbereichen der Bundesrepublik Deutschland gegründete **Netzwerk Digitale Nachweise**[15] (NDN) untersucht den Anwendungsfall von digitalen Nachweisen in unterschiedlichen Kontexten. Dabei steht der Austausch von Informationen und die Vorstellung von thematisch passenden Projekten im Vordergrund des Netzwerks. Digitale Nachweise sollen fälschungssicher und maschinenlesbar gestaltet werden, sodass der Ursprung und die Integrität der Nachweisdaten über einen lebenslangen Zeitraum geprüft und die Nachweisdaten automatisiert in digitale Prozesse integriert werden können. Der ursprüngliche Fokus der Arbeitsgruppe lag auf dem Anwendungsfall Blockchain-verifizierbarer Nachweise. Hier wird zusätzlich zum Nachweis in Schriftform eine digitale Nachweisdatei erzeugt. Mit Hilfe einer mathematischen Einwegfunktion wird eine Prüfsumme der Nachweisdatei erstellt, ein sogenannter Hashwert, der zusammen mit der Identitätskennung

[11] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.html
[12] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunkte_SSI_DLT.html
[13] https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/sichere_digitale_ident.html
[14] https://check.cert4trust.de
[15] http://netzwerkdigitalenachweise.de/

der ausstellenden Institution manipulationssicher in eine Blockchain geschrieben wird. Der Empfänger der Nachweisdatei hat die Möglichkeit, mit einfachen technischen Mitteln die Echtheit dieser zu überprüfen. Aktuell wird betrachtet, welche Mehrwerte neue Technologien im Bereich der Nachweise bieten. Dazu gehören insbesondere die Bereiche „Berufsbildung“ und „Lebenslanges Lernen“. Technologisch wird der Einsatz der sogenannten „Verifiable credentials“ im nationalen wie europäischen Kontext betrachtet. In diesem Zusammenhang ist die Teilnahme am EBSI-Early Adopterprogram oder auch die Teilnahme an den LargeScalePilots beim Einsatz der EU Digital Identity Wallet (EUDIW) zu nennen.

Europaweit wird inzwischen in verschiedenen Projekten bzw. Arbeitsgruppen (zum Beispiel **European Blockchain Services Infrastructure** (EBSI)[16] oder European Self-Sovereign Identity Framework (ESSIF)) auch daran gearbeitet, Nachweise nicht mehr als Dokumente zu sehen, sondern als einzelne, überprüfbare Referenzen (sogenannte „Verifiable Credentials“). EBSI hat eine Infrastruktur aufgesetzt, die es ermöglicht auf europäischer Ebene digitale Nachweise auf Verifiable Credentials Basis zu verarbeiten. In diesem Zusammenhang gibt es auch einen „Diploma Use Case“, der den Europäern mehr digitale Kontrolle über ihre Bildungszertifikate geben soll.

Die Technische Universität München, das Hasso-Plattner-Institut für Digital Engineering an der Universität Potsdam und der Deutsche Akademische Austauschdienst untersuchten im Forschungsprojekt „**Digitale Bildungsnachweise für Hochschulen (DiBiHo)**“[17][18] die Frage, wie ein vertrauenswürdiger, verteilter und international interoperabler Infrastrukturstandard für das Ausgeben, Speichern, Anzeigen und Überprüfen akademischer Bildungsnachweise beschaffen sein soll – wenn die Lernenden im Mittelpunkt stehen. Dafür werden Musterprozesse verschiedener Anwendungsfälle (Abschlusszeugnis, MOOC, Stipendiennachweis) beschrieben und evaluiert. Ziel ist die technologieagnostische Exploration zur Eignung von Konzepten, Datenformaten und Standards für den digitalen, internationalen Transfer von digitalen Bildungsnachweisen sowie die Förderung von Lernendenmobilität und vereinfachte internationale Anschlussfähigkeit von Bildungssystemen.

Abbildung 2 Projekt DiBiHo

[16] https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home
[17] https://www.it.tum.de/it/dibiho/
[18] https://www.daad.de/en/the-daad/what-we-do/dibiho/

3.2 Projekt Bildungsraum Digital (BIRD) und Bildungsraum

Das Forschungs- und Entwicklungsprojekt Bildungsraum Digital (BIRD) unter Leitung der Universität Potsdam erarbeitet den ersten Prototypen der digitalen Vernetzungsinfrastruktur Bildung des Bundesministeriums für Bildung und Forschung (BMBF)[19]. Zur Erschließung und zum Aufbau eines digitalen Bildungsraums[20], der alle Bildungsbereiche umschließt, fördert das BMBF neben BIRD mehrere dutzend Einzelvorhaben, in denen innovative Bildungsangebote- und -anwendungen für Lernende und Lehrende (weiter-)entwickelt und die über eine föderierte IT-Infrastruktur miteinander vernetzt werden. Die Anschlussfähigkeit dieser Projekte mit den Basiskomponenten einer digitalen Vernetzungsinfrastruktur wird über die Referenzprototypen des BIRD-Projekts validiert. Ziel ist es, bestehende digitale Bildungsplattformen und digitale Lehr-, Lern- und Serviceangebote so miteinander zu vernetzen, dass digitale Bildung einfacher zugänglich und individuelle Lernreisen nahtlos digitaler erlebbar werden.

Digitale Bildungsnachweise sind hier hoch relevant. Das Nutzungsspektrum dieser Nachweise ist breit gefächert und umfasst alle Bildungsetappen und die dahinterliegenden Verwaltungsprozesse. Im Projekt wird das Ziel verfolgt, maschinenlesbare und fälschungssichere digitale Bildungsnachweise unabhängig vom Nachweistypus (z.B. Schul- und Abiturzeugnisse, Berufsausbildungszeugnisse, Studienleistungen, berufliche Weiterqualifikationen oder jeweilige Teilleistungen) zu entwerfen. Anhand von ausgewählten Anwendungsfällen werden die Konzepte getestet und umgesetzt und dabei auch in der Domäne Bildung angrenzende Verfahren (z.B. Visavergabe) in den Blick genommen. Schließlich soll eine digitale Lösung entstehen, die einfach zu bedienen ist, kontinuierlich technologisch weiterentwickelt werden kann, auf offenen Standards basiert und auch komplexe hierarchische Nachweisstufen abbilden kann. Mit dem Ansatz von BIRD kann ein wichtiger Schritt in Richtung Digitalisierung der Verwaltungsleistungen in der Domäne Bildung mit einem nutzer- und nutzerinnenzentrierten und selbstsouveränen Umgang mit Bildungsnachweisen verbunden werden, der Lernende auf ihrer lebenslangen Bildungsreise unterstützt und einen sicheren und schnellen Austausch von Informationen gewährleistet.

BIRD widmet sich folgenden Aufgaben:

- dem Einsatz einer zentralen Instanz (Bildungs-PKI) für die Prüfung der Authentizität der Herausgebenden und deren digitaler Bildungsnachweise ohne den Einsatz von Vertrauensdiensteanbietern im Sinne der eIDAS-Verordnung,
- der Berücksichtigung von dezentralen Strukturen für die Ermittlung der Identität der Herausgebenden,
- dem generischen Einsatz von digitalen Bildungsnachweisen unter Nutzung generischer Workflows (Herausgeben, Transport, Speichern, Bewahren, Digitalisieren, Zurückziehen, Authentifizieren, Autorisieren),
- der Integration in bereits bestehende Prozesse und IT-Lösungen ohne die Notwendigkeit händischer Übertragungen,
- der technischen Abbildung der Fragestellung: “Welche Herausgebende (ggf. bis auf Mitarbeitendenebene) darf welche Typen von digitalen Bildungsnachweisen ausstellen?”,
- der Analyse, inwiefern der skizzierte Lösungsansatz ggf. an ein eIDAS Szenario angebunden werden kann,
- die Gestaltung einer anwendungsfreundlichen Gesamtlösung, um ohne Systembrüche aus den jeweiligen Anwendungen wie Schulverwaltungssystemen, Student Lifecycle Management Systemen o.Ä. beispielsweise die Erstellung, Überprüfung und Bewahrung von digitalen Bildungsnachweisen zu gewährleisten,

[19] https://www.daad.de/de/der-daad/was-wir-tun/digitalisierung/bird/
[20] https://www.bildungsraum.de/

- die Berücksichtigung von föderalen und kommunalen Strukturen hinsichtlich Digitalisierung und Bewahrung von bereits existenten Papier-Bildungsnachweisen
- dem Aufbau einer Architektur, die möglichst agnostisch in Bezug auf Form und Inhalt der digitalen Bildungsnachweise sowie der eigentlichen Signatur ist.

Als zentrale Instanz wird eine X509/PKI Infrastruktur genutzt. Diese Technologie ist fest in der Domäne Bildung und vielen anderen Bereichen global verankert und akzeptiert. Alle Entwicklungen in Bezug auf den Prototypen sind entweder Open-Source oder nutzen Open-Source Komponenten. Die Weiterentwicklung und Pflege sind mit geringen, bis keinen Hindernissen möglich. Die Komponenten sollen hinsichtlich Veränderungen bezüglich technischer (z.B. Signatur) und inhaltlicher (z.B. EDCI) Standards so flexibel wie technisch möglich gehalten werden.

Die digitalen Bildungsnachweise bestehen sowohl aus einem PDF-Anteil (Darstellungsebene), der mit jedem Browser angezeigt werden kann, als auch aus Datenstrukturen (z.B. inhaltlich im Format X-Schule oder ELMO und technisch im Format JSON oder XML), die es gestattet, die Nachweisdaten elektronisch auszulesen und zu verarbeiten. Die im PDF (PDF/A-3) integrierten und mit einer/einem fortgeschrittenen Signatur/ Siegel (AdES) versehen Datenstrukturen werden dann mit einer/ einem qualifizierten Signatur/ Siegel (qeS, qeSi) für das PDF versehen. Im Rahmen des Prototyps hat das Projektteam BIRD die Möglichkeiten des Einsatzes der qeS analysiert. Dabei wurde festgestellt, dass die qeS nicht garantiert, dass die herausgebende Stelle auch die Berechtigung hat den jeweiligen digitalen Bildungsnachweis herauszugeben. Trotzdem ist hier von Vorteil, dass mit der qeS die Integrität des Gesamtdokuments gestärkt wird und die eIDAS Integration erfolgt. Dafür ist es nicht notwendig je Herausgeberin eine qeS zu beschaffen, sondern eine für die Domäne Bildung bzw. für die Bildungs-PKI. Dies ergibt einen Kostenvorteil, der auch für die Nutzung von digitalen Bildungsnachweisen für die breite Masse entscheidend sein kann.

Für das Vertrauen in digitale Bildungsnachweise braucht es eine dritte (fachliche) Instanz, die die Herausgeberin prüft und feststellt welche digitalen Bildungsnachweise in welcher Periode durch die Herausgeberin ausgestellt werden dürfen. Die nachgelagerte PKI sorgt dann für die Verheiratung von fachlichem und technischem Vertrauen durch zentrale Dienste für Zertifikate (Herausgeben, Verifizieren, Zurückziehen) und Signaturen/ Siegel (Herausgeben, Zurückziehen, Verifizieren).

Der generische, funktionsfähige und anpassbare BIRD-Prototyp wird im Rahmen des OZG-Projektes „Digitales Schulzeugnis“ mit den beteiligten Ländern und der Vernetzungsinfrastruktur digitale Bildung im Rahmen von Feldtests.

3.3 Digitale Vernetzungsinfrastrukur Bildung („Mein Bildungsraum“)

Das Themenfeld Bildung[21] ist eins der 14 großen Themenfelder des Onlinezugangsgesetzes[22], in denen Bürgerinnen und Bürger Verwaltungsleistungen im Bildungsbereich online zugänglich gemacht werden soll. Das federführende Bundesressort ist das Bundesministerium für Bildung und Forschung (BMBF), auf Länderebene ist Sachsen-Anhalt federführend zuständig. Gemeinsam wird die digitale Vernetzungsinfrastruktur Bildung realisiert, die einen sicheren Zugang zu deutschen und europäischen Bildungsangebote gewährleisten wird. Die digitale Vernetzungsinfrastruktur wird bundesweit Bildungsplattformen und Bildungsangebote einbinden und den Bildungszugang erleichtern.

Ziel der digitalen Vernetzungsinfrastruktur ist die Ermöglichung einer lebensbegleitenden Bildungsreise in allen Bildungsbereichen und in allen Lebensphasen. Dadurch wird ermöglicht, digitale Bildungsangebote und die dazugehörigen Verwaltungsleistungen zentral nutzbar zu machen und einen vereinfachten Zugang zu den Bildungsangeboten zu ermöglichen. Um eine sichere Vernetzung der Akteure auf allen Ebenen zu gewährleisten, sollen zu der Umsetzung der digitalen Vernetzungsinfrastruktur Regeln und Standards

[21] https://www.digitale-verwaltung.de/Webs/DV/DE/onlinezugangsgesetz/ozg-foederal/themenfelder/bildung/bildung-node.html

[22] https://www.bmi.bund.de/DE/themen/moderne-verwaltung/verwaltungsmodernisierung/onlinezugangsgesetz/onlinezugangsgesetz-node.html

etabliert werden. Außerdem erhält der Nutzer einen einheitlichen Zugang (Single Sign-On) zu verschiedenen Bildungsangeboten und Bildungsplattformen. Die digitale Vernetzungsinfrastruktur „Mein Bildungsraum“[23] besteht aus mehreren Komponenten: Digitale Identitäten, Ablage, Digitale Bildungsnachweise, Datenraum und Schaufenster. „Mein Bildungsraum“ ermöglicht die datenschutzkonforme Ablage von Bildungsnachweisen in der Ablage-App.

[23] https://www.meinbildungsraum.de/

4 Rechtlicher Rahmen

4.1 eIDAS-Verordnung, Vertrauensdienstegesetz und -verordnung

Die eIDAS-Verordnung[24], kurz eIDAS, schuf im Europäischen Wirtschaftsraum (EWR) einheitliche Vorgaben für vertrauenswürdige digitale Transaktionen auf Basis elektronischer Identifizierungsmittel (eID) sowie elektronischer Vertrauensdienste im Binnenmarkt. Als Identifizierungsmittel gelten hierbei z.B. der elektronische Personalausweis in Deutschland sowie dessen europäische Pendants. Gemäß Art. 6 eIDAS sollte jede öffentliche Stelle innerhalb der EU und EFTA jede notifizierte eID akzeptieren. Darüber hinaus sind beim Zugang zu elektronischen Diensten die notwendigen Vertrauensniveaus für den jeweils gewünschten Service durch die Institution zu beachten und zu prüfen, die den Service bereitstellt. Artikel 8 eIDAS unterscheidet die folgenden Vertrauensniveaus für Identifizierungsverfahren

- niedrig
- substanziell
- hoch

Detailliertere Anforderungen enthält der [Beschluss 2015/1506][25].

Die (qualifizierten) Vertrauensdienste umfassen elektronische Signaturen, Siegel, Zeitstempel, Verifikationsdienste (Prüfung von Signaturen, Siegeln etc.), Bewahrungsdienste (Beweiswerterhaltung), Einschreib- und Zustelldienste sowie Websitezertifikate. Durch die Zulassung z.B. von Server- und Fernsignaturen ohne Signaturkarte sowie von Siegeln (Signaturen für Organisationen) wird die Nutzung dieser Mittel erheblich erleichtert. Zudem definiert die eIDAS-Verordnung 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. Die eIDAS-Verordnung definiert für die Bewahrungsdienste gemäß Art. 34 eIDAS auch spezielle Anforderungen für die beweiswerterhaltende Aufbewahrung. Die Konformitätsbewertung der (qualifizierten) Vertrauensdienste obliegt akkreditierten Konformitätsbewertungsstellen unter Aufsicht der jeweiligen nationalen Aufsichtsstellen, in Deutschland der Bundesnetzagentur. Als technische Grundlage werden europäische Standards und Normen herangezogen. Den qualifizierten Vertrauensdiensteanbietern (VDA) obliegt die volle Haftung für ihre Leistungen sowie die Beweislast im Fehlerfall, verbunden mit entsprechenden Nachweis- und Meldepflichten. Das nachstehende Bild verdeutlicht dieses Vertrauensmodell der eIDAS-Verordnung:

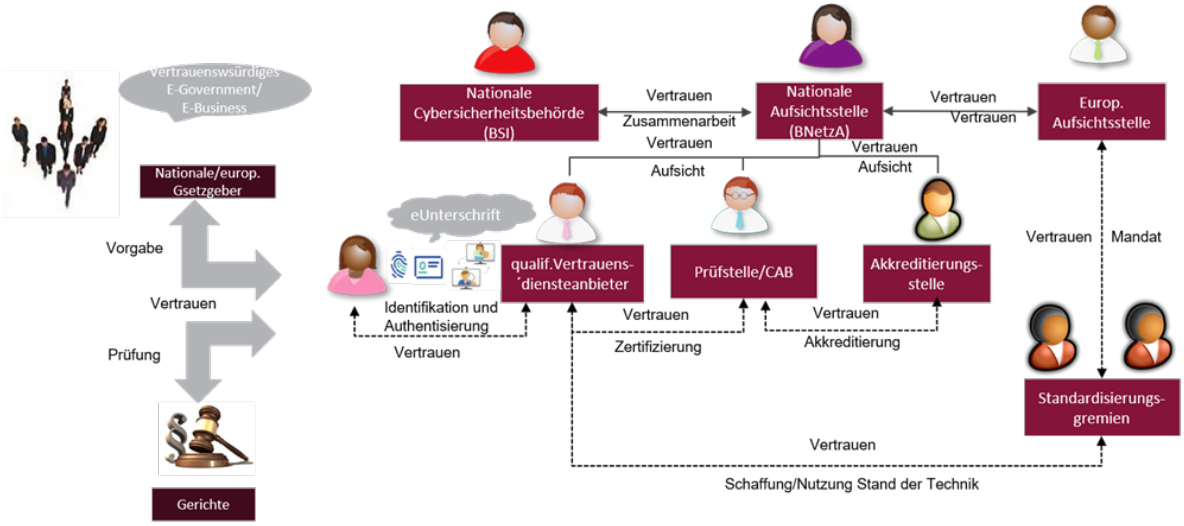

Abbildung 3 Vertrauensmodell der eIDAS-Verordnung

[24] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910
[25] https://eur-lex.europa.eu/eli/dec_impl/2015/1506/oj

Im Zuge der Umsetzung der eIDAS-Verordnung werden delegierte Rechtsakte bzw. Durchführungsrechtsakte erlassen. Diese enthalten Verweise auf die Standards und Spezifikationen von europäischen und internationalen Normungsorganisationen 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 gebührend berücksichtigt. Die genannten Standardisierungsgremien haben mit Mandat M416 der Europäischen Kommission die explizite Aufgabe, die rechtlichen Regelungen der eIDAS-Verordnung durch konkrete technische Standards zu untersetzen und so die Umsetzung durch Interoperabilität und Harmonisierung von Vertrauensdiensten und elektronischen Identifizierungsmitteln zu erleichtern. Die nachstehende Grafik zeigt das Zusammenwirken vom Rechtsrahmen mittels der eIDAS-Verordnung und den technischen Normen durch ETSI/CEN im Überblick [ENISA].

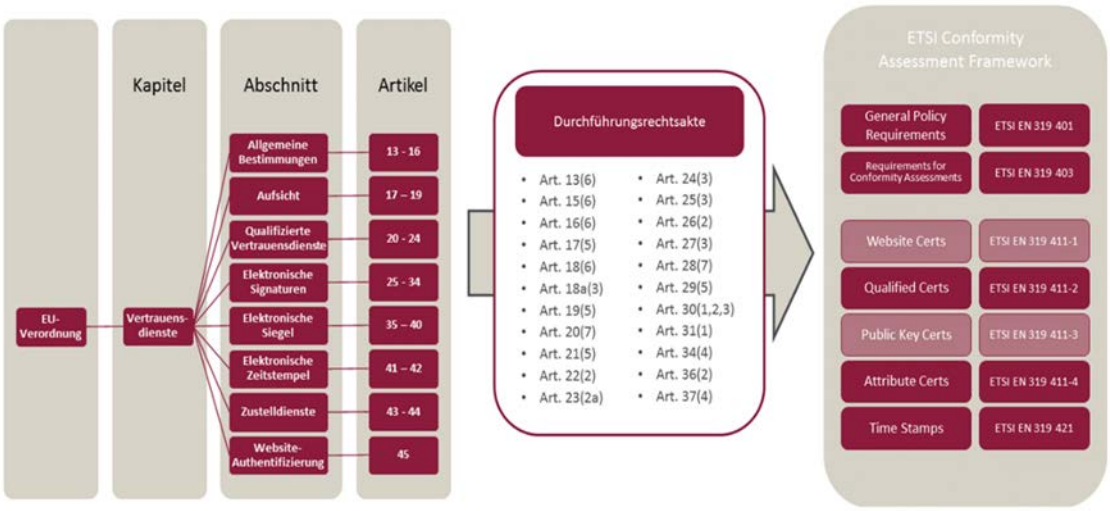

Abbildung 4 Beziehung eIDAS, Durchführungsrechtsakte und ETSI-Standardisierung

In Deutschland wird die wirksame Durchführung von eIDAS durch das Vertrauensdienstegesetz geregelt [VDG]. Dieses beinhaltet, neben Detaillierungen zu Haftungsregelungen und Vorgaben für (qualifizierte) Vertrauensdienste insbesondere die Beweiswerterhaltung signierter Dokumente in § 15.

Weitere Informationen finden sich zur eIDAS-Verordnung auf der Webseite des BSI[26] und zu den elektronischen Vertrauensdiensten auf der Webseite der Bundesnetzagentur[27].

4.2 E-Government-Gesetz und Onlinezugangsgesetz

Im Jahr 2013 wurde das Gesetz zur Förderung der elektronischen Verwaltung erlassen (**E-Government-Gesetz**, EGovG)[28]. Das EGovG (Bund) adressiert das Verwaltungshandeln des Bundes, auf Ebene der Länder existieren jeweils eigene E-Government-Gesetze (EGovG NRW für Nordrhein-Westfalen ab 2016, EGovG LSA ab 2017 für Sachsen-Anhalt uvm.).

Das EGovG (Bund) verpflichtet bspw. Bundesbehörden einen elektronischen Identitätsnachweis gemäß Personalausweisgesetz (oder gem. eID-Karte-Gesetz oder gem. Aufenthaltsgesetz) anzubieten. § 5 EGovG (Bund) ermöglicht elektronische Nachweise und § 6 elektronische Aktenführung. In § 7 wird das Ersetzende Scannen für Bundesbehörden ermöglicht. Demgemäß ist das Ersetzende Scannen möglich, sofern das gewählte Scanverfahren dem Stand der Technik mit der Maßgabe der inhaltlichen wie bildlichen

[26] https://www.bsi.bund.de/dok/7831030
[27] https://www.elektronische-vertrauensdienste.de/EVD/DE/Uebersicht_eVD/start.html
[28] https://www.bmi.bund.de/DE/themen/moderne-verwaltung/e-government/e-government-gesetz/e-government-gesetz-node.html

Übereinstimmung der digitalen Kopie entspricht (s.a. [TR-03138] (RESISCAN)). § 9a legt Basisdienste des Verwaltungsportals des Bundes fest, so u.a. den elektronischen Identitätsnachweis über das Nutzerkonto Bund (siehe auch unten) und Online-Antragsformulare. Das **Onlinezugangsgesetz (OZG)** wurde 2017 erlassen und hat das Ziel, den Onlinezugang zu Verwaltungsleistungen zu ermöglichen. Es verpflichtet Bund, Länder und Kommunen ihre Verwaltungsleistungen auch digital über sogenannte Verwaltungsportale anzubieten. Das OZG kennt insgesamt 14 Themenfelder, eines der Themenfelder ist „Bildung“[29] – es enthält die vier Lebenslagen „Schule“, „Studium“, „Berufsausbildung“ und „Weiterbildung“. Technische Komponenten im Rahmen des OZG sind der Portalverbund und die Nutzerkonten – die Nutzerkonten können Bürgerkonten für natürliche Personen sein (Lernende, Lehrende) als auch Organisationskonten für juristische Personen (Behörden etc.). Über das Postfach eines Nutzerkontos können elektronische Dokumente empfangen werden. Das BSI erstellt Technische Richtlinien (bspw. [TR-03107], [TR-03160]) und schafft damit eine sichere Basis und berät zu Fragen der Informationssicherheit.

Aktuell läuft ein Gesetzgebungsverfahren zur Änderung des OZG und des E-Government-Gesetzes, die Einführung des qualifizierten elektronischen Siegels zum Ersatz der Schriftform ist dabei Teil des aktuellen Entwurfs.

4.3 Fachgesetze

Für die Digitalisierung von Zeugnissen sind bestehende Formerfordernisse zu beachten. So stellen die Originale schulischer Zeugnisse wie auch Hochschulzeugnisse (Verleihung akademischer Grade) Urkunden dar und unterliegen teilweise dem Ausschluss elektronischer Form[30]. Auch Berufsausbildungszeugnisse dürfen explizit (noch) nicht in elektronischer Form ausgestellt werden[31]. Das Original wird aktuell in Papierform ausgestellt und dem Zeugnisinhaber übergeben. Seitens der Schulen resp. Universitäten werden Zweitschriften bzw. Entwürfe vorgehalten, die denselben Formerfordernissen wie das Original zu genügen haben. Bei Bedarf, auf Anfrage des Zeugnisinhabers beispielsweise bei Verlust des Originals, wird durch die verantwortliche Behörde auf Basis der Entwürfe eine erneute Ausfertigung vorgenommen.

Die Aufbewahrungsfristen für zeugnisrelevante Aufzeichnungen wie beispielsweise schulische oder universitäre Abschlusszeugnisse, Prüfungsakten etc. betragen zwischen 30 und 60 Jahren, beginnend i.d.R. ab dem 01.01. des Folgejahres des jeweiligen Abschlusses. Insbesondere Hochschulzeugnisse gelten in der Regel als dauerhaft archivwürdig. Die Dauer wird in länder- und hochschulspezifischen Regelungen definiert[32], dort kann ebenfalls festgelegt sein ob organisationseigene oder staatliche bzw. Landesarchive zuständig sind.

Ausschließlich amtliche Beglaubigungen von Zeugnissen, ausstellbar durch jede öffentliche Behörde können in rein digitaler Form erfolgen, allerdings nur unter Verwendung einer qualifizierten elektronischen Signatur (§ 33 VwVfG) gemäß eIDAS. Digitale „Ausfertigungen“ oder auch „elektronische Abbilder“ von Zeugnissen kommen bereits jetzt an einigen Stellen zum Einsatz.

[29] https://www.onlinezugangsgesetz.de/Webs/OZG/DE/themen/digitalisierungsprogramm-foederal/themenfelder/bildung/bildung-node.html

[30] Vgl. u.a. § 17 Hochschulgesetz des Landes Sachsen-Anhalt (HSG LSA). in der Fassung der Bekanntmachung vom 1. Juli 2021 sowie § 30 Hochschulgesetz (HochSchG) Rheinland-Pfalz vom 23. September 2020 Gesamtausgabe in der Gültigkeit vom 31.07.2021 bis 31.12.2022

[31] Vgl. Berufsbildungsgesetz (BBiG) vom 04.05.2020 §16

[32] Vgl. etwa Bayerisches Archivgesetz (BayArchivG) vom 22. Dezember 1989, Artikel 14

5 Fachliche Anforderungen

5.1 Dokumentation, Nachweis und Compliance

Vertrauenswürdigkeit geschäftsrelevanter Aufzeichnungen und Transaktionen erfordert in Deutschland und Europa vertrauenswürdige Dritte, die auf Basis gesetzlicher Vorgaben sowie geltender Standards und Normen agieren und wiederum durch vertrauenswürdige Dritte in einer Vertrauenskette transparent überprüft wie ermächtigt werden.

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

- Authentizität
- Integrität
- Nachvollziehbarkeit
- Vertraulichkeit
- Verfügbarkeit
- Verkehrsfähigkeit

Dabei stellen Integrität, Verfügbarkeit und Vertraulichkeit die Grundwerte aus Sicht der Informationssicherheit dar, aus denen die übrigen Anforderungen abgeleitet werden.

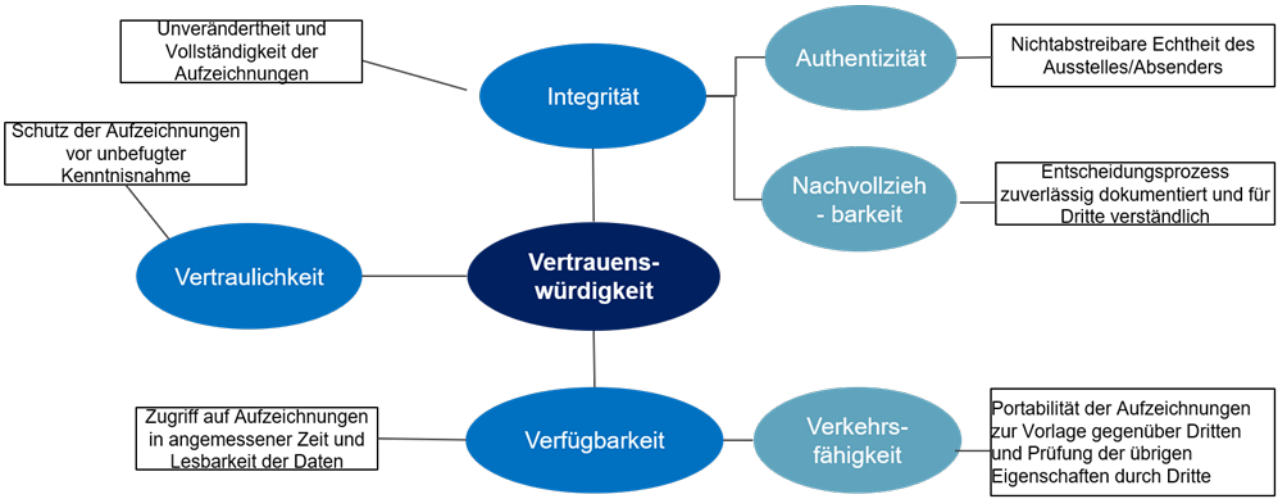

Abbildung 5 Signifikante Eigenschaften geschäftsrelevanter Dokumente

Ziel ist dabei die Erzeugung von Dokumenten, die als eindeutiger Nachweis von Geschäftsprozessen und geschäftlichen Entscheidungen gegenüber vertrauenswürdigen Dritten dienen können. Dabei dient die (elektronisch überprüfbare) digitale Information bereits als eindeutiger Bildungsnachweis. So kann z.B. eine Hochschulreife automatisiert durch ein System ausgelesen und das Vorliegen der Zulassungsvoraussetzungen für ein Studium festgestellt werden, so dass die Einschreibung in einer Universität komplett digital abgebildet werden könnte. Die für die Nachvollziehbarkeit wesentliche elektronische Aktenführung auch digitaler Zeugnisse sollte dabei den Vorgaben des Organisationskonzepts[33] elektronische Verwaltungsarbeit, so insbesondere dem Baustein E-Akte entsprechen.

[33] https://www.verwaltung-innovativ.de/DE/Verwaltungsdigitalisierung/orgkonzept_everwaltung/orgkonzept_everwaltung_node.html

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. Der Nachweis wird dabei an den Aufzeichnungen selbst geführt, was deren Verkehrsfähigkeit, also Übermittlung und Übertragbarkeit an die Prüfbehörde, Gericht, etc., erfordert. Vertraulichkeit erfordert einen wirksamen Datenschutz und geeignete Maßnahmen zur Informationssicherheit

Der Einsatz elektronischer Vertrauensdienste gemäß eIDAS wie (qualifizierter) elektronischer Signaturen, Siegel und Zeitstempel ermöglicht nach geltendem Recht den sicheren wie verkehrsfähigen Nachweis von Authentizität, Integrität digitaler Aufzeichnungen wie beispielsweise digitaler Zeugnisse am Dokument selbst. So weist die qualifizierte elektronische Signatur eindeutig den Aussteller eines Dokuments nach, das qualifizierte elektronische Siegel dessen Herkunft sowie der qualifizierte Zeitstempel die Integrität zu einem bestimmten Zeitpunkt (sogenannter Proof of Existence)[34].

In jedem Fall sind die Anforderungen an die Nachweisfähigkeit geschäftsrelevanter Aufzeichnungen bis zum Ablauf der geltenden Aufbewahrungsfristen, bei Zeugnissen bis zu 60 Jahren, nachzuweisen. Dies erfordert eine beweissichere Bewahrung nach dem Stand der Technik, die auch die Verfügbarkeit der Aufzeichnungen gewährleistet.

Die nachstehende Tabelle zeigt, welche eIDAS-Werkzeuge (Vertrauensdienste oder digitale Identitäten) zur Erfüllung der Anforderungen an ein ordnungsgemäßes Records Management herangezogen werden sollten.

Tabelle 1 Erfüllung der Anforderungen an ordnungsgemäßes Records Management mit eIDAS-Werkzeugen

Anforderung	***Werkzeug (Beispiel)***
Authentizität	Identifizierungsmittel (Vertrauensniveau hoch oder substanziell) (qualifizierte) elektronische Signatur oder Siegel (Erzeugung und Prüfung) Qualifizierte Bewahrungsdienste (Erhaltung)
Integrität	(qualifizierte) elektronische Signatur oder Siegel sowie qualifizierte Zeitstempel Qualifizierte Bewahrungsdienste (Evidence Records mit qualifiziertem Zeitstempel)
Nachvollziehbarkeit	Identifizierungsmittel (Vertrauensniveau hoch oder substanziell) Vollständige elektronische Akte Qualifizierte Bewahrungsdienste
Vertraulichkeit	Datenschutzkonzept, Datenschutzfolgeabschätzung Verfahrensbezogenes Sicherheitskonzept
Verfügbarkeit	Qualifizierte Bewahrungsdienste
Verkehrsfähigkeit	Qualifizierte Bewahrungsdienste (unter Nutzung selbsttragender AIP)

[34] https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

5.2 IT-Grundschutz

Der IT-Grundschutz[35] ist ein solides Fundament für die erforderliche Informationssicherheit einer digitalen Zeugnis-Infrastruktur. Der IT-Grundschutz verfolgt dabei einen ganzheitlichen Ansatz und betrachtet neben technischen Aspekten auch infrastrukturelle, organisatorische und personelle Themen. Es gibt die BSI-Standards:

- 200-1: Managementsystem für Informationssicherheit (ISMS)
- 200-2: Methodik
- 200-3: Risikomanagement
- 200-4: Business Continuity Management und 100-4: Notfallmanagement

Die grundlegende Veröffentlichung ist das IT-Grundschutz-Kompendium [BSI Grundschutz], es beschreibt in Form von Bausteinen mögliche Gefährdungen und zugehörige Sicherheitsanforderungen. Die Themen reichen dabei von Anwendungen (APP) über Netze (NET) und vielen weiteren bis IT-Systeme (SYS).

Mithilfe der Methodik nach IT-Grundschutz können Sicherheitskonzepte einfach erstellt werden. Einen ersten Einstieg zum Aufbau eines ISMS bietet der „Leitfaden zur Basis-Absicherung nach IT-Grundschutz“[36]. IT-Grundschutz-Profile[37] sind Schablonen für bestimmte Anwendungsfälle, quasi Musterszenarien für Anwendungsfelder. Es gibt bereits ein IT-Grundschutz-Profil für Hochschulen.

[35] https://www.bsi.bund.de/grundschutz.html
[36] https://www.bsi.bund.de/dok/10051454
[37] https://www.bsi.bund.de/dok/it-grundschutz-profile

6 Erzeugung und Ausstellung digitaler Zeugnisse

6.1 Organisatorische Aspekte

Die Einführung digitaler Zeugnisse sollte grundsätzlich im Kontext der gesamten Digitalisierung der jeweiligen Bildungseinrichtung(en) betrachtet werden. Die Einführung digitaler Zeugnisse sollte zudem im Zusammenhang mit der elektronischen Akte (sofern verfügbar) und beweissicheren Bewahrung betrachtet werden, da nur so die Dokumentations- und Nachweispflichten erfüllt werden können.

Insofern empfiehlt es sich insbesondere die folgenden Aspekte zu betrachten:

- Harmonisierung der Zugangs-/Kommunikationskanäle für Antragsstellung und Bescheid mit den übrigen digitalen Leistungen der Bildungseinrichtung
- Harmonisierung der Verfahren zur Identifizierung und Authentisierung der Nutzer
  - Zugang via Nutzerkonten
  - Zugang über lokale Services
  - Festlegung der notwendigen Vertrauensniveaus
- Einbindung in das elektronische Dokumentenmanagement bzw. die elektronische Aktenführung und beweissichere Bewahrung, eventuell Anbindung „ersetzendes Scannen“
- Integration in ganzheitliches Vorgehen zur Nutzung qualifizierter elektronischer Signaturen, Siegel, Zeitstempel: Prüfung weiterer Anwendungsfälle von Signaturen und Siegeln und Integration der Vertrauensdienste in die jeweiligen Fachverfahren
- Festlegung der notwendigen Rollen, Verantwortlichkeiten und internen Regelungen
- Aussonderung, Bewahrung und digitale Langzeitarchivierung

Die nachstehende Grafik zeigt ein mögliches Zielbild beispielhaft.

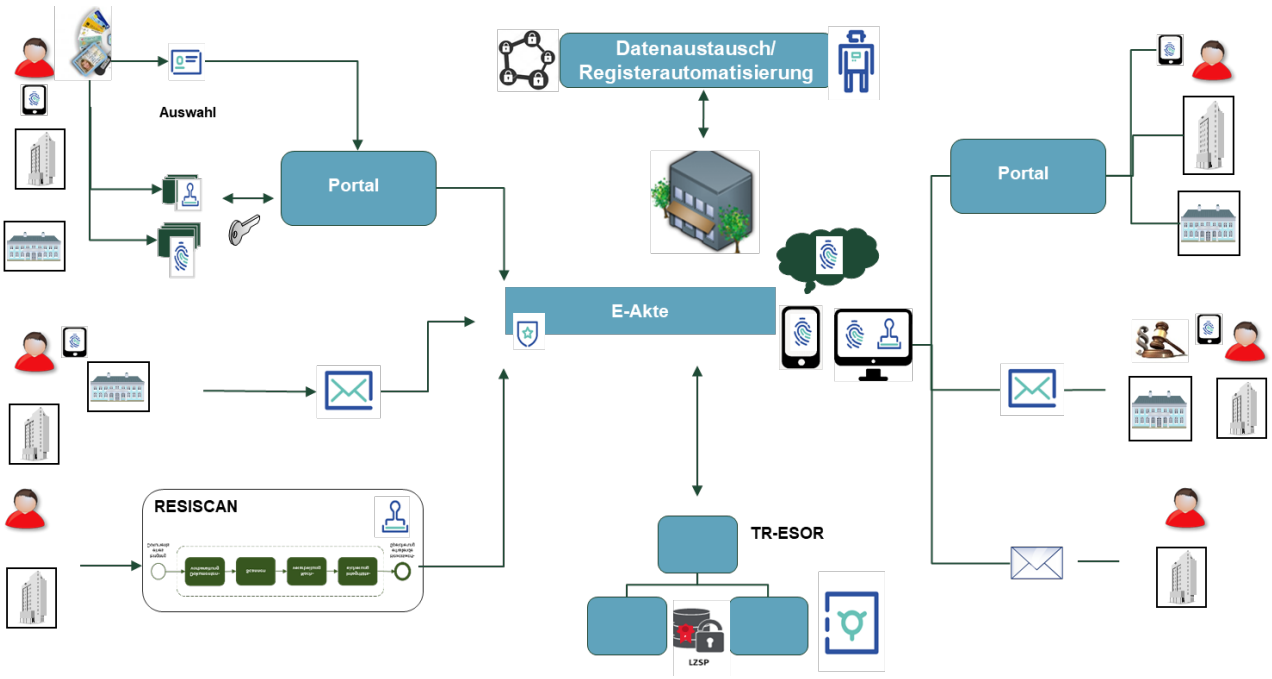

Abbildung 6 Beispiel einer Gesamtarchitektur zur Digitalisierung

Hinsichtlich der Projektorganisation bietet sich eine Orientierung am Projektleitfaden des Organisationskonzepts elektronische Verwaltungsarbeit an[38]. Darüber hinaus sollen klare Rollen und Verantwortlichkeiten benannt und gemeinsam mit folgenden beispielhaften Aspekten in Richtlinien definiert bzw. in vorhandene integriert werden:

- Erstellung, Verwaltung, Speicherung der Zeugnisse
- Identifizierung und Authentisierung
- Informationssicherheit und Datenschutz
- IT-Betrieb

6.2 Technische Aspekte

Hinsichtlich der technischen Ausgestaltung digitaler Zeugnisse also deren Datenaustausch- und Dateiformaten und den kryptographischen Sicherungsmitteln bestehen jeweils verschiedene Optionen. Diese werden im Folgenden prägnant dargestellt.

6.2.1 Datenaustausch- und Dateiformate

Grundsätzlich sind aktuell die folgenden Datenaustauschformate für Ausstellung und Austausch digitaler Zeugnisse etabliert. Die Liste ist nicht abschließend, es sind weitere Formate sind denkbar.

Dateiformate (allgemeine):

JSON: Das im Standard RFC 8259 definierte JSON (JavaScript Object Notation) Format ist ein Datenformat, welches in Textform Daten hält und für den Datenaustausch konzipiert ist. Es ist dabei anwendungsunabhängig und wird von den meisten Programmiersprachen unterstützt. Dabei definiert JSON einen kleinen Satz von Formatierungsregeln zur Darstellung der Datensätze, welche von einem Parser gelesen werden können. Dadurch, dass JSON keine Vorgaben macht, was gespeichert wird, sollte hierfür ein einheitliches Schema definiert werden, nach dem alle Anwendungen die JSON Formate richtig interpretieren. JSON ist ein etabliertes Austauschformat. Mit JAdES liegt auch ein Standardformat für (qualifizierte) elektronische Signaturen und Siegel in Europa vor, zudem wird als Schnittstellenformat breit eingesetzt.

XML: XML (Extensible Markup Language) ist ein weiteres Datenaustausch- und Speicherformat, welches von W3C standardisiert wurde und dessen Nutzung im Zusammenhang mit IETF-Protokollen über das RFC 3470 definiert ist. XML ist eine hierarchische Markup-Sprache. Sie verwendet öffnende und schließende Tags, um Daten zu definieren. Sie dient der Speicherung und dem Austausch von Daten und wird aufgrund ihrer extremen Flexibilität für alles von der Dokumentation bis zur Grafik verwendet. Im Zusammenhang mit digitalen Zeugnissen wird XML in einigen Implementierungen verwendet, um Schlüssel-Wert-Paare und Signaturen zu speichern. XML ist als Austauschformate seit langen Jahren etabliert, so beruhen bspw., die Formate nach [TR-03125], XÖV oder auch XFDU auf XML. Ebenso liegt mit XAdES auch ein Standardformat für (qualifizierte) elektronische Signaturen und Siegel in Europa vor

PDF/A-2: Das PDF/A Dateiformat ist speziell für die Langzeitarchivierung von PDF-Dokumenten ausgelegt. Der PDF/A Standard basiert dabei auf dem ISO-19005 bzw. ISO 32000-1 Standard und gibt einige Restriktionen für die Langzeitarchivierung vor. Ab der Version PDF/A-2 ist der Standard mit PAdES konform. PDF/A kann als Datenaustausch- und Speicherformat verwendet werden. PDF/A ist als Archivierungsformat weltweit etabliert und wird bspw. auch in der BSI TR-3125 Anhang F empfohlen. Das Bundesarchiv empfiehlt aus archivarischer Sicht PDF/A-2 (idealerweise PDF/A-2a)[39].

[38] https://www.verwaltung-innovativ.de/SharedDocs/Publikationen/Organisation/projektleitfaden.html?nn=8886362

[39] https://www.bundesarchiv.de/DE/Content/Downloads/Anbieten/informationsforum-2019-empfehlungen-anwendung-pdfa-versionen.pdf?__blob=publicationFile

Datenaustauschformate (domänenspezifische):

XBildung[40]: Ein übergreifender Datenaustauschstandard für das Bildungswesen (in Deutschland) basierend auf einer einheitlichen und herstellerneutralen Spezifikation. Methoden und Teile von XÖV (XÖV = XML in der öffentlichen Verwaltung) werden übernommen. Es gibt die beiden Fachstandards XHochschule und XSchule sowie das neue Fachmodul XBerufsbildung. Beispielsweise kennt XBildung natürliche Personen/Lernende, XSchule kennt „Schüler" und XHochschule kennt „Studierende".

EMREX mit ELMO XML: Ein bereits bestehender Standard für den internationalen Transfer von Studentendaten ist EMREX. EMREX nutzt dafür den Datenstandard namens ELMO. EMREX ist schon in einigen Ländern der EU verbreitet und bietet in Ländern wie Finnland auch schon digitale Zeugnisse für Studierende an. Das ELMO XML-Format basiert auf dem CEN EN 15981-2011 EuroLMAI Standard. Das ELMO Format ist ein Datenmodell, welches hauptsächlich Hochschulabschlüsse und Leistungsnachweise von Hochschulen beschreibt. Aber auch Zeugnisse der sekundären Bildung (wie z.B. Abiturzeugnisse und ähnliches) werden unterstützt. Die Authentifizierung der Studierenden wird momentan für jedes Land individuell implementiert und angebunden.

6.2.2 Erzeugung und Nutzung kryptographischer Sicherungsmittel

Die Nutzung kryptographischer Sicherungsmittel wie (qualifizierter) elektronischer Signaturen (qeS), Siegel (qeSi) und Zeitstempel ermöglicht nach geltendem Recht einen eindeutigen Nachweis der Authentizität und Integrität an den digitalen Dokumenten selbst und damit in verkehrsfähiger Form. Sie ermöglichen zudem die Erzielung eines höheren Beweiswerts für die anwendende Organisation und damit signifikante Vorteile im Nachweis digitaler Dokumente wie z.B. Zeugnisse. Grundsätzliche Empfehlungen zu kryptographischen Kommunikationsverfahren als auch der jeweiligen Schlüssellängen geben die [TR-03116] Teil 4 und die [TR-02102].Neben (qualifizierten) elektronischen Signaturen und Siegeln können auch fortgeschrittene eingesetzt werden. Dabei ist jedoch zu beachten, dass nur die qeS die Schriftform und nur das qeSi den eindeutigen Herkunftsnachweis einschließlich des erhöhten Beweiswerts nach Art. 35 eIDAS beinhaltet. Empfänger eines digitalen Zeugnisses erfahren so, wer ein digitales Zeugnis ausgestellt hat (welche natürliche und/oder juristische Person, d.h. welche Behörde, welche Bildungseinrichtung).

Es kann jeder europäische qualifizierte Vertrauensdiensteanbieter (VDA) verwendet werden. Eine Übersicht der zugelassenen VDA bietet der EU/EEA Trusted List Browser[41] und die eIDAS Map[42].

Die nachstehende Tabelle zeigt die wesentlichen Unterschiede zwischen Signaturen, Siegeln und Zeitstempeln:

Tabelle 2 Vergleich Signatur, Siegel, Zeitstempel

Lösung	***Eigenschaften***
(qualifizierte) elektronische Signatur	Beruht auf (qualifiziertem) Zertifikat einer natürlichen Person Ersetzt die handschriftliche Unterschrift sowie die Schriftform
(qualifiziertes) elektronisches Siegel	Beruht auf (qualifiziertem) Zertifikat einer juristischen Person Nachweis der Herkunft elektronischer Dokumente
(qualifizierter) elektronischer Zeitstempel	Nachweis der Herkunft elektronischer Dokumente Beruht auf vertrauenswürdiger Zeitquelle Nachweis, dass ein Dokument zum angegebenen Zeitpunkt integer vorlag (sog. Proof of Existence) Enthält fortgeschrittene Signatur des qualifizierten Vertrauensdienstes

[40] https://xbildung.de/
[41] https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home
[42] https://www.eid.as/tsp-map/#/

Erzeugung (qualifizierter) elektronischer Signaturen, Siegel und Zeitstempel

Die Erzeugung (qualifizierter) elektronischer Signaturen und Siegel erfolgt auf Basis qualifizierter Zertifikate. Diese werden ausschließlich durch qualifizierte Vertrauensdiensteanbieter (VDA) erzeugt. Hierzu ist die eindeutige Identifizierung

- bei qeS: des Unterzeichners, also der natürlichen Person
- bei qeSi: des Siegelinhabers, also der juristischen Person

durch den VDA notwendig. Die Identifizierung der natürlichen Person kann dabei digital insbesondere durch eine notifizierte europäische eID sowie weitere Verfahren erfolgen.

Das ausgestellte Zertifikat wird anschließend abgelegt:

- In einem sicheren Hardware-Sicherheits-Modul (HSM)[43] beim VDA (für eine Fernsignatur oder Fernsiegel)
- In einem sicheren Hardware-Sicherheits-Modul (HSM) des VDA in der Umgebung der anwendenden Organisation (für eine Signierung in der Umgebung der Organisation)
- Auf einer Smartcard unter Bereitstellung des Kartenlesers (für eine Signierung in der Umgebung der Organisation)

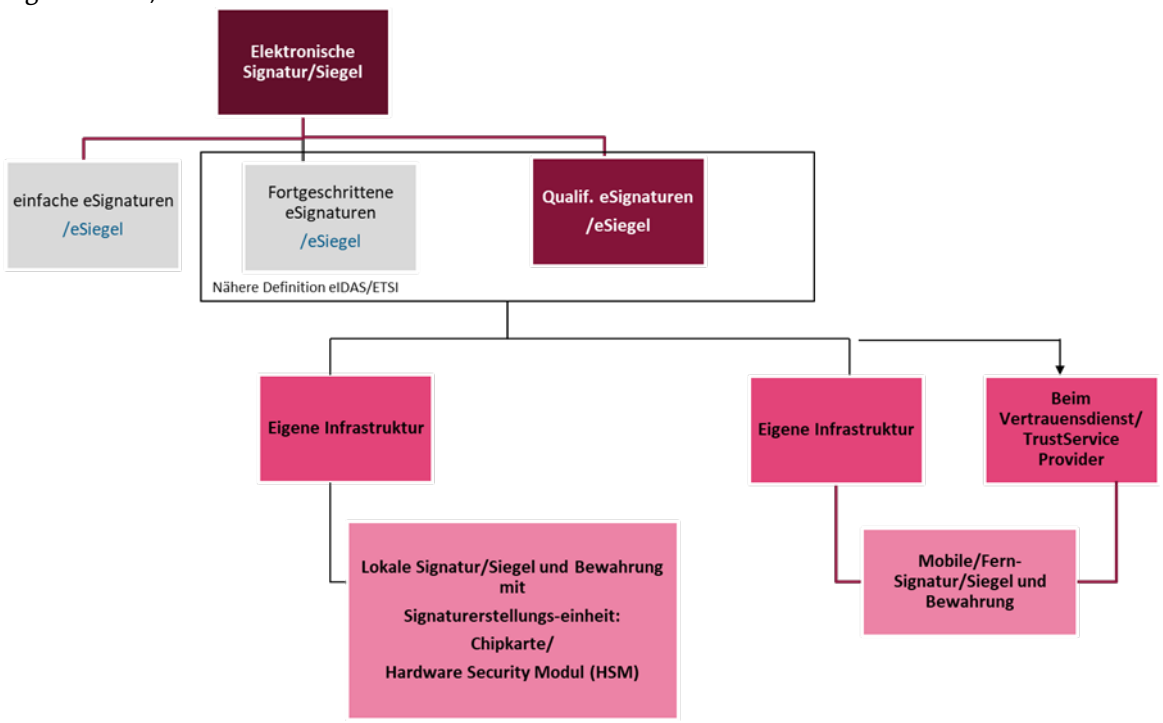

Abbildung 7 Varianten zur Erzeugung (qualifizierter) elektronischer Signaturen und Siegel

Technisch wird im Kern über das zu signierende Dokument ein Hashwert erzeugt und dieser mit dem (qualifizierten) Zertifikat verschlüsselt. Hierzu ist eine starke Zwei-Faktor-Authentisierung (2FA) durch den Zertifikatsinhaber notwendig. Softwareseitig wird eine marktübliche Signatursoftware (im Falle des HSM/der Signaturkarte in anwendender Organisation) oder Signaturplattform des qualifizierten VDA (im Falle der Fernsignatur/des Fernsiegels) benötigt.

Damit ermöglicht eIDAS auch eine nutzerfreundliche Fernsignatur ohne aufwändige Signaturkarten und Kartenleser. Abhängig vom VDA kann das zu signierende Dokument auf datenschutzkonformem, sicherem

[43] Zertifiziert gem. CC-PP nach CEN EN 419 241, Zertifizierung ist Bedingung für die Zulassung des Vertrauensdiensteanbieters als qualifizierter VDA

wie zertifiziertem Weg zur Signaturerstellung hochgeladen oder nur eine Hashsignatur erzeugt werden. Im Falle der qeS wird ein qualifiziertes Zertifikat je Unterzeichner, im Falle des qeSi ein qualifiziertes Zertifikat je Organisation benötigt. Es ist insofern empfehlenswert zu prüfen, ob für digitale Zeugnisse in jedem Fall eine qualifizierte Signatur zum Ersatz der Schriftform notwendig oder das qualifizierte elektronische Siegel ausreichend ist

Hinsichtlich des Einsatzes (qualifizierter) elektronischer Signaturen, Siegel und Zeitstempel ist zu beachten:

- Es kann jeder qualifizierte Vertrauensdienst in Europa verwendet werden. Alle qualifizierten VDA finden sich in der Vertrauensliste der Europäischen Kommission: https://eidas.ec.europa.eu/efda/tl-browser
- jeder qualifizierte Vertrauensdienst haftet vollständig für die von ihm angebotenen (qualifizierten) Vertrauensdienste, die Beweislast liegt beim qualifizierten VDA, was für den Anwender zusätzliche Sicherheit birgt

Es gelten derzeit die folgenden Standardformate für (qualifizierter) elektronischer Signaturen, Siegel, die durch die VDA verwendet werden und mit jeder marktüblichen Signatursoftware erzeug- und prüfbar sind.

Tabelle 3 Standardformate für (qualifizierte) elektronische Signaturen und Siegel

Format	***Standard***
CAdES (CMS-Basiert)	ETSI EN 319 122-1
XAdES (XML-basiert)	ETSI EN 319 132-1
PAdES (PDF-basiert)	ETSI EN 319 142-1
ASiC (ZIP-Container)	ETSI EN 319 162-1

Beim Einsatz (qualifizierter) elektronischer Signaturen, Siegel und Zeitstempel sollte berücksichtigt werden, dass jede öffentliche Stelle ohnehin jede mindestens fortgeschrittene elektronische Signatur, Siegel und Zeitstempel jedes europäischen qualifizierten Vertrauensdiensteanbieters annehmen und prüfen sollte. Da hierfür ohnehin die nötige Technik aufzubauen ist, wird, mit Blick auf den absehbar hohen Beweiswert, die Nutzung kryptographischer Sicherungsmittel für digitale Zeugnisse empfohlen.

Details zu regulatorischen und technischen Fragen der Signaturerzeugung und -Prüfung resp. qualifizierten Vertrauensdiensten in eIDAS enthalten die [BSI Leitlinie Signatur] sowie die Studie der [ENISA].

7 Digitalisierung papierner Zeugnisse

Elementare Grundlage elektronischer Prozesse ist die Digitalisierung papierner Aufzeichnungen. Mit Blick darauf, dass Verwaltungsakten insbesondere bei Massenakten (z.B. Justizakten, Antragsunterlagen etc.) erfahrungsgemäß schnell einen Umfang von mehreren Regalkilometern annehmen, ist die Papierlagerung allein aus Kostensicht kritisch zu betrachten. Die Digitalisierung sollte also auch die anschließende Vernichtung der papiernen Originale umfassen. Dieses ersetzende Scannen ist gemäß E-Government-Gesetzen von Bund und Ländern möglich, sofern es nach dem Stand der Technik erfolgt. Als Stand der Technik gilt die [TR-03138] (RESISCAN)[44] des BSI im jeweils aktuellen Stand.

Sofern ein ersetzendes Scannen papierner Zeugnisse durch öffentliche Stellen erfolgt, sollte dieses gemäß [TR-03138] erfolgen, dabei sind grundsätzlich die folgenden Schritte zu beachten:

1. Erstellung einer Strukturanalyse anhand des definierten Scansystems
2. Erstellung einer Schutzbedarfsanalyse der zu scannenden Dokumente
3. Ableitung der Sicherheitsmaßnahmen gemäß TR RESISCAN

Die Ergebnisse werden in Verfahrensdokumentation und Scankonzept zusammengefasst.

Die Nutzung kryptographischer Sicherungsmittel wie (qualifizierter) elektronischer Signaturen, Siegel und Zeitstempel ermöglicht auch beim ersetzenden Scannen eine möglichst hohe Nachweisfähigkeit. Abhängig vom Schutzbedarf des Scanguts ist deren Einsatz gemäß TR ohnehin notwendig.

Die Einführung des ersetzenden Scannens sollte im Verbund mit der elektronischen Akte oder einem anderen weiterverarbeitenden IT-Verfahren und im Zusammenhang mit der beweiswerterhaltenen Bewahrung gemäß [TR-03125] erfolgen. Nur so kann eine langfristige Nachweisfähigkeit nach dem Stand der Technik gewährleistet werden. Durch die Zertifizierungsverfahren für Scanprozesse gemäß [TR-03138] und Produkte zur Beweiswerterhaltung gemäß [TR-03125], wird die Umsetzung des Stands der Technik transparent - für Anwender, Prüfbehörden und Dritte.

[44] https://www.bsi.bund.de/resiscan

8 Digitale Bildungsnachweise mit optisch verifizierbarem kryptographischem Schutz (Digitale Siegel)

Zahlreiche Verwaltungsprozesse in Deutschland resultieren in der Erstellung von Bescheiden, Zertifikaten oder sonstigen Dokumenten. Damit solche Dokumente als Nachweis gegenüber Dritten verwendet werden können, wurden sie traditionell mit Dienstsiegeln und/oder Unterschriften der Bearbeitenden versehen. Die handschriftliche Unterschrift kann in vielen Bereichen schon seit langem durch eine qualifizierte elektronische Signatur ersetzt werden, und die mit der eIDAS-Verordnung [eIDAS-VO] EU-weit eingeführten qualifizierten Siegel, die einen elektronischen Herkunftsnachweis darstellen, verfügen über dieselben mathematischen Eigenschaften.

Mit fortgeschrittenen oder qualifizierten elektronischen Signaturen oder Siegeln lässt sich die Authentizität und Integrität elektronischer Dokumente jederzeit überprüfen, solange sie in der ursprünglichen Form elektronisch vorliegen. Werden die Dokumente in Papierform dargestellt oder auf einem mobilen Endgerät vorgezeigt, kann die Integritätssicherung nicht mehr überprüft werden, da durch den Medienbruch die Eigenschaften verloren gehen. Um dies zu vermeiden, wurden optisch verifizierbare digitale Siegel[45] entwickelt, die die wesentlichen Daten eines Nachweises in strukturierter Form und kryptographisch gesichert enthalten.

Mittels optisch verifizierbarer digitaler Siegel gemäß TR-03171 in Form von Barcodes lassen sich Bildungsnachweise auch optisch auf Echtheit und Unverfälschtheit prüfen. Die wesentlichen Daten eines Dokuments werden in dem optischen digitalen Siegel codiert und mit einem Integritätsschutz in Form eines elektronischen Siegels versehen. Wurde bei der Erstellung des optisch verifizierbaren digitalen Siegels auf dem Bildungsnachweis ein entsprechendes Zertifikat verwendet, so handelt es sich bei dem geschützten Datensatz um ein mit einer qualifizierten elektronischen Signatur bzw. einem qualifizierten elektronischen Siegel versehenes Dokument. Die Prüfung des optischen Siegels erfolgt mit Hilfe einer Smartphone App, welche durch das Scannen des Barcodes auf dem Endgerät die zuvor codierten Inhaltsdaten ausgelesen werden und auf Authentizität und Integrität überprüft werden kann. Die App hat Zugriff auf die zuvor hinterlegten Profile in der Profilverwaltung sowie den Zertifikaten in der Zertifikatsverwaltung und kann so das optisch verifizierbare digitale Siegel auslesen.

[45] https://www.bsi.bund.de/dok/digitale-siegel

9 Identifizierung und Authentisierung

In verschiedenen Phasen des Lebenszyklus eines digitalen Zeugnisses ist die Identifizierung und Authentisierung von Akteuren erforderlich, vor allem bei diesen:

- Bei der Beantragung eines digitalen Zeugnisses, von der antragstellenden Person
- Bei der Erstellung des digitalen Zeugnisses als unterzeichnende (siegelnde) Person (die im Auftrag der Bildungseinrichtung agiert)
- Die Übergabe des digitalen Zeugnisses erfolgt ebenfalls nur an berechtigte Personen die sich erfolgreich authentisieren können.

Im Zeitalter der papiernen Dokumente konnte dies einfach durch das Prüfen des Ausweises geschehen. Zum Ausstellen digitaler Zeugnisse benötigt es jetzt auch Methoden, Personen digital zu identifizieren und authentisieren. Je nach Phase und verwendeter Technologie werden eventuell unterschiedliche Möglichkeiten zur Identifizierung und Authentisierung verfügbar sein, so kann beispielsweise ein Nutzerkonto an dessen Postfach ein Zeugnis übermittelt wurde vielleicht eine Zwei-Faktor-Authentisierung mit einem Token anbieten und für den Fall dass ein digitales Zeugnis auf dem klassischen Wege qualifiziert elektronisch signiert wird verwendet die signierende Person vielleicht eine Signaturkarte mit einer PIN als Authentisierungsmittel.

Entsprechend Artikel 8 der Verordnung (EU) Nr. 910/2014 [eIDAS-VO] gibt es die Sicherheitsniveaus niedrig, substanziell und hoch. Diese sind in der Durchführungsverordnung (EU) 2015/1502 weiter ausgeführt und im Anhang ebendieser Durchführungsverordnung finden sich entsprechende technische Spezifikationen und Verfahren. Die Technische Richtlinie [TR-03107] Teil 1 führt entsprechend aus die Vertrauensniveaus (engl. „assurance level“) und setzt in Beziehung zu den Sicherheitsniveaus gemäß IT-Grundschutz (IT-GS):

- **Normal** (in etwa das Sicherheitsniveau normal gemäß IT-GS)
- **Substantiell** (zwischen den Sicherheitsniveaus normal und hoch gemäß IT-GS)
- **Hoch** (in etwa das Sicherheitsniveau hoch gemäß IT-GS)

Die Festlegung, welches Vertrauensniveau für die Ausstellung digitaler Zeugnisse oder digitaler Bildungsnachweise benötigt wird, obliegt der zeugnisausstellenden Einrichtung bzw. ergibt sich aus deren rechtlichen Vorgaben. Unterstützend kann das „Praxistool Vertrauensniveau“[46] herangezogen werden. Wie bereits in Kapitel 2.3 beschrieben ist es möglich dass gerade digitale Abschlusszeugnisse ein mindestens substantielles oder auch ein hohes Vertrauensniveau erforderlich machen können.

Möglichkeiten zur Identifizierung und Authentisierung sind etwa die Folgenden, mit dem jeweiligen möglichen Vertrauensniveau (VN):

- Nutzername/Passwort: VN normal
- Elektronischer Identitätsnachweis, auch bekannt als Online-Ausweisfunktion (eventuell in Verbindung mit einem Nutzerkonto des Bundes oder eines Bundeslandes): VN hoch
- Smart-eID, online ausweisen mit dem Smartphone ohne Karte: in Kürze - noch kein VN
- EUDI-Wallet[47], online ausweisen mit der EUDI-Wallet: geplant - VN bis hoch

Weitergehende Informationen finden sich auf der Webseite des BSI beim Thema Staat und Verwaltung > „elektronische Identitäten“[48].

[46] https://vn-check.ozg-umsetzung.de/index.php/12295
[47] https://www.personalausweisportal.de/SharedDocs/kurzmeldungen/Webs/PA/DE/2023/11_digitale_brieftasche.html
[48] https://www.bsi.bund.de/dok/6615870

10 Validierung digitaler Zeugnisse

10.1 Grundsatz

Im Zusammenhang mit digitalen Zertifikaten kann die Validierung zwei Bereiche betreffen. Der erste ist die Validierung der Datei, sei es eine PDF-, XML- oder JSON-Datei, um zu prüfen, ob sie mit der richtigen Syntax gemäß den allgemeinen Spezifikationen von z.B. PDF, XML bzw. JSON erstellt wurde. Syntaktisch wird dann validiert gegen ein vorhandenes Schema, im Fall von XML-basierten Zeugnissen kann XBildung (bzw. XSchule oder XBerufsbildung) zum Einsatz kommen. Moderne Validierungssoftware verfügen über integrierte Validatoren für die Syntax der zu prüfenden Daten. Der zweite Bereich ist die Validierung von elektronischen Signaturen, Siegeln und Zeitstempeln.

Bei digitalen Zeugnissen basiert die Validierung von elektronischen Signaturen und Siegeln auf der Public-Key-Kryptografie. Das Zeugnis wird mit einem privaten Schlüssel eines öffentlichen/privaten Schlüsselpaares digital signiert, wobei der öffentliche Schlüssel der validierenden Partei bekannt ist. Der öffentliche Schlüssel kann auf verschiedene Weise veröffentlicht werden: Er kann direkt in dem signierten Dokument erwähnt werden oder in einem X.509-Zertifikat enthalten sein. In allen Fällen sollte die validierende Partei Zugriff auf den öffentlichen Schlüssel haben, um die erstellte Signatur zu validieren.

Schließlich kann bei einigen Zeugnissen ein qualifizierter Zeitstempel erforderlich sein, um sicherzustellen, dass das digitale Dokument vor einem bestimmten Datum erstellt und seitdem nicht geändert wurde. In diesem Fall ist die Verwendung einer qualifizierten Zeitstempelstelle (Qualified Time Stamp Authority) als vertrauenswürdige dritte Partei erforderlich.

10.2 Validierung kryptographischer Sicherungsmittel

Die Prüfung (qualifizierter) elektronischer Signaturen, Siegel und Zeitstempel kann zum einen lokal in der Behörde oder durch einen qualifizierten Validierungsdienst erfolgen. Sofern die Validierung als Dienst für Dritte z.B. durch einen öffentlichen IT-Dienstleister vorgenommen wird, sollte dieser ein qualifizierter Validierungsdienst sein.

Die Validierung umfasst grundsätzlich folgende beiden Schritte

- Mathematische Gültigkeit, d.h. Integritätsprüfung
  - Prüfung des Hashs der Signatur gegen den Hash des Dokuments: Beim ersten Schritt wird die mathematische Gültigkeit der Signatur zum Nachweis der Integrität geprüft.
- Gültigkeit der Zertifikate
  - Prüfung, ob das zur Signaturerstellung verwendete Zertifikat zum Referenzzeitpunkt, d.h. bei einer qualifizierten elektronischen Signatur gemäß Kettenmodell (Ausnahmefall) der Zeitpunkt der Signaturerstellung und bei einer zur Authentifizierung verwendeten Signatur gemäß Schalenmodell (Regelfall) der aktuelle Zeitpunkt, gültig ist.
  - Korrektheit des Verwendungszwecks der Zertifikate: Für die Gültigkeit und Korrektheit eines Zertifikats wird geprüft, ob die durch den Aussteller des Zertifikats gesetzte Signatur bzw. Siegel gültig ist, ob Zertifikatserweiterungen gemäß [eIDAS-VO], Artikel 38 Absatz 3 und der Verwendungszweck des Zertifikats richtig gesetzt wurden, ob ein Zertifikatspfad zu einem vertrauenswürdigen Wurzel-Zertifikat oder Vertrauensanker gebildet werden kann und ob das Zertifikat nicht gesperrt wurde (siehe TR-ESOR).
  - Prüfung der behördlichen/institutionellen Zuständigkeit und Ausstellbefugnis: besonders bei digitalen Zeugnissen kann zusätzlich gefordert sein zu prüfen, das die signierende/siegelnde Stelle tatsächlich diese Art von Zeugnis oder Bildungsnachweis ausstellen darf. Hierfür ist jedoch ein

zusätzlicher Dienst erforderlich der zuverlässig darüber Auskunft geben kann ob ein konkretes Zertifikat das einer öffentlichen Bildungseinrichtung ist (Stichwort Bildungsinstitutionsverzeichnis).

Nur mit einer erfolgreichen Validierung liegt eine gültige qeS/qeSi vor. Details zur Validierung finden sich in der Leitlinie für digitale Signatur-/Siegel-, Zeitstempel- formate sowie technische Beweisdaten (Evidence Record) [BSI Leitlinie Signatur] sowie in der Technischen Richtlinie [TR-03125] (TR-ESOR), Anlage TR-ESOR-M.2: Krypto-Modul.

10.3 Validierung der Datenformate

XML

Eine XML-Datei mit einer Signatur folgt einer Signatursyntax und -verarbeitung, die in IETF RFC 3275 standardisiert ist. XML-Signaturen werden über eine Umleitung auf beliebige digitale Inhalte (Datenobjekte) angewendet. Datenobjekte werden verarbeitet, der resultierende Wert wird in ein Element (mit anderen Informationen) eingefügt und dieses Element wird dann verarbeitet und kryptographisch signiert. Damit die validierende Partei die Signatur verstehen kann, sollte sie Informationen über die Kanonisierungsmethode (Standardisierung der XML-Daten), den Verarbeitungsalgorithmus (z. B. einen Hash-Algorithmus) und einen digitalen Signaturalgorithmus enthalten. Sobald diese Informationen in den XML-Daten übertragen sind, kann die validierende Partei prüfen, ob das XML-Zertifikat mit dem privaten Schlüssel eines öffentlichen privaten Schlüsselpaares signiert ist. Der öffentliche Schlüssel sollte ebenfalls im Dokument genannt werden. Schließlich kann das Vertrauen in den öffentlichen Schlüssel mit einem X.509-Zertifikat über eine Zertifikatskette bis hin zu einem vertrauenswürdigen Wurzelzertifikat bzw. Vertrauensanker umgefasst werden.

ELMO

Die Validierung einer ELMO-Datei sollte die gleichen Anforderungen erfüllen wie die Validierung von XML-Dateien. Das Vertrauen in die Gültigkeit der Signatur wird durch die Verwendung eines Registers für öffentliche Schlüssel namens EMReg geschaffen. Hier werden die öffentlichen Schlüssel, die mit den Signierschlüsseln der Institutionen verbunden sind, veröffentlicht. Daher kann die validierende Partei den öffentlichen Schlüssel des privaten Schlüssels, der die Signatur erstellt hat, im EMReg-Register überprüfen und dieses Register als Vertrauensanker annehmen.

JSON

Für die Validierung von JSON gelten ähnliche Anforderungen wie für das XML-Datenformat. Es sollte über eine standardisierte Kanonisierungsmethode, einen Digest-Algorithmus und einen Signaturalgorithmus verfügen. Damit beide Parteien ein gemeinsames Verständnis und eine gemeinsame Unterstützung dieser Methoden und Algorithmen haben, wurden Standards geschaffen, die eine Teilmenge von Kanonisierungsmethoden, Digest- und Signaturalgorithmen umfassen. Während zum Beispiel die Internet Assigned Numbers Authority (IANA) eine Vielzahl von Algorithmen unterstützt, definiert die Internet Engineering Task Force (IETF) eine kleinere Teilmenge als Standard im RFC-7518. Eine noch kleinere Anzahl von Algorithmen wird laut W3C in der JWS Signature Suite unterstützt.

Die Validierung einer JSON-Datei ist ähnlich wie bei einer XML-Datei. Die ausstellende Partei signiert das Zeugnis mit einem privaten Schlüssel eines öffentlich-privaten Schlüsselpaares. Der öffentliche Schlüssel wird ebenfalls im Zertifikat erwähnt. Die überprüfende Partei validiert das Zeugnis im JSON-Format, indem sie die Integritätsprüfung durchführt. Die validierende Partei verwendet den öffentlichen Schlüssel, um den Hash der digitalen Signatur zu entschlüsseln. Die validierende Partei berechnet den Hashwert der Originaldatei und vergleicht ihn mit dem entschlüsselten Hashwert. Wenn die beiden Hashes übereinstimmen, ist die Signatur verifiziert. Das Vertrauen in den öffentlichen Schlüssel kann mit einem X.509-Zertifikat über eine Zertifikatskette bis hin zu einem vertrauenswürdigen Wurzelzertifikat bzw. Vertrauensanker umgefasst werden.

PDF/A

Einbettung von elektronischen Signaturen, Siegeln und Zeitstempel in PDF-Dokumente ist, wie in [Beschluss 2015/1506] gefordert, das PAdES Baseline Profile gemäß [ETSI TS 103 172] bzw. Europäische Norm [ETSI EN 319 142-1] zu berücksichtigen (siehe TR-ESOR-F).

Ähnlich wie bei XML und JSON unterstützt PDF/A die Einbettung von Signaturen in das Dokument selbst, anstatt sie als separate Daten zu verwalten oder einem bestehenden Dokumentenformat hinzuzufügen. Auf diese Weise kann ein Zertifikat (z. B. ein X.509-Zertifikat, ein signierter Message Digest und ein Zeitstempel) nativ als Signatur in die PDF-Datei selbst eingefügt werden. Die validierende Partei verwendet den im X.509-Zertifikat erwähnten öffentlichen Schlüssel, um den Hash der digitalen Signatur zu entschlüsseln. Die validierende Partei berechnet den Hashwert der Originaldatei und vergleicht ihn mit dem entschlüsselten Hashwert. Wenn die beiden Hashes übereinstimmen, ist die Signatur verifiziert. Das Vertrauen in den öffentlichen Schlüssel im X.509-Zertifikat kann über eine Zertifikatskette bis hin zu einem vertrauenswürdigen Wurzelzertifikat bzw. Vertrauensanker umgefasst werden.

11 Beweiswerterhaltung und Bewahrung digitaler Zeugnisse

Grundsätzlich ist zu unterscheiden zwischen Archivierung und Bewahrung. Bewahrung[49] (englisch: preservation) bedeutet beweiswerterhaltende Langzeitspeicherung und betrifft diejenigen Daten und Dokumente, die noch zur Erfüllung ihrer ursprünglichen Funktion herangezogen werden können. Beispiel: ein ehemaliger Absolvent möchte Jahrzehnte später seine digitalen Zeugnisse nutzen. Hierbei kommen digitale Zwischenarchive und die BSI TR-03125 (TR-ESOR) zum Einsatz. Archivierung im engeren Sinne bedeutet die daran anschließende, dauerhafte Langzeitarchivierung. Der Fokus dieser Handreichung ist vor allem auf dem Lebenszyklus digitaler Zeugnisse von der Phase der Erstellung bis zur Phase der Bewahrung (inklusive), benennt aber auch Aspekte der Phase der Archivierung.

Wie beschrieben, sollte entsprechend geltenden regulatorischen Vorgaben, bis zum Ablauf der geltenden Aufbewahrungsfristen der Nachweis von Authentizität, Integrität, Verkehrsfähigkeit und Nachvollziehbarkeit elektronischer Unterlagen gegenüber Gerichten, Prüfbehörden, Dritten jederzeit verlustfrei möglich sein - eine umfassende Herausforderung, insbesondere angesichts Aufbewahrungsfristen von 30 bis zu 60 und mehr Jahren für digitale Zeugnisse (insbesondere bei Hochschulzeugnissen). Eine wesentliche Grundlage für eine ordnungsgemäße elektronische Aufbewahrung oder Langzeitspeicherung bildet eine sachgerechte Aktenführung und Erfüllung geltender Dokumentations- und Nachweispflichten [OkeVA], so dass digitale Zeugnisse als Unterlagen entstehen, die als eindeutiger Nachweis von Geschäftsprozessen und geschäftlichen Entscheidungen gegenüber Dritten (Gerichte, Prüfbehörden etc.) dienen können. Der nestor-Archivstandard „Archivierung von Studierendendaten aus Fachverfahren“ betrachtet die Archivierung speziell im Kontext der Hochschulen[50].

Die Nutzung kryptographischer Mittel, wie fortgeschrittene oder qualifizierte elektronischer Signaturen und qualifizierte Zeitstempel sowie künftig elektronischer Siegel, ermöglicht nach geltendem Recht die Erhaltung des für die Nachweisführung notwendigen Beweiswerts, ohne die Verkehrsfähigkeit einzuschränken (siehe [BMWi07], [eIDAS-VO]). Diese kryptographischen Mittel werden direkt am Dokument/Daten angebracht, so dass er Beweiswert, ebenso wie das Dateiformat oder die Metadaten zur inhaltlichen Beschreibung eines Dokuments, eine inhärente Eigenschaft der jeweiligen elektronischen Unterlagen bildet. Dementsprechend sollten Maßnahmen zur beweissicheren Langzeitspeicherung auch direkt an den elektronischen Unterlagen ansetzen. Im Folgenden werden Standards und Normen zur Bewahrung aufgeführt und es wird die Technische Richtlinie [TR-03125] des BSI als verbindlicher Stand der Technik zur beweiswerterhaltenden Bewahrung beschrieben.

[49] Der Begriff Aufbewahrung wird oft synonym verwendet.
[50] https://d-nb.info/1294122746/34

11.1 Standards und Normen zur Bewahrung

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

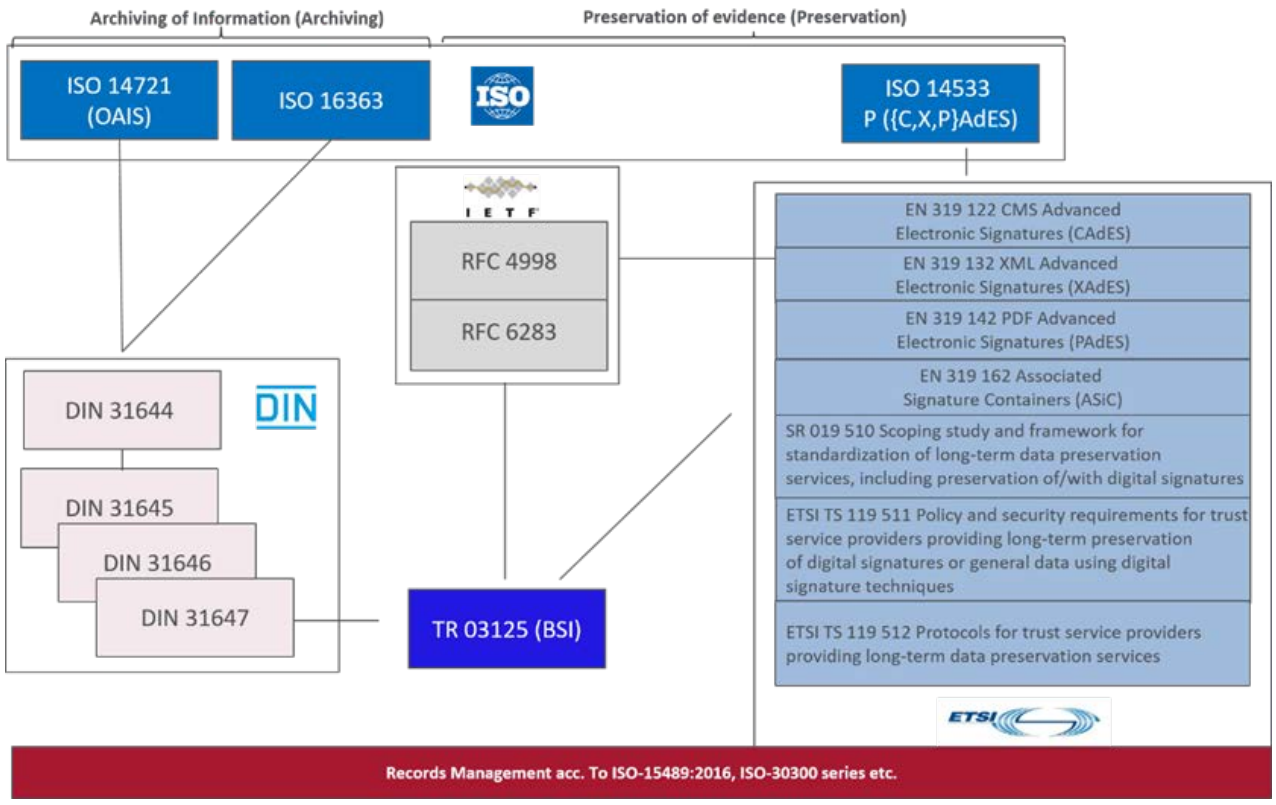

Abbildung 8 Relevante Standards und Normen zur beweissicheren Langzeitspeicherung

Elementare Basis bildet ein ordnungsgemäßes Records Management. Das in [ISO 14721] normierte OAIS-Modell sowie die hierauf aufbauenden DIN-Standards 31644 etc. definieren die notwendigen Prozesse und Informationspakete eines vertrauenswürdigen digitalen Langzeitarchivs. Die [DIN 31647] wiederum beschreibt die notwendigen Funktionen zur Beweiswerterhaltung in einem OAIS-konformen vertrauenswürdigen digitalen Langzeitarchiv. Um Authentizität und Integrität langfristig zu erhalten und nachzuweisen, gilt es, das Langzeitarchiv um die notwendigen technischen Maßnahmen, also Signaturen, Zeitstempel oder Siegel auf Basis der im Zuge der [eIDAS-VO] entstandenen ETSI, vor allem hinsichtlich der Bewahrungsdienste gemäß Art. 34 [eIDAS-VO], zu ergänzen. Hierzu gehören vor allem [ETSI TS 119511] und [ETSI TS 119512]. Die [TR-03125] des BSI führt die Vorgaben zur Informations- und Beweiswerterhaltung logisch zusammen und definiert im Kern eine Middleware zur Beweiswerterhaltung einschließlich der notwendigen Informationspakete sowie der Maßgaben zur Integration in ein vollständiges OAIS-konformes Langzeitarchiv.

11.2 Beweiswerterhaltende Langzeitspeicherung nach BSI TR-03125

Als Stand der Technik zur Beweiswerterhaltung gilt in Deutschland die Technische Richtlinie [TR-03125] (TR-ESOR)[51] des BSI, aktuell in Version 1.3. 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 Technischen Richtlinie 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 Zertifizierungserleichterungen. Darüber hinaus wurden vom BSI Open-Source-Testwerkzeuge entwickelt, die auf Basis der definierten Schnittstellen und Formate der [TR-03125] die technische Interoperabilität der Schnittstellen, AIPs und Beweisdaten (Evidence Records) zwischen den Herstellern erleichtern. Die [TR-03125] selbst beruht resp. integriert nationale wie internationale Standards, zum Beispiel [ETSI TS119511] und [ETSI TS119512]. Die Referenzarchitektur der [TR-03125] zeigt die folgende Grafik:

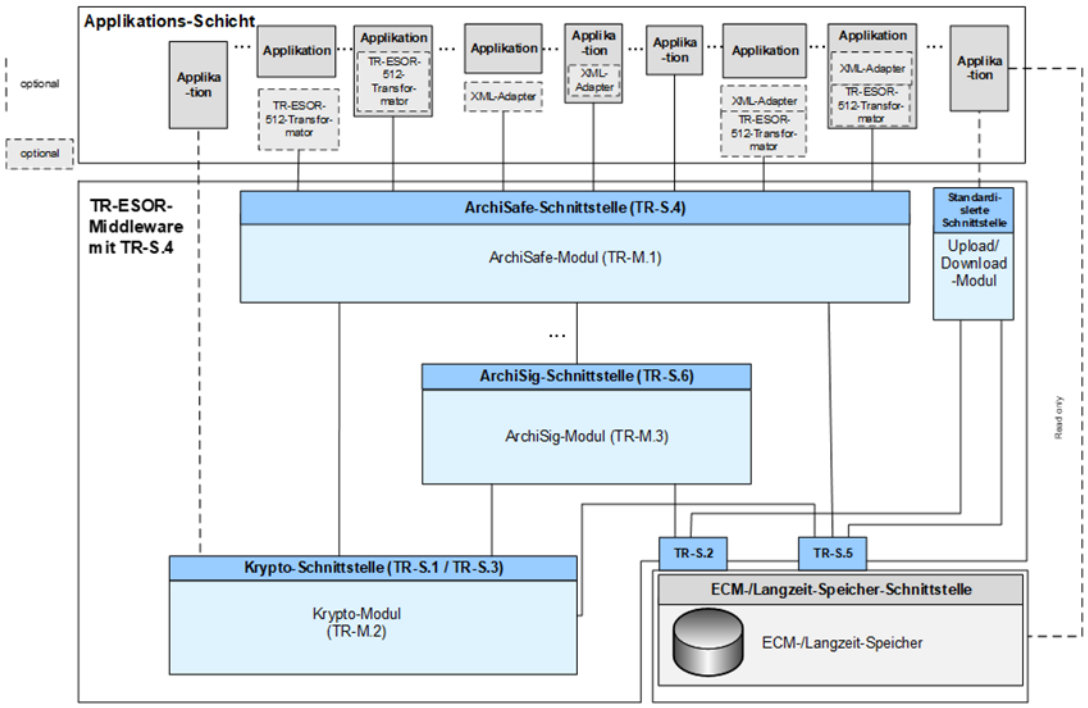

Abbildung 9 Referenzarchitektur der TR-03125

Das Zertifizierungsverfahren des BSI für Bewahrungsprodukte ermöglicht zum einen eine gezielte Auswahl von Verfahren und erleichtert zum anderen die Zertifizierung qualifizierter Bewahrungsdienste, also Dienstleistern für die Beweiswerterhaltung. Einen Einstieg in die TR-ESOR bietet die [BSI Leitlinie TR-ESOR].Für Anwender besteht auch die Möglichkeit, die Beweiswerterhaltung bzw. Bewahrung durch einen externen qualifizierte Bewahrungsdiensteanbieter durchführen zu lassen. Wesentlicher Vorteil wäre, dass dieser vollständig die Verantwortung für die korrekte Bewahrung übernimmt. Dabei kann jeder europäische qualifizierte Bewahrungsdienst verwendet werden. Eine Übersicht findet sich unter https://www.eid.as/tsp-map/#/ Das Organisationskonzept elektronische Verwaltungsarbeit enthält ebenfalls Informationen in Form des Baustein E-Langzeitspeicherung[52].

[51] https://www.bsi.bund.de/tr-esor

[52] https://www.verwaltung-innovativ.de/SharedDocs/Publikationen/Organisation/e_langzeitspeicherung.pdf?__blob=publicationFile&v=3

12 Empfehlungen

In den vorangehenden Kapiteln wurden verschiedene technischen Ansätze vorgestellt und andiskutiert. Auch wenn dieses Dokument nicht versucht eine Gesamtarchitektur für eine digitale Zeugnis- und Bildungsnachweisinfrastruktur zu entwerfen, ergeben sich aus den vorigen Betrachtungen sowie aus den Diskussionen mit den unterschiedlichen fachlichen Experten die folgenden Empfehlungen. Jede einzelne wird in Anlehnung an RFC2119 explizit als verpflichtend (MUSS), empfohlen (SOLLTE) oder als optional (KANN) spezifiziert:

a) Es SOLLTEN geeignete Datenformate wie PDF/A-2 oder XML oder JSON für die Erstellung von digitalen Zeugnissen und Bildungsnachweisen zu verwenden.

b) Die Zeugnis- bzw. Bildungsnachweisdokumente MÜSSEN „kryptographisch signiert“ im Sinne der Definition der [TR-03125] (TR-ESOR)[53] sein. Hierbei MÜSSEN die Vorgaben zu kryptographischen Verfahren der BSI TR-03116-4 bzw. der TR-02102-1 beachtet werden.

c) Es MUSS entweder ein mindestens fortgeschrittenes elektronisches Siegel entsprechend Artikel 36 der Verordnung (EU) Nr. 910/2014 oder eine mindestens fortgeschrittene elektronische Signatur entsprechend Artikel 26 der Verordnung (EU) Nr. 910/2014 verwendet werden. Entsprechend den Anforderungen der Fachseite KÖNNEN auch elektronische Siegel und elektronische Signaturen in Kombination verwendet werden. Es KANN aufgrund rechtlicher Vorgaben erforderlich sein das ein qualifiziertes elektronisches Siegel und/oder eine qualifizierte elektronische Signatur anzuwenden ist.

d) Um die Verwendbarkeit im europäischen Raum zu erhöhen MÜSSEN die Vorgaben der europäischen Standards eingehalten werden die im Anhang des Durchführungsbeschlusses (EU) 2015/1506 aufgelistet sind (das sind die AdES Baseline Profiles ETSI TS 103171 bzw. ETSI TS 103172 bzw. ETSI TS 103173 bzw. ETSI TS 103174).

e) Die verwendeten Siegel und Signaturen SOLLTEN der Konformitätsstufe B-T[54] entsprechen (enthalten einen „timestamp token“ oder ausführlicher ein „trusted token proving that the signature itself actually existed at a certain date and time“ [ETSI EN 319 122-1]).

f) Es MUSS ein definierter Vertrauensanker zur Anwendung kommen, dies kann entweder die Wurzel einer vertrauenswürdigen PKI sein oder eine Vertrauensliste wie bspw. die EU Vertrauensliste[55]. Zur Validierung SOLLTE als zusätzlicher Schritt geprüft werden ob der Zertifikatsinhaber die Befugnis zur Signatur/Siegelung dieser Bildungsnachweise hat (sofern ein Bildungsinstitutionsverzeichnis verfügbar ist).

g) Es SOLLTE für alle erforderlichen Identifizierungen und Authentisierungen jeweils ein Mindest-Vertrauensniveau gemäß [TR-03107] Teil 1 definiert werden (normal, substantiell oder hoch).

h) Es SOLLTEN nur Authentisierungsmittel bestehend aus zwei Faktoren zum Einsatz kommen (Zwei-Faktor-Authentisierung).

i) Es SOLLTE frühzeitig die beweiswerterhaltende Langzeitspeicherung unter Verwendung eines nach [TR-03125] (TR-ESOR) zertifizierten Produktes oder unter Verwendung eines qualifizierten

[53] „Mit dem Begriff der „kryptographisch signierten Dokumente“ sind in dieser TR neben den gemäß [eIDAS-VO], Artikel 3 Nr. 12 qualifiziert signierten, den gemäß [eIDAS-VO], Artikel 3 Nr. 27 qualifiziert gesiegelten oder den gemäß [eIDAS-VO], Artikel 3 Nr. 34 qualifiziert zeitgestempelten Dokumenten (im Sinne der eIDAS-Verordnung) auch Dokumente mit einer fortgeschrittenen Signatur gemäß [eIDAS-VO], Artikel 3 Nr. 11 oder mit einem fortgeschrittenen Siegel gemäß [eIDAS-VO], Artikel 3 Nr. 26 oder mit einem elektronischen Zeitstempel gemäß [eIDAS-VO], Artikel 3 Nr. 33 erfasst, wie sie oft in der internen Kommunikation von Behörden entstehen. Nicht gemeint sind hier Dokumente mit einfachen Signaturen oder Siegeln basierend auf anderen (z. B. nicht-kryptographischen) Verfahren.“

[54] https://ec.europa.eu/digital-building-blocks/wikis/display/ESIGKB/What+are+the+B-T-LT+and+LTA+levels+of+an+electronic+signature

[55] https://ec.europa.eu/tools/lotl/eu-lotl.xml

Bewahrungsdienstes vorzusehen und die digitalen Zeugnisse bzw. Bildungsnachweise frühzeitig in ein solches System einzuspeisen. Digitale Zeugnisse für die eine Aufbewahrungsflicht über einen Zeitraum von 10 und mehr Jahren besteht MÜSSEN beweiswerterhaltend langzeitgespeichert werden.

j) Es SOLLTEN für ALLE involvierten IT-Systeme (Serverkomponenten, Netzwerkkomponenten usw.) die relevanten Sicherheitsanforderungen (Bausteine) aus dem BSI IT-Grundschutz-Kompendium [BSI Grundschutz] umgesetzt werden.

k) Sofern existierende papierne Zeugnisse digitalisiert und ersetzend gescannt werden sollen KANN das ersetzende Scannen nach [TR-03138] (RESISCAN) implementiert werden.

l) Digitale Bildungsnachweise KÖNNEN mit optisch verifizierbaren digitalen Siegeln nach [TR-03171] versehen werden um im Fall eines Medienbruchs den kryptographischen Schutz der Integrität und den Nachweis der Herkunft zu erhalten.

13 Zusammenfassung und Ausblick

Die obigen Überlegungen beziehen manche aktuellen Vorgänge und Entwicklungen nicht mit ein, da diese noch nicht abgeschlossen sind. Ein solcher Vorgang der besonders hervorzuheben ist, ist die Revision der Verordnung (EU) Nr. 910/2014 [eIDAS-VO]. Die sog. **„eIDAS 2.0“**[56] beinhaltet eine Reihe von Neuerungen, unter anderem eine elektronische Brieftasche („Wallet“[57]) und damit verbunden weitergehende elektronische Nachweise („Attestations“). Daraus können sich potentiell neue, zusätzliche Möglichkeiten auch in Bezug auf Bildungsnachweise ergeben. Die „qualified electronic attestations“ wären dann eine zusätzliche Möglichkeit der Abbildung digitaler Zeugnisse. Die in diesem Dokument referenzierten bisherigen klassischen Elemente bleiben jedoch weiterhin Teil der eIDAS-VO.

Abschließend lässt sich feststellen, dass eine ganze Reihe von rechtlichen Regularien, technischen Standards auch auf europäischer Ebene und Technischen Richtlinien des BSI verfügbar sind mit denen eine Digitalisierung von Bildungsnachweisen im Allgemeinen und (Schul-)Zeugnissen im Speziellen möglich wird. Die Digitalisierung auch im Bereich der Bildungseinrichtungen und ihrer Verwaltungen kann dabei unterstützen, Arbeitsabläufe zumindest teilweise zu automatisieren, Papierberge abzubauen und Ressourcen freizusetzen für die Anteile bei denen der menschliche Faktor besonders nutzbringend ist. Diese Digitalisierung ist aber nur dann erfolgreich, wenn dem Gedanken von „**Security by design**“ von Anfang an gefolgt wird. Mithilfe gemeinsamer Standards können so sichere und interoperable Lösungen entstehen.

Es gibt zunehmend Bereiche in denen öffentliche Dokumente und auch Urkunden digitalisiert werden oder auch gänzlich nur noch in digitaler Form verfügbar sind. Aktuell laufen mehrere Aktivitäten zu digitalen Bildungsnachweisen und Zeugnissen, sowohl auf der Ebene der Länder, des Bundes als auch auf europäischer Ebene. Diese reichen von Forschungs- und Entwicklungsprojekten über konkrete Pilotierungen bis hin zu ersten produktiven Umsetzungen. Es bleibt daher spannend, in welchem Bereich, wann welche konkreten Fortschritte erreicht werden können.

[56] https://www.consilium.europa.eu/de/press/press-releases/2022/12/06/european-digital-identity-eid-council-adopts-its-position-on-a-new-regulation-for-a-digital-wallet-at-eu-level/

[57] https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

14 Abkürzungsverzeichnis

Tabelle 4: Abkürzungsverzeichnis

Akronym	***Bedeutung***
AdES	Advanced Electronic Signature (fortgeschrittene elektronische Signatur)
AIP	Archivinformationspaket (engl. Archival Information Package)
BMBF	Bundesministerium für Bildung und Forschung
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
DLT	Distributed-Ledger-Technologie
EBSI	European Blockchain Services Infrastructure
eID	Elektronische Identität
eIDAS	Electronic identification, authentication and trust services
ESSIF	European Self Sovereign Identity Framework
HSM	Hardware-Sicherheitsmodul
JSON	JavaScript Object Notation
JWS	JSON-Websignatur
OAIS	Open Archival Information System
QES, qeS	Qualifizierte elektronische Signatur
qeSi	Qualifiziertes elektronisches Siegel
SSI	Self-sovereign Identities (selbstverwaltete Identitäten)
TR	Technische Richtlinie
VDA	Vertrauensdiensteanbieter
XML	Extensible Markup Language

Literaturverzeichnis

[Beschluss 2015/1506] Durchführungsbeschluss (EU) 2015/1506 der Kommission vom 8. September 2015 zur Festlegung von Spezifikationen für Formate fortgeschrittener elektronischer Signaturen und fortgeschrittener Siegel, die von öffentlichen Stellen gemäß Artikel 27 Absatz 5 und Artikel 37 Absatz 5 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt anerkannt werden. 2015

[BSI Grundschutz] BSI IT-Grundschutz-Kompendium. 2023

[BSI Leitlinie Signatur] Leitlinie für digitale Signatur- / Siegel-, Zeitstempelformate sowie technische Beweisdaten (Evidence Record). 2020

[BSI Leitlinie TR-ESOR] Leitlinie für die beweiswerterhaltende Aufbewahrung gemäß BSI TR-03125 TR-ESOR – Eine Handlungshilfe für Behörden und Unternehmen –. 2021

[BSI SSI] BSI Eckpunktepapier für Self-sovereign Identities (SSI). 2021

[DIN 31647] DIN 31647:2015-05 Information und Dokumentation - Beweiswerterhaltung kryptographisch signierter Dokumente. 2015

[eIDAS-VO] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG. 2014

[ENISA] ENISA Overview of Standards Specifying formats of advanced electronic signatures and seals. 2019

[ETSI TS 119511] ETSI TS 119 511 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques. 2019

[ETSI TS 119512] ETSI TS 119 512 Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services. 2020

[ISO 14721] ISO 14721:2012 Space data and information transfer systems — Open archival information system (OAIS) — Reference model. 2012

[TR-02102] BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen. 2023

[TR-03107] BSI TR-03107 Elektronische Identitäten und Vertrauensdienste im E-Government. 2019

[TR-03116] BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung. 2023

[TR-03125] BSI TR-03125 Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR). 2022

[TR-03138] BSI TR-03138 Ersetzendes Scannen (RESISCAN). 2020

[TR-03160] BSI TR-03160 Servicekonten. 2023

[TR-03171] BSI TR-03171 Optisch verifizierbarer kryptographischer Schutz von Verwaltungsdokumenten (Digitale Siegel)

[VDG] Vertrauensdienstegesetz vom 18. Juli 2017 (BGBl. I S. 2745), das durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist. 2017