Bundesamt
für Sicherheit in der
Informationstechnik

Leitlinie für digitale Signatur-/ Siegel-, Zeitstempelformate sowie technische Beweisdaten (Evidence Record)

Dokument:	Leitlinie für digitale Signatur-/Siegel-, Zeitstempel-formate sowie technische Beweisdaten (Evidence Record)
Version:	1.0
Datum:	26.03.2020

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: tresor@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Einleitung

1.1 Gegenstand des Dokuments

Um die Anwendung, also Erzeugung und Prüfung mindestens fortgeschrittener elektronischer Signaturen und Siegel sowie qualifizierter elektronischer Zeitstempel und technische Beweisdaten (englisch: Evidence Records) in der Bundesverwaltung zu erleichtern, begrenzt diese Leitlinie, u.a. basierend auf dem Durchführungsrechtsakt 2015/1506 der EU-Kommission, die Anzahl der relevanten Signatur-/Siegelformate. Des Weiteren benennt die Leitlinie die grundlegenden Verpflichtungen und Empfehlungen für deren Erzeugung und Prüfung sowie für die Bewahrung bzw. Beweiswerterhaltung (qualifizierter) elektronischer Signaturen, Siegel, Zeitstempel und (signierter) Daten mittels Signaturtechniken (Signaturen, Siegel, Zeitstempel, Evidence Records).

Gegenstand des Dokuments ist zum einen die Darstellung der gemäß dem regulatorischen Rahmen [eIDAS-VO, (EU)2015/1506] für die Erzeugung und Prüfung relevanten Formate für mindestens fortgeschrittene elektronische Signaturen und Siegel sowie zum anderen die Empfehlung grundlegender Maßgaben zur praktischen Anwendung.

Die Leitlinie deckt darüber hinaus die wesentlichen Anwendungsfälle für kryptographische Signaturen und Siegel sowie qualifizierte elektronische Zeitstempel und Evidence Records (Beweiswerterhaltung) ab. Sie kann jedoch Sonderfälle nicht ausschließen, die von dieser Leitlinie nicht abgedeckt sind. Es wird EMPFOHLEN, diese Sonderfälle im konkreten Fall mit den zuständigen Aufsichtsstellen zu klären.

Im vorliegenden Dokument wird die Verbindlichkeit von Anforderungen durch die an [RFC 2119] angelehnten deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, EMPFOHLEN, SOLL NICHT, KANN gekennzeichnet.

1.2 Zielgruppe

Zielgruppe der Leitlinie ist die unmittelbare und mittelbare Bundesverwaltung. Darüber hinaus besitzt diese Leitlinie empfehlenden Charakter.

2 Kurzer Abriss Regulatorischer Rahmen

2.1 Grundsatz[1]

Seit Juli 2016 ist die „Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG“ vom 23.07.2014 [eIDAS-VO] vollständig anwendbar. Als EU-Verordnung ist die [eIDAS-VO] unmittelbar geltendes Recht in allen EU-Mitgliedsstaaten sowie im Europäischen Wirtschaftsraum (EWR). Die Verordnung sowie die hierauf basierenden Durchführungsrechtsakte dienen der Harmonisierung des Binnenmarkts u.a. für elektronische Signaturen, Siegel und Zeitstempel in EU und EWR.

In Deutschland wurde im Zuge der [eIDAS-VO] im Jahre 2017 durch Artikel 12 des eIDAS-Durchführungsgesetzes („Gesetz zur Durchführung der 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“) [eIDAS-DG] das Signaturgesetz [SigG] sowie die Signaturverordnung [SigV] aufgehoben.

Das eIDAS-Durchführungsgesetz ist ein Artikelgesetz, dessen Kernstück als Artikel 1 das Vertrauensdienstegesetz [VDG] darstellt. Das Vertrauensdienstegesetz wird seit 2019 durch die Vertrauensdiensteverordnung [VDV] ergänzt.

Die eIDAS-Verordnung [eIDAS-VO] spezifiziert neben (einfachen) elektronischen Signaturen [eIDAS-VO, Artikel 3 Nr. 10], fortgeschrittene Signaturen [eIDAS-VO, Artikel 3 Nr. 11] und qualifizierte Signaturen [eIDAS-VO, Artikel 3 Nr. 12] sowie darüber hinaus elektronische Zeitstempel [eIDAS-VO, Artikel 3 Nr. 33] und qualifizierte elektronische Zeitstempel [eIDAS-VO, Artikel 3 Nr. 34].

Als Pendant zu elektronischen Signaturen für natürliche Personen führt die eIDAS-Verordnung zusätzlich elektronische Siegel ein, die auch von Organisationen (juristischen Personen) verwendet werden können, und definiert dabei neben einfachen elektronischen Siegeln [eIDAS-VO, Artikel 3 Nr. 25] auch fortgeschrittene elektronische Siegel [eIDAS-VO, Artikel 3 Nr. 26] und qualifizierte elektronische Siegel [eIDAS-VO, Artikel 3 Nr. 27]. Weiterhin ermöglicht [eIDAS-VO] durch die im Erwägungsgrund (52) genannte „Fernsignatur“ die mobile Erstellung (qualifizierter) elektronischer Signaturen und entsprechender Siegel.

Qualifizierte elektronische Zeitstempel genügen den Anforderungen gemäß [eIDAS-VO, Artikel 42] und werden mit einer fortgeschrittenen elektronischen Signatur eines qualifizierten Vertrauensdiensteanbieters versehen oder mit einem fortgeschrittenen elektronischen Siegel eines qualifizierten Vertrauensdiensteanbieters versiegelt oder es wird ein gleichwertiges Verfahren verwendet.

Kryptographische Signaturen, Siegel und Zeitstempel erfordern eine Erneuerung der zugrundeliegenden Signatur- und Hashalgorithmen und damit Beweiswerterhaltung nach dem Stand der Technik, sofern sie länger benötigt werden, als die Sicherheitseignung der zugrundeliegenden Algorithmen gegeben ist. Ebenso ist zum Zwecke der Nachweisführung die langfristige Prüfbarkeit der Signaturen, Siegel und Zeitstempel zu gewährleisten.

Darüber hinaus werden in der [eIDAS-VO] neue Vertrauensdienste wie z.B. elektronische Zustelldienste [eIDAS-VO, Artikel 43, 44], Webseitenzertifikate [eIDAS-VO, Artikel 45], Validierungsdienste [eIDAS-VO, Artikel 33] und Bewahrungsdienste [eIDAS-VO, Artikel 34, 40] eingeführt.

Als nationale Aufsichtsstelle für die Vertrauensdienste zur „Erstellung, Überprüfung und Validierung elektronischer Signaturen, elektronischer Siegel oder elektronischer Zeitstempel und Dienste für die

[1] Vgl. [TR-ESOR], BSI: Technische Richtlinie 03125, Beweiswerterhaltung kryptographisch signierter Dokumente, BSI TR-03125, v1.2.2, Kap. 4.2.1

Zustellung elektronischer Einschreiben sowie von diese Dienste betreffenden Zertifikaten“ sowie die „Bewahrung von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten“ fungiert gemäß § 2 Abs. 1 [VDG] die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur).

„Von der Aufsicht für die Vertrauensdienste durch die Bundesnetzagentur unberührt bleiben die Aufgaben des Bundesamtes für Sicherheit in der Informationstechnik gem. [BSIG] und weiteren Fachgesetzen. So obliegt dem BSI gem. § 2 Abs. 2 [VDG] insbesondere die

- Erstellung technischer Standards in nationalen, europäischen und internationalen Gremien in Abstimmung mit der Bundesnetzagentur,
- die Bewertung von Algorithmen und zugehörigen Parametern sowie
- die Erstellung technischer Vorgaben und die Bewertung technischer Standards für den Einsatz von Vertrauensdiensten in Digitalisierungsvorhaben nach Maßgabe der entsprechenden Fachgesetze.“

Das BSI fungiert zudem gem. § 2 Abs. 3 [VDG] als die für Informationssicherheit zuständige nationale Stelle gem. [eIDAS-VO Artikel 19 Abs. 2]. Hierzu gehört bspw. die Prüfung und Zertifizierung konkreter Produkte, die von den Vertrauensdiensteanbietern eingesetzt werden (z.B. Hardware-Sicherheitsmodule, sichere Signaturerstellungseinheiten nach Common Criteria Protection Profiles oder Produkte zur Beweiswerterhaltung gem. [TR-ESOR]).

Eine enge Zusammenarbeit von Bundesnetzagentur sowie des BSI gewährleistet eine sichere wie rechtskonforme Umsetzung der Vertrauensdienste durch die Vertrauensdiensteanbieter entsprechend der [eIDAS-VO].

Weitere Details zu den rechtlichen Rahmenbedingungen finden sich unter folgenden Links sowie der [TR-ESOR]:

- https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/eIDAS_node.html
- https://www.bsi.bund.de/tr-esor
- https://www.elektronische-Vertrauensdienste.de

3 Annahme und Prüfung von Signaturen, Siegeln und Zeitstempeln

Alle öffentlichen Stellen, so auch die Bundesverwaltung, **MÜSSEN**, alle mindestens fortgeschrittenen elektronischen XML-, CMS-, PDF-Signaturen und entsprechende Siegel der Konformitätsstufen B, T oder LT sowie zugehörige Container gem. ASiC (ETSI EN 319 162-1) in den in Durchführungsrechtsakt [(EU) 2015/1506] definierten Formaten (vgl. Anlage 1) akzeptieren, verarbeiten und prüfen können.

Wenn andere Signaturformate verwendet werden, **MUSS** gem. dem Durchführungsrechtsakt (EU) 2015/1506 vom Mitgliedsstaat des betreffenden Vertrauensdiensteanbieters ein kostenloses Validierungstool zur Verfügung gestellt werden (vgl. Erwägungsgrund (7) und Artikel 4 des Durchführungsbeschlusses [(EU) 2015/1506]).

Alle öffentlichen Stellen, so auch die Behörden der Bundesverwaltung, **MÜSSEN** jeden qualifizierten elektronischen Zeitstempel (siehe Art. 41 Abs. 3 [eIDAS-VO]) akzeptieren und verarbeiten können.

Die Prüfberichte für elektronische Signaturen, Siegel und Zeitstempel **MÜSSEN** gemäß dem Stand der Technik erzeugt werden (vgl. [ETSI TS 119 102-2], [OASIS-VR], [OASIS VR-XSD] und [TR-ESOR-VR]).

Sofern die Signatur-/Siegel-/Zeitstempelprüfung als IT-Dienst gegenüber weiteren externen Behörden (z. B. bei einem IT-Dienstleister des Bundes) erbracht wird, **MUSS** die Validierung durch einen qualifizierten Validierungsdienst erfolgen.

Bei der lokalen Prüfung (qualifizierter) elektronischer Signaturen, Siegel bzw. Zeitstempeln durch eine Behörde innerhalb der eigenen, lokalen IT-Infrastruktur **KANN** die Validierung auch durch marktübliche Signaturprüfkomponenten ohne Einbindung eines qualifizierten Validierungsdienstes erfolgen.
Dokumente, die vor dem Inkrafttreten des Durchführungsrechtsakts (EU) 2015/1506 und Vertrauensdienstegesetzes, jedoch nach dem Inkrafttreten des [EGovG] signiert oder zeitgestempelt wurden, sind unabhängig von den o. g. Formaten anzunehmen (siehe § 2 Abs. 1 [EGovG]).

Bei jeder Signatur-/Siegel-/Zeitstempelprüfung, z.B. im Postein-/-ausgang, während der Bearbeitung oder bei der Langzeitspeicherung, müssen die Validierungsdaten zur Signatur/Siegel/Zeitstempel in geeigneter Weise im entsprechenden Datenobjekt abgelegt bzw. anderweitig gespeichert werden.

Sofern elektronische Signaturen/Siegel/Zeitstempel vorliegen, für welche die Validierung nicht zu einem eindeutig bestimmten Ergebnis, sondern zu „**INDETERMINATE**“ gemäß [ETSI EN 319 102-1] (Kap. 5.1.1) führt[2], wird die Speicherung der Daten inklusive des Validierungsergebnisses und die nachfolgende, möglicherweise manuelle, Behandlung und Prüfung der Datenobjekte durch sachkundige Personen, z.B. Informationssicherheitbeauftragter, Systemverantwortliche für die Signaturkomponenten, Vertrauensdiensteanbieter etc., **EMPFOHLEN**.

[2] Dies kann z.B. dann der Fall sein, wenn der Signaturzeitpunkt mangels Zeitstempel oder Evidence Record nicht eindeutig bestimmbar ist. Außerdem kann dies bei „Alt-Signaturen“ und entsprechenden Zeitstempeln, die vor Inkrafttreten des [**VDG**] erzeugt wurden, und für die eine vollständige Signaturprüfung nicht mehr ohne weiteres möglich ist (z.B. da der Zertifizierungsdiensteanbieter keine Zertifikatsstatusinformation mehr bereitstellt und diese auch im dauerhaften Verzeichnis DA:VE nicht vorhanden sind) oder auf Grund von anderen technischen Problemen (z.B. auf Grund von Abweichungen von den einschlägigen technischen Standards) der Fall sein.

4 Erzeugung von Signaturen und Siegeln

Bei der Erzeugung mindestens fortgeschrittener elektronischer Signaturen und Siegel **MÜSSEN** die im Durchführungsrechtsakt [(EU) 2015/1506] (Vgl. Anlage 1) oder in [TR-ESOR-F, (A5.1-1) - (A5.1-4)][3] definierten Formaten (für XML, CMS- und PDF-Signaturen) mit geeigneten Konformitätsstufen verwendet werden.

Aus Gründen der Praktikabilität wird EMPFOHLEN, bei der Erzeugung mindestens fortgeschrittener elektronischer Signaturen und Siegel die Formate CAdES und PAdES mit geeigneten Konformitätsstufen gemäß dem Durchführungsrechtsakt [(EU) 2015/1506] zu verwenden.

Sofern die erstellte elektronische Signatur / das elektronische Siegel unmittelbar nach der Erzeugung in ein System zur Beweiswerterhaltung (TR-ESOR) eingespeist wird und der Empfänger der Signatur bzw. des Siegels später den zugehörigen Evidence Record abrufen kann oder diesen zusammen mit der Signatur bzw. dem Siegel erhält, müssen keine weiteren Zeitstempel in die Signatur bzw. das Siegel eingefügt werden, d.h. es genügt die Konformitätsstufe B des entsprechenden AdES-Formats Sofern dies nicht gegeben ist, wird die Erzeugung von digitalen Signaturen (zumindest) im entsprechenden AdES-T-Format **EMPFOHLEN**.

Sofern die Erzeugung (qualifizierter) elektronischer Signaturen_und Siegel als Dienst für weitere **externe** Behörden, z.B. bei einem IT-Dienstleister des Bundes, erbracht wird, **MUSS** ein qualifizierter Vertrauensdienst zur Erzeugung (qualifizierter) elektronischer Signaturen und Siegel genutzt werden.

Sofern die Erzeugung (qualifizierter) elektronischer Signatur-/ und Siegelzertifikate als Dienst für weitere **externe** Behörden, z.B. bei einem IT-Dienstleister des Bundes, erbracht wird, **MUSS** ein qualifizierter Vertrauensdienst zur Erzeugung (qualifizierter) elektronischer Signaturen- und Siegelzertifikate genutzt werden.

Bei Erzeugung der (qualifizierten) elektronische Signatur und Siegel durch eine Behörde für sich selbst in ihrer eigenen IT-Infrastruktur **KÖNNEN** die (qualifizierten) elektronischen Signaturen bzw. Siegel auch durch die Behörde selbst (z.B. auf Basis einer Signaturkarte) oder per Anfrage bei einem (qualifizierten) Vertrauensdiensteanbieter (als Fernsignatur) erzeugt werden.

[3] Formate gem. EN 319 122, EN 319 132, EN 319 142, EN 319 162

5 Erzeugung von Zeitstempeln

Die Erzeugung qualifizierter elektronischer Zeitstempel **MUSS** definitionsgemäß durch einen qualifizierten Vertrauensdienst zur Erzeugung qualifizierter elektronischer Zeitstempel erfolgen.

Die erzeugten Zeitstempel **MÜSSEN** konform zu [IETF RFC3161] und [IETF RFC5816] sein. [4]

[4] Vgl. [ISO14533] sowie [ETSI TS119512]

6 Erzeugen und Validierung von XML-basierten „ArchivInformationsPakete ((L)XAIP)“

Als Stand der Technik für konkrete Produkte zur Beweiswerterhaltung gilt in Deutschland gem. § 6 [EGovG] sowie § 15 [VDG][5] die [TR-ESOR], aktuell ab V1.2.1, die insbesondere die Anforderungen des im Januar 2020 publizierten europäischen ETSI-Standards für Bewahrungsdienste [ETSI TS119512] hinsichtlich des Formats für technische Beweisdaten „Evidence Record“ gemäß [ETSI TS119512, Kap. A] [6] und des Formats für Bewahrungsobjekt-Formate XAIP [ETSI TS119512, Kap. A.3.2] enthält.

Die [TR-ESOR], V1.2.2 und höher, integriert unter anderem zusätzlich die Anforderungen des im Januar 2020 publizierten europäischen ETSI-Standards für Bewahrungsdienste [ETSI TS119512] insbesondere hinsichtlich der Interoperabilitätsschnittstelle „ETSI TS119512“ ([ETSI TS119512, Kap. 5.3]).

Zur Beweiswerterhaltung **MUSS** demgemäß ein XML-basiertes „ArchivInformationsPaket (L)XAIP gemäß **([TR-ESOR-F], Kap. 3)** “, identifiziert durch die URL

`http://www.bsi.bund.de/tr-esor/xaip/1.2`

gemäß [ETSI TS 119 512] und [TR-03125-F], basierend auf [ISO 14721 (OAIS)] und [ISO 13527 (XFDU)], erzeugt und geprüft werden. Vor dem Hintergrund der entstandenen Standards [ETSI TS 119 511] und [ETSI TS 119 512] für Bewahrungsdienste für elektronische Signaturen, Siegel, Zeitstempel und (signierte) Daten gemäß der eIDAS-Verordnung plant das Bundesamt für Sicherheit in der Informationstechnik (BSI), ein Prüfwerkzeug für (L-)XAIP gemäß [TR-03125-F] als Open Source zur Verfügung zu stellen.

[5] Vgl . BDrs 18/12494

[6] Für die Prüfung ist der Einsatz eines [TR-ESOR] konformen Produkts notwendig, darüber hinaus kann für die Prüfung eines Evidence Records das OpenSource-Tool des BSI verwendet werden: https://github.com/ervta/ERVerifyTool.

7 Erzeugung und Validierung von Evidence Records

Evidence Records **MÜSSEN** gemäß [TR-ESOR-ERS, „Basis-ERS-Profil“ bzw. „Basis-XERS-Profil“][7] erzeugt sowie gemäß diesem Basisprofil bzw. den diesen zu Grunde liegenden Standards [IETF RFC 4998] bzw. [IETF RFC 6283] geprüft werden. Vor dem Hintergrund der entstandenen Standards [ETSI TS 119 511] und [ETSI TS 119 512] für Bewahrungsdienste für elektronische Signaturen, Siegel, Zeitstempel und (signierte) Daten gemäß der eIDAS-Verordnung hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) der offenen eIDAS-Community[8] ein Prüfwerkzeug für Evidence Records gemäß [IETF RFC 4998] sowie [TR-ESOR-ERS, „Basis-ERS-Profil“] als Open Source zur Verfügung gestellt[9].

[7] Vgl. auch ETSI TS 119 512
[8] Hersteller, Vertrauensdiensteanbieter, Anwender, Standardisierungsgremien
[9] Siehe https://github.com/ervta/ERVerifyTool.

8 Besonderheiten in der Beweiswerterhaltung kryptographisch signierter Dokumente

8.1 Grundsatz

Sofern die Bewahrung (qualifizierter) elektronischer Signaturen, Siegel und Zeitstempel als Dienst gegenüber weiteren externen Behörden (z.B. IT-Dienstleister des Bundes) erbracht wird, **MUSS** die Bewahrung durch einen qualifizierten Vertrauensdienst für die Bewahrung von (qualifizierten) elektronischen Signaturen, Siegel und Zeitstempel mittels digitaler Signaturtechniken gemäß [TR-ESOR] erfolgen[10].

Der qualifizierte Bewahrungsdienst **MUSS** gemäß [ETSI EN 319 401] und [ETSI TS 119 511] konformitätsgeprüft worden sein, wobei **EMPFOHLEN** wird, die Konformitätsprüfung bzw. Zertifizierung auf Basis von [Ass 319 401] und [Ass 119 511] durchzuführen. Als Stand der Technik für das eingesetzte Bewahrungs-Produkt **MUSS** in jedem Fall, auch wenn die Bewahrung nicht durch einen qualifizierten Bewahrungsdienst erfolgt, gem. [EGovG] und [VDG] ein [TR-ESOR]-zertifiziertes Produkt angewendet werden.

Weitere Details finden sich in Kap. 4.2.1.1 ff. [TR-ESOR]: https://www.bsi.bund.de/tr-esor. Hinsichtlich der Beweiswerterhaltung mindestens fortgeschrittener elektronischer Signaturen, Siegel und qualifizierter Zeitstempel sowie der zugehörigen signierten Daten **MÜSSEN** die Vorgaben der [TR-ESOR] zur langfristigen Beweiswerterhaltung gemäß [ETSI TS 119 511, Kapitel 7.15], [ETSI TS 119 512, Anhang F.1.6], [VDG, § 15], und [TR-ESOR M.3] auf Basis von Evidence Records gemäß [TR-ESOR-ERS], [IETF RFC 4998] und [IETF RFC 6283] sowie die Vorgaben zum Bewahrungs-Protokoll gemäß [ETSI TS 119 512] bzw. [TR-ESOR-E] mit [TR-ESOR-APP] im jeweils aktuellen Stand beachtet werden.

Weitere wesentliche Ausführungen zur Erzeugung und Validierung kryptographischer Signaturen, Siegel, qualifizierter Zeitstempel, Zertifikatsformate, Zertifikatsvalidierungsformate und Evidence Records finden sich insbesondere in Kap. 5 [TR-ESOR M.2] sowie Kap. 5 [TR-ESOR F].

Sofern die Validierung als IT-Dienst gegenüber weiteren externen Behörden erbracht wird, **MUSS** die Validierung (qualifizierter) elektronischer Signaturen, Siegel und Zeitstempel durch einen qualifizierten Validierungsdienst durchgeführt werden. Erfolgt die Validierung bzw. Bewahrung durch eine Behörde selbst in ihrer eigenen, lokalen IT-Infrastruktur, so **KANN** die Validierung (qualifizierter) elektronischer Signaturen/Siegel und Zeitstempel auch durch die Behörde selbst oder per Anfrage bei einem externen Vertrauensdiensteanbieter durchgeführt werden.

Die Prüfberichte für Signaturen, Siegel, Zeitstempel, Evidence Records und (L)XAIP gemäß (**[TR-ESOR-F], Kap. 3) MÜSSEN** gem. Stand der Technik erzeugt werden (vgl. [ETSI TS119102-2], [OASIS-VR], [OASIS VR-XSD] und [TR-ESOR-VR]).

Bei der Beweiswerterhaltung **MUSS** hinsichtlich sicherheitsgeeigneter Signatur- und Hashalgorithmen [ETSI TS 119 312] sowie [SOG-IS] im jeweils aktuellen Stand beachtet werden.

Um eine langfristige Prüfbarkeit der (qualifizierten) elektronischen Signaturen und Siegel sowie qualifizierten Zeitstempel sowie deren Beweiswerterhalt zu gewährleisten, wird **EMPFOHLEN**, die signierten/gesiegelten/zeitgestempelten Dokumente frühzeitig an ein TR-ESOR-System zur Beweiswerterhaltung kryptographisch signierter Dokumente nach dem Stand der Technik zu übergeben, das durch die Behörde selbst betrieben wird oder das von einem qualifizierten Bewahrungsdienst (z.B. IT-Dienstleister des Bundes) angeboten wird.

[10] Gem. § 6 E-Government-Gesetz Bund sowie § 15 Vertrauensdienstegesetz gilt die TR-ESOR als verbindlicher Stand der Technik zur Beweiswerterhaltung. Für Bundesbehörden ist zu dem § 8 Abs. 2 [BSIG] für die Anwendung Technischer Richtlinien des BSI zu beachten.

Je älter das Dokument sowie dessen kryptographische Signatur/Siegel/Zeitstempel, desto höher ist das Risiko, eine vorherige Manipulation nicht mehr nachweisen zu können und der ursprüngliche Beweiswert nicht mehr besteht, da die zugrundeliegenden Algorithmen aufgrund Veraltens angreifbar und damit nachrechenbar werden oder die Gültigkeit der Zertifikate gemäß Gültigkeitsmodell erlischt.

Einem qualifizierten Bewahrungsdienst des Bundes wird **EMPFOHLEN**, gegenüber **allen** den (qualifizierten) Vertrauensdienst nutzenden Behörden festzuschreiben, dass eine Bewahrung des Beweiswertes einer elektronischen Signatur, eines elektronischen Siegels oder eines elektronischen Zeitstempels nur erfolgen kann, wenn dieser Beweiswert zum Zeitpunkt der Übergabe an den qualifizierten Bewahrungsdienst noch vorhanden war. Ein vorheriger Beweiswertverlust kann nicht geheilt werden. Für die Bewahrung des Beweiswertes vor der Übergabe bzw. die Abschätzung, bis zu welchem Zeitpunkt keine Bewahrung erforderlich ist, ist die Behörde selbst verantwortlich.

Anlage 1: Übersicht der verpflichtenden Signatur- und Siegelformate

Alle mindestens fortgeschrittenen elektronischen Signaturen und Siegel **MÜSSEN**[11] den unten genannten Baseline Profiles einer/einem der folgenden technischen Spezifikationen und Standards des europäischen Normungsinstituts ETSI mit einer geeigneten Konformitätsstufe[12] entsprechen:

Format	**Verpflichtende Standards**
CAdES Baseline Profile (CMS-Signaturen/Siegel)	[ETSI TS 103 173] ETSI TS 103173 v.2.1.1 bzw. [ETSI EN 319 122-1] ETSI EN 319 122-1 v1.1.1
XAdES Baseline Profile (XML-Signaturen/Siegel)	[ETSI TS 103 171] ETSI TS 103171 v.2.2.1 bzw. [ETSI EN 319 132-1] ETSI EN 319 132-1 v1.1.1
PAdES Baseline Profile (PDF-Signaturen/Siegel)	[ETSI TS 103 172] ETSI TS 103172 v.2.2.2 bzw. [ETSI EN 319 142-1] ETSI EN 319 142-1 v1.1.1
ASiC-Baseline-Profile (ASiC-Signatur-Containerdateien)	[ETSI TS 103174] ETSI TS 103174 v.2.2.1 bzw. [ETSI EN 319 162-1] ETSI EN 319 162-1 v1.1.1

Tabelle 1: Signatur- und Siegelformate

[11] mit Ausnahme der für die Langzeitspeicherung vorgesehenen Klausel
[12] Vgl. Kapitel 4.

Anlage 2: Übersicht der verpflichtenden Zeitstempel- und Evidence Record - Formate und Bewahrungsobjekt-Format

Zeitstempel

Format	Verpflichtende Standards
Zeitstempel	[IETF RFC3161] und [IETF RFC5816]

Tabelle 2: Zeitstempel - Formate

Evidence Records

Erzeugung

Format	Verpflichtende Standards
TR-ESOR-ERS, „Basis-ERS-Profil“ bzw. „Basis-XERS-Profil	[TR-ESOR-ERS]

Tabelle 3: Evidence Record Formate zur Erzeugung

Validierung

Format	Verpflichtende Standards
TR-ESOR-ERS, „Basis-ERS-Profil“ bzw. „Basis-XERS-Profil bzw. diesem Profil zugrundeliegende nachstehenden RFCs	[TR-ESOR-ERS]
ASN.1-basierte Evidence Record	[IETF RFC 4998]
XML-basierte Evidence Record	[IETF RFC 6283]

Tabelle 4: Evidence Record – Formate zur Prüfung

Bewahrungsobjekte

Format	Verpflichtende Standards
(L)XAIP	[ETSI TS 119 512] und [TR-ESOR]

Tabelle 5: Bewahrungsobjekt - Formate

Literaturverzeichnis

[Ass 319 401] BSI, *Criteria for Assessing Trust Service Providers against ETSI Policy Requirements, Part 1: Assessment Criteria for all TSP - ETSI EN 319 401*

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

[(EU) 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.

[EGovG] Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz - EGovG) vom 25.07.2013

[eIDAS-VO] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG“ vom 23.07.2014

[eIDAS-DG] Gesetz zur Durchführung der 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. Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 52, ausgegeben zu Bonn am 28. Juli 2017

[ETSI EN 319 102-1]ETSI EN 319 102 – 1, *Electronic Signatures and Infrastructers (ESI); Procedures for Creation and Validation of AdES Digital Signatures*; *Part 1: Creation and Validation,* v1.1.1, (2016-05), siehe unter http://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.01_60/en_31910201v010101p.pdf

[ETSI EN 319 122-1] ETSI EN 319 122 – 1, *Electronic Signatures and Infrastructers (ESI); CAdES digital signatures, Part 1: Building blocks and CAdES baseline signatures*, v1.1.1, (2016-04), siehe unter http://www.etsi.org/deliver/etsi_en/319100_319199/31912201/01.01.01_60/en_31912201v010101p.pdf

[ETSI EN 319 132-1] ETSI EN 319 132 – 1, *Electronic Signatures and Infrastructures (ESI); XAdES digital signatures, Part 1: Building blocks and XAdES baseline signatures*, v1.1.1, (2016-04), siehe unter

http://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.01.01_60/en_31913201v010101p.pdf

[ETSI EN 319 142-1] ETSI EN 319 142 – 1, *Electronic Signatures and Infrastructeres (ESI); PAdES digital Signatures, Part 1: Building blocks and PAdES baseline signatures*, v1.1.1 (2016-04), siehe unter http://www.etsi.org/deliver/etsi_en/319100_319199/31914201/01.01.01_60/en_31914201v010101p.pdf

[ETSI EN 319 162-1] ETSI EN 319 162 – 1, *Electronic Signatures and Infrastrucutres (ESI); Associated Signature Containers (ASiC), Part 1: Building blocks and ASiC baseline containers*, v1.1.1 (2016-04), siehe unter http://www.etsi.org/deliver/etsi_en/319100_319199/31916201/01.01.01_60/en_31916201v010101p.pdf

[ETSI EN 319 401] ETSI EN 319 401, *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*. ETSI v2.2.1 (2018-04)

[ETSI TS 103 171] ETSI TS 103 173, *Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile*, v.2.1.1 (2012-03), http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf

[ETSI TS 103 172] ETSI TS 103 172, *Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile,* v.2.2.2 (2013-04), https://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf

[ETSI TS 103 173] ETSI TS 103 173, *Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile*, v.2.2.1 (2013-04), http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf

[ETSI TS 103 174] ETSI TS 103 174, *Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile,* v.2.2.1 (2013-06), https://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf

[ETSI TS 119 511] 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,* V1.1.1 (2019-06), https://www.etsi.org/deliver/etsi_ts/119500_119599/119511/01.01.01_60/ts_119511v010101p.pdf

[ETSI TS 119 512] ETSI TS 119 512, *Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services,* V1.1.1 (2020-01), https://www.etsi.org/deliver/etsi_ts/119500_119599/119512/01.01.01_60/ts_119512v010101p.pdf

[IETF RFC2119] IETF RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels,* https://www.ietf.org/rfc/rfc2119.txt

[IETF RFC3161] IETF RFC 3161, *Time-Stamp Protocol (TSP)*, https://www.ietf.org/rfc/rfc3161.txt

[IETF RFC4998] IETF RFC 4998, *Evidence Record Syntax (ERS),* https://www.ietf.org/rfc/rfc4998.txt

[IETF RFC5816] IETF RFC 5816 ‚*ESSCertIDv2 Update for RFC 3161,* https://www.ietf.org/rfc/rfc5816.txt

[IETF RFC6283] IETF RFC 6283, *Extensible Markup Language Evidence Record Syntax (XMLERS)*, https://www.ietf.org/rfc/rfc6283.txt

[MiniKGovG] Bundesministerium des Innern, *Minikommentar zum Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften*, Berlin 2013

[OASIS VR] Hühnlein, D., *OASIS DSS v1.0 Profile for Comprehensive Multi-Signature Verification Reports Version 1.0*, Committee Specification 01, 12 November 2010, http://docs.oasis-open.org/dss-x/profiles/verificationreport/oasis-dssx-1.0-profiles-vr-cs01.pdf

[SigG] Gesetz über die Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (SigG), vom 16.5.2001, BGBl. 2001, Teil I Nr. 22, S. 876 ff., geändert durch Art 1 G v. 4.1.2005 I 2, zuletzt durch Art. 4 G v. 17.07.2009

[SigV] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV), vom 16.11.2001, BGBl. 2001, Teil I Nr. 59, S. 3075 ff., geändert durch Art 2 G v. 4.1.2005 I 2, zuletzt durch Art. 1 ÄndVO v. 15.11.2010

[SOG-IS] SOG-IS Crypto Working Group: *SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms*, https://www.sogis.org/uk/supporting_doc_en.html

[TR-ESOR] BSI TR 03125: *Beweiswerterhaltung kryptographisch signierter Dokumente, Hauptdokument,* V1.2.1 und höher, https://www.bsi.bund.de/tr-esor

[TR-ESOR-E] BSI TR 03125: *Beweiswerterhaltung kryptographisch signierter Dokumente: Anlage TR-ESOR-E Konkretisierung der Schnittstelle auf Basis des eCard-API-Frameworks,* v 1.2.1 und höher

[TR-ESOR-E-APP] BSI TR 03125: *Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage TR-ESOR-TRANS TRESOR-E-Appendix,* v1.2.2, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf

[TR-ESOR-ERS] BSI TR 03125: *Beweiswerterhaltung kryptographisch signierter Dokumente: Anlage TR-ESOR-ERS Evidence Record gemäß RFC4998 und RFC6283*, v1.2.1 und höher

[TR-ESOR-F] BSI TR 03125: *Beweiswerterhaltung kryptographisch signierter Dokumente: Anlage TR-ESOR-F Formate und Protokolle*, v1.2.1 und höher

[TR-ESOR-M.1 [BSI TR 03125: *Beweiswerterhaltung kryptographisch signierter Dokumente: Anlage TR-ESOR-M.1 ArchiSafe Modul,* v1.2.1 und höher

[TR-ESOR-M.2] BSI TR 03125: *Beweiswerterhaltung kryptographisch signierter Dokumente: Anlage TR-ESOR-M.2 Krypto-Modul,* v1.2.1 und höher

[TR-ESOR-M.3] BSI TR 03125: *Beweiswerterhaltung kryptographisch signierter Dokumente: Anlage TR-ESOR-M.3 ArchiSig-Modul,* v1.2.1 und höher

[TR-ESOR-VR] BSI TR 03125: *Preservation of Evidence of Cryptographically Signed Documents: Annex TR-ESOR-VR: Verification Reports for Selected Data Structures,* v1.2.1 und höher

[XFDU] ISO 13527:2010, Space data and information transfer systems – XML formatted data unit (XFDU) structure and construction rules, 2010

[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

[VDV] Verordnung zu Vertrauensdiensten (Vertrauensdiensteverordnung - VDV) vom 15. Februar 2019. (BGBl. I S. 114-115)