

DIN 31647

ICS 01.140.20

**Information und Dokumentation –
Beweiswerterhaltung kryptographisch signierter Dokumente**

Information and documentation –
Preservation of evidence of cryptographically signed documents

Information et documentation –
Conservation de la valeur probante de documents signés par un dispositif cryptographique

Gesamtumfang 27 Seiten

DIN-Normenausschuss Bibliotheks- und Dokumentationswesen (NABD)

Inhalt

	Seite
Vorwort	3
Einleitung.....	4
1 Anwendungsbereich	6
2 Normative Verweisungen.....	6
3 Begriffe	7
4 Abkürzungen	16
5 Funktionale Anforderungen an ein System zur Beweiswerterhaltung	17
5.1 Anforderungen	17
5.1.1 Art und Weise der Erzeugung von Hashwerten	17
5.1.2 Nachvollziehbarkeit	18
5.1.3 Fähigkeit zum ungehinderten Datenaustausch.....	18
5.2 Funktionen.....	19
5.2.1 Allgemeines.....	19
5.2.2 Funktion 1: Einholung und Prüfung der beweisrelevanten Daten des SIP/Version	19
5.2.3 Funktion 2: Erzeugen von technischen Beweisdaten des AIP	19
5.2.4 Funktion 3: Abruf des AIP mit den technischen Beweisdaten zum Zweck der externen Integritäts- und Authentizitätsprüfung	19
5.2.5 Funktion 4: Prüfung der technischen Beweisdaten.....	20
5.2.6 Funktion 5: Erhaltung durch Erneuerung der technischen Beweisdaten des AIP	20
Anhang A (informativ) Archivpakete mit kryptographischen Beweismitteln	22
Anhang B (informativ) Anwendungsbeispiele.....	25
Literaturhinweise	26
Bilder	
Bild A.1 — Struktur eines Archivpaketes mit kryptografischen Sicherungsmitteln.....	23

Vorwort

Für das vorliegende Dokument ist der Arbeitsausschuss NA 009-00-15 AA „Schriftgutverwaltung und Langzeitverfügbarkeit digitaler Informationsobjekte“ im DIN-Normenausschuss Bibliotheks- und Dokumentationswesen (NABD) verantwortlich. Es wurde vom zuständigen Arbeitskreis NA 009-00-15-06 AK „Arbeitskreis Beweiswerterhaltung kryptographisch signierter Dokumente“ erarbeitet.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. DIN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Einleitung

Die Nutzung der Informationstechnologie zur Abbildung von Geschäftsprozessen ist allgemein etabliert. Immer häufiger liegen geschäftsrelevante Unterlagen ausschließlich elektronisch vor. Elektronische Dokumente können jedoch aus sich heraus weder wahrgenommen noch gelesen werden. Sie liefern aus sich heraus auch keine Hinweise für ihre Integrität und Authentizität im elektronischen Rechts- und Geschäftsverkehr. Als zentrale Herausforderungen stellen sich insofern Fragen der IT-Sicherheit, der Erfüllung von Dokumentations- und Nachweispflichten sowie die Beachtung spezifischer rechtlicher Rahmenbedingungen wie z. B. Formerfordernisse. Im Zweifels-/Streitfall muss erfahrungsgemäß z. B. die Erfüllung geltender Dokumentationspflichten oder Formerfordernisse nachgewiesen werden, um juristische oder wirtschaftliche Nachteile zu vermeiden. Fragen nach einer eindeutigen Authentifizierung, dem eindeutigen Nachweis der Identität und Authentizität des Absenders oder Ausstellers eines Dokuments, stellen wichtige Herausforderungen in der digitalen Welt dar.

Dies gilt umso mehr vor dem Hintergrund geltender Aufbewahrungsfristen zwischen zwei und 110 Jahren oder dauerhaft, die zudem erst Jahrzehnte nach Entstehen des Dokuments einsetzen. Besondere Anforderungen bestehen dabei an die Beweiswerterhaltung kryptographisch signierter Dokumente, da die Sicherheitseignung der eingesetzten kryptographischen Algorithmen mit der Zeit abnehmen kann, was den Beweiswert der Dokumente gefährdet, so dass im Rahmen der langfristigen Aufbewahrungsdauer kryptographisch signierter Dokumente spezifische Maßnahmen für den Erhalt des Beweiswerts notwendig sind.

Im Fokus des Beweiswerts steht der eindeutige Nachweis von Authentizität und Integrität der betreffenden Daten vor Gerichten, Prüfbehörden und Dritten. In dieser Norm werden unter Authentizität die Übereinstimmung des kryptographisch signierten Dokuments mit den Ursprungsdaten (Echtheit der Dokumente) und deren eindeutige Zurechenbarkeit zu einem Aussteller (Verfasser, Ersteller und/oder Absender) verstanden. Hiervon unterscheiden sich der in der vorliegenden Norm nicht weiter verfolgte Bereich der Geschichtswissenschaft und der dort abweichend definierte Begriff der Authentizität erheblich. Dort bedeutet Authentizität im Zusammenhang mit der digitalen Langzeitarchivierung und bezogen auf Repräsentationen, dass die zu archivierende Information seit dem Beginn des Übernahmeverfahrens in das Langzeitarchiv nicht verändert wurde, auch wenn Repräsentationen verändert wurden (siehe DIN 31644).

Integrität im Sinne der Beweiswerterhaltung wird als gegeben betrachtet, wenn die betreffenden Daten vollständig sind und bezüglich ihrer signifikanten Eigenschaften nachweislich keine Veränderungen oder Manipulationen an den Daten festgestellt werden können. Von „Beweiswert“, also der Eignung eines Beweismittels, die Überzeugung des Gerichts zu beeinflussen, wird dementsprechend in dieser Norm nur im juristischen Sinne gesprochen.

Die kryptographische Signierung elektronischer Dokumente ermöglicht es, den rechtlichen bzw. juristischen Beweiswert der Dokumente in besonderem Maße zu sichern. Jedes elektronische Dokument kann zwar einen Beweiswert vor Gericht besitzen, aber der Beweiswert kryptographisch signierter Dokumente ist vor Gericht faktisch nicht bestreitbar. Fortgeschrittene oder qualifizierte elektronische Signaturen und qualifizierte Zeitstempel (kryptographische Sicherungsmittel) stellen dabei nach geltendem Recht die zur eindeutigen Nachweisführung hinsichtlich Authentizität und Integrität elektronischer Dokumente notwendige Beweiswerterhaltung direkt am eigentlichen Dokument sicher, da Signaturen und Zeitstempel direkt am Dokument angebracht werden. In der praktischen Umsetzung ist dabei für jeden Anwendungsfall durch die Verantwortlichen zu entscheiden, welches kryptographische Verfahren eingesetzt wird bzw. welches für den jeweiligen Prozess optimal geeignet ist (Customizing).

Der Beweiswert ist also eine inhärente Eigenschaft der jeweiligen elektronischen Dokumente. Dementsprechend müssen Maßnahmen zur Beweiswerterhaltung auch direkt an den elektronischen Dokumenten ansetzen. Diese Norm beschreibt die notwendigen Maßnahmen zur Beweiswerterhaltung. Sie trifft dabei keine Aussage darüber, in welchen Fällen der Einsatz kryptographischer Verfahren zur Erhaltung des Beweiswerts erforderlich ist. Wenn aus gesetzlichen oder fachlichen Anforderungen heraus der Einsatz kryptographischer Verfahren zur Erhaltung des Beweiswerts erforderlich ist, müssen die in dieser Norm definierten Anforderungen erfüllt werden.

In den Fällen, in denen der Beweiswert vollumfänglich zu erhalten ist, ist er von der Erstellung oder dem Eingang des Dokuments bis zum Ablauf seiner geltenden Aufbewahrungsfristen zu erhalten. Diese können zwischen zwei und 110 Jahren liegen und auch teils dauerhaft bestehen. Während dieser Zeit muss, neben der Authentizität und Integrität, die Verkehrsfähigkeit der kryptographisch signierten Dokumente erhalten bleiben. Die Verkehrsfähigkeit im Kontext der Beweiswerterhaltung ermöglicht den ungehinderten Austausch elektronischer Dokumente zur Prüfung des Beweiswerts, z. B. bei der Vorlage bei Prüfinstitutionen, Gerichten oder dem Austausch zwischen IT-System ohne Schmälerung des Beweiswertes. Die Nutzung kryptographischer Mittel, wie fortgeschrittener oder qualifizierter elektronischer Signaturen und Zeitstempel, ermöglicht nach geltendem Recht eine vertrauenswürdige Beweiswertsicherung, ohne die Verkehrsfähigkeit einzuschränken [1], [2].

Zur Beweiswerterhaltung ist es notwendig, das elektronische Dokument in einem geeigneten IT-System abzulegen. Geschah die Ablage so, dass das Dokument nicht verfälscht sowie die kryptographischen Sicherungsmittel und damit das Dokument selbst auf den Aussteller eindeutig rückführbar ist, dann ist der Beweiswert des elektronischen Dokuments erhalten geblieben.

Neben der Beweiswerterhaltung ist es notwendig sicherzustellen, dass die Informationen im Dokument noch lesbar, vollständig und wieder auffindbar sind. Die Informationserhaltung ist jedoch nicht Gegenstand der vorliegenden Norm. Das bedeutet, dass ein digitales Langzeitarchiv (dLZA), in dem die Beweiswerterhaltung kryptographisch signierter Dokumente erfolgt und das auch die langfristige Lesbarkeit der aufbewahrten Daten sicherstellen soll, sowohl

— Beweiswerterhaltung (entsprechend dieser Norm)

als auch

— Informationserhaltung (OAIS nach ISO 14721:2012 [3] und DIN 31644 [23])

ermöglicht. Wie eine solche Gesamtlösung umgesetzt wird, ist abhängig vom konkreten Bedarf der jeweiligen Institution und muss im Anwendungsfall geklärt werden. Im Rahmen einer praktischen Umsetzung sind dann entsprechend den rechtlichen und fachlichen Anforderungen die notwendigen Maßnahmen, z. B. unter Aufgreifen des Migrations- oder Emulationsverfahrens, zu definieren.

1 Anwendungsbereich

Diese Norm legt im Kontext der elektronischen Langzeitarchivierung fachliche und funktionale Anforderungen an die Beweiswerterhaltung kryptographisch signierter Dokumente unter Wahrung der Authentizität, Integrität und Verkehrsfähigkeit der Dokumente fest. Hierzu werden konkrete Funktionen eines generischen Systems zur Beweiswerterhaltung kryptographisch signierter Dokumente¹⁾ beschrieben. Die Norm bezieht sich innerhalb des Anwendungsbereichs auf alle elektronischen Dokumente/Daten, deren durch kryptographische Elemente erzeugter Beweiswert erhalten werden soll.

Die Funktionen zur Beweiswerterhaltung stellen kein eigenständiges System zur elektronischen Langzeitarchivierung dar. Vielmehr ergänzen sie ein in Anlehnung an das OAIS-Modell aufgebautes elektronisches Langzeitarchiv, z. B. ein vertrauenswürdiges digitales Langzeitarchiv (dLZA) im Sinne der DIN 31644, um zusätzliche Funktionen, die notwendig sind, um eine Beweiswerterhaltung kryptographisch signierter Dokumente durchführen zu können.

Die Beweiswerterhaltung nach dieser Norm kann also ein spezifischer Anwendungsfall der DIN 31644 sein. Wenn in einem dLZA die Beweiswerterhaltung kryptographisch signierter Dokumente realisiert werden soll, so wären in einem solchen Fall neben DIN 31644 die Anforderungen dieser Norm zu berücksichtigen. Dementsprechend sind Fragen zur Informationserhaltung, wie sie u. a. in DIN 31644 enthalten sind, zwar beim Aufbau eines vertrauenswürdigen dLZA zu berücksichtigen, jedoch kein Bestandteil dieser Norm.

Diese Norm lehnt sich insbesondere hinsichtlich der Informationspakete an das OAIS-Modell an. Die Norm beschreibt grundlegende Anforderungen an die Informationspakete eines dLZA, um die zur Beweiswerterhaltung kryptographisch signierter Dokumente notwendigen Informationen zu erhalten. Die konkrete technische Umsetzung ist nicht Bestandteil dieser Norm. Daneben wird in einem informativen Anhang beispielhaft beschrieben, wie die zur Beweiswerterhaltung kryptographisch signierter Dokumente notwendigen Informationen in einem AIP abgelegt und beschrieben werden können (siehe Anhang A und Anhang B).

Die Norm gilt nicht für die Aufbewahrung analoger Unterlagen. Sie bezieht sich im Wesentlichen auf die Aufbewahrung kryptographisch signierter Dokumente bis zum Ablauf der geltenden Aufbewahrungsfristen. Die Langzeitarchivierung in Gedächtnisorganisationen nach Ablauf der Aufbewahrungsfristen ist in der Regel kein Anwendungsfeld dieser Norm.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

IETF RFC 4998 – *Evidence Record Syntax (ERS)*²⁾

1) Im Folgenden wird aus Gründen der Lesbarkeit vom System zur Beweiswerterhaltung gesprochen.

2) Bezugsquelle: IETF RFC 4998 – Evidence Record Syntax (ERS), 2007.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1

Archivablage

(en: archival storage)

funktionale Entität im Referenzmodell OAIS, die jene Funktionen und Prozesse beinhaltet, die die Speicherung und Verfügbarkeit der Archivpakete sicherstellen

[QUELLE: DIN 31644:2012-04, 2.1]

3.2

Archivdatenobjektidentifikator

AOID

(en: archive object identifier)

weltweit eindeutige Archiv-Informationsobjekt-ID, welche vom dLZA für die Speicherung eines AIP generiert und an die aufrufende Geschäftsanwendung zurückgeliefert wird

Anmerkung 1 zum Begriff: Die AOID dient als Referenz auf das AIP und dient der zuverlässigen Wiederauffindbarkeit der Dokumente und Daten sowie als Schlüssel für den autorisierten Zugriff auf die im dLZA abgelegten AIP.

Anmerkung 2 zum Begriff: In Anlehnung an TR 03125 TR-ESOR [4].

3.3

Archivpaket

Archivinformationspaket

AIP

(en: archival information package)

konzeptionelle, logische Einheit im Referenzmodell OAIS, die ein Paket darstellt, das im digitalen Langzeitarchiv gespeichert wird

Anmerkung 1 zum Begriff: Das Paket besteht aus Inhaltsdaten und den für die Langzeitarchivierung notwendigen Metadaten. Zur Beweiswerterhaltung kommen zudem die beweisrelevanten Daten und die Beweisdaten hinzu.

Anmerkung 2 zum Begriff: Damit im Sinne dieser Norm das AIP selbsttragend ist, müssen dem AIP die beweisrelevanten Daten sowie die technischen Beweisdaten hinzugefügt werden. Das bedeutet, es muss möglich sein, das AIP auch ohne eine dem dLZA vorgelagerte Geschäftsanwendung zu interpretieren und zu verifizieren. Zur Beweiswerterhaltung muss die Überführung des AIP in ein anderes dLZA sichergestellt werden, ohne hierfür das AIP zunächst in die im Übernahmeprozess erzeugte Form reproduzieren zu müssen.

[QUELLE: DIN 31644:2012-04, 2.2, modifiziert: Anmerkung 2 zum Begriff hinzugefügt; Synonym hinzugefügt]

3.4

Aufnahme

(en: ingest)

funktionale Entität im Referenzmodell OAIS, die jene Funktionen und Prozesse beinhaltet, die die Übernahme der Transferpakete von den Produzenten, die Transformation in Archivpakete und die Aufnahme ins Archiv sicherstellen

[QUELLE: DIN 31644:2012-04, Begriff 2.3]

3.5

Authentizität

Übereinstimmung mit den Ursprungsdaten (Echtheit der Dokumente) und deren eindeutige Zurechenbarkeit zu einem Aussteller (Verfasser, Ersteller und/oder Absender) im Sinne der Beweiswerterhaltung kryptographisch signierter Dokumente

Anmerkung 1 zum Begriff: In Anlehnung an TR 03125 TR-ESOR [4].

Anmerkung 2 zum Begriff: In DIN 31644 [23], DIN 31645 [10] und DIN 31646 [11] bedeutet Authentizität im Zusammenhang mit der digitalen Langzeitarchivierung und bezogen auf Repräsentationen, dass die zu archivierende Information seit dem Beginn des Übernahmeverfahrens in das Langzeitarchiv nicht verändert wurde, auch wenn Repräsentationen verändert wurden.

3.6

Beweisdaten

technische Beweisdaten

(en: evidence records)

Informationen zum Nachweis der Unversehrtheit der Integrität und Authentizität der Archivpakete

Anmerkung 1 zum Begriff: In Anlehnung an TR 03125 TR-ESOR [4]; in Übereinstimmung mit den IETF-Spezifikationen RFC 4998 [12] und RFC 6283 [1] enthält ein technischer Beweisdatensatz Archivzeitstempel ausreichender Qualität über die gespeicherten Archivpakete, die die Unversehrtheit der Daten nachweisen, und zusätzlich Informationen, welche die Richtigkeit und die Gültigkeit elektronischer Signaturen zum Signaturzeitpunkt sowie die rechtzeitige Signaturerneuerung entsprechend der rechtlichen Anforderungen belegen.

3.7

beweisrelevante Daten

alle Daten, die für eine Beweisführung notwendig und gegenüber den Inhaltsdaten sowie den Metadaten abgegrenzt sind, sowie die Sperrdaten für Signaturen, Zeitstempel und alte Beweisdaten.

Anmerkung 1 zum Begriff: Beweisrelevante Daten enthalten auch die für die Prüfung der Signatur bzw. Zeitstempelsignatur notwendigen Prüfdaten wie z. B. Zertifikate sowie CRL-Listen und OCSP-Responses zu diesen Zertifikaten. Die Beweisdaten belegen, dass das Dokument ab dem Zeitpunkt der Aufnahme in das System zur Beweiswerterhaltung nicht mehr verändert wurde. Die beweisrelevanten Daten belegen, dass die ggf. außerhalb des Systems erzeugten Signaturen und Zeitstempel gültig sind bzw. zum Erstellungszeitpunkt gültig waren. Eine Signatur kann auch zu mehreren Datenobjekten gehören.

Anmerkung 2 zum Begriff: In Anlehnung an TR 03125 TR-ESOR [4].

Anmerkung 3 zum Begriff: Beweisrelevante Daten dienen als Authentizitätsnachweis.

3.8

Beweiswert

Eignung eines Beweismittels, die Überzeugung eines Dritten, insbesondere eines Gerichts, zu beeinflussen

3.9

Beweiswerterhaltung

Maßnahmen, die geeignet sind, den Beweiswert elektronischer Dokumente mindestens für die Dauer der vorgeschriebenen Aufbewahrungszeiträume sicherzustellen

Anmerkung 1 zum Begriff: Die Maßnahmen zur Beweiswerterhaltung kryptografisch signierter Dokumente ergänzen die Langzeiterhaltungsmaßnahmen eines digitalen Langzeitarchivs im Sinne dieser Norm.

Anmerkung 2 zum Begriff: Technisch wird die Beweiswerterhaltung durch Beweisdaten und beweisrelevante Daten realisiert.

3.10

Customizing

Auswahl des kryptographischen Verfahrens an die jeweiligen Rahmenbedingungen des jeweiligen Beweiswerterhaltungsprozesses zur optimalen Gestaltung des Gesamtprozesses

3.11

Datenobjekt

digitales Objekt im Kontext der Beweiswerterhaltung kryptografisch signierter Dokumente

Anmerkung 1 zum Begriff: In Anlehnung an ISO 14721:2012 [3].

3.12**digitales Langzeitarchiv****dLZA**

Organisation (bestehend aus Personen und technischen Systemen), die die Verantwortung für den Langzeiterhalt und die Langzeitverfügbarkeit von Information in digitaler Form sowie die Bereitstellung für eine bestimmte Zielgruppe übernommen hat

Anmerkung 1 zum Begriff: Zur Beweiswerterhaltung erfüllt das dLZA darüber hinaus die Anforderungen der vorliegenden Norm.

Anmerkung 2 zum Begriff: Dabei bedeutet Langzeit, über Veränderungen in der Technik (Soft- und Hardware) und in der Zielgruppe hinweg. Dies umfasst in dieser Norm regelmäßig den Zeitraum bis zum Ablauf der geltenden Aufbewahrungsfristen.

Anmerkung 3 zum Begriff: Hierfür wird im deutschen Sprachgebrauch mitunter auch der Begriff der „elektronischen (digitalen) Langzeitspeicherung“ verwendet, um den Unterschied zur kurzzeitigen „lebenden Schriftgutablage“ bzw. zum Backup hervorzuheben.

Anmerkung 4 zum Begriff: In Anlehnung an ISO-14721:2012 [3].

[QUELLE: DIN 31644:2012-04, 2.6, modifiziert: Anmerkung zum Begriff hinzugefügt.]

3.13**digitales Objekt**

Objekt, das sich aus einer Reihe von Bitsequenzen zusammensetzt

Anmerkung 1 zum Begriff: In Anlehnung an Referenzmodell für ein OAIS, deutsche Übersetzung [13].

3.14**Evidence Record Syntax****ERS**

Standard der Internet Engineering Taskforce (IETF), welcher ein Verfahren zur Langzeitabsicherung einer großen Menge elektronischer Dokumente mithilfe nichtabstreitbarer kryptografischer, organisatorischer und technischer Verfahren und die zugehörigen Datenstrukturen beschreibt

Anmerkung 1 zum Begriff: Die ERS wurde im August 2007 von der IETF nach langer technischer Diskussion in den Stand eines RFC erhoben und wird im dortigen Verzeichnis unter der Nummer 4998 geführt. Vorarbeiten zu diesem Standard sind im Rahmen des vom Deutschen Bundesministerium für Wirtschaft und Arbeit im Rahmen des Vorhabens VERNET geförderten Projekt ArchiSig geleistet worden.

3.15**Fixity Information**

Methoden und Daten, die zur langfristigen Prüfung der Authentizität und Integrität elektronischer Dokumente notwendig sind

Anmerkung 1 zum Begriff: Im Kontext der Beweiswerterhaltung handelt es sich dabei z. B. um die Beweisdaten und die beweisrelevanten Daten.

Anmerkung 2 zum Begriff: Der englische Begriff „Fixity Information“ sollte im Kontext der Beweiswerterhaltung so beibehalten werden (anstatt Persistenzinformationen).

3.16**fortgeschrittene elektronische Signatur**

elektronische Signatur, die gemäß SigG [14], § 2 Nr. 2 ausschließlich dem Signaturschlüssel-Inhaber zugeordnet ist, die die Identifizierung des Signaturschlüssel-Inhabers ermöglicht, die mit Mitteln erzeugt wird, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann und die mit den Daten, auf die sie sich beziehen, so verknüpft ist, dass eine nachträgliche Veränderung der Daten erkannt werden kann