Beweiswerterhaltung im Kontext eIDAS – Eine Fallstudie

Steffen Schwalm[1] · Ulrike Korte[2] · Detlef Hühnlein[3]
Tomasz Kusber[1]

[1]BearingPoint GmbH
{Steffen.Schwalm | Tomasz.Kusber}@bearingpoint.com

[2]BSI
Ulrike.Korte@bsi.bund.de

[3]ecsec GmbH
Detlef.Huehnlein@ecsec.de

Zusammenfassung

Es besteht eine hohe Notwendigkeit, nicht nur in der öffentlichen Verwaltung, sondern auch in Unternehmen, Geschäftsprozesse zu digitalisieren und für die elektronischen Dokumente und Daten auch in ferner Zukunft die Lesbarkeit, Verfügbarkeit sowie die Integrität, Authentizität und Verkehrsfähigkeit über Jahre bis hin zu Jahrzehnten gewährleisten zu müssen. Gleichzeitig erfordert der europäische Binnenmarkt länderübergreifend, sichere wie nachweisbare elektronische Geschäftsprozesse. Seit September 2014 gilt die EU-Verordnung Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG. Sie schafft eine europaweit verbindliche Grundlage für die vertrauenswürdige elektronische Interaktion zwischen Bürgern, Unternehmen und öffentlichen Verwaltungen. Mit der Schaffung gemeinsamer Formate für Signaturen, Siegel und Zeitstempel durch begleitende ETSI- und CEN-Normen sowie der verbindlichen Definition von der Rechtswirkung der Signaturen etc. liefert die eIDAS-Verordnung zudem eine Basis zur langfristigen Nachweisbarkeit elektronischer Transaktionen, die allerdings bislang schwerpunktmäßig auf die Beweiswerterhaltung je Signatur fokussiert – also relativ hohem Aufwand erzeugt. Mit dem Ziel einer wirtschaftlichen, beweissicheren Archivierung wurde von den Autoren mit einem europäischen Konzern im Rahmen einer Case Study eine Lösung entwickelt, welche die Formate gem. ETSI mit der Nutzung von Hashbäumen gem. RFC 4998/6283 kombiniert und zugleich die Interoperabilität unterschiedlicher technischer Beweisdaten gewährleistet.

1 Einleitung

1.1 Information- und Beweiswerterhaltung im Überblick

Um elektronische Unterlagen langfristig beweissicher aufzubewahren, gilt es, deren Authentizität, Integrität, Verkehrsfähigkeit und Verfügbarkeit zu gewährleisten. Elektronische Dokumente liefern jedoch aus sich heraus keine Hinweise für ihre Integrität und Authentizität sowie die Ordnungsmäßigkeit im elektronischen Rechts- und Geschäftsverkehr. Gleichzeitig

P. Schartner (Hrsg.) · D•A•CH Security 2016 · syssec (2016) 379-392.

bestehen jedoch umfassende Dokumentations- und Aufbewahrungspflichten, deren Dauer zwischen zwei und 110 Jahre oder gar dauernd umfasst. Während dieser Fristen muss es zudem möglich sein, die Dokumente Prüfbehörden oder Gerichten vorzulegen und anhand der Daten die genannten Nachweise zu führen (Verkehrsfähigkeit) und somit auch deren Lesbarkeit zu gewährleisten. Die Nutzung kryptographischer Sicherungsmittel wie qualifizierte elektronischer Signaturen, Siegel oder Zeitstempel ermöglicht nach geltendem Recht und fachlichen Standards die langfristige Beweiswerterhaltung sowohl signierter als auch unsignierter Unterlagen. Insofern sind von Behörden wie Unternehmen Vorkehrungen zur treffen, die sowohl die Informations- als auch Beweiswerterhaltung gem. aktueller Standards und Normen ermöglichen. Wesentliche Basis bildet ein ordnungsgemäßes Records Management, welches anhand klarer Richtlinien, Verantwortlichkeiten und Prozesse die Identifikation und strukturierte wie anforderungsgerechte Ablage geschäftsrelevanter Unterlagen gewährleistet (vgl. [ISO30301, ISO15489, ISO18128, ISO18829]).

Darüber hinaus das OAIS-Modell [ISO14721] und die [ISO16363, DIN31644, DIN31645] die Prozesse und Informationspakete zur Informationserhaltung innerhalb eines vertrauenswürdigen digitalen Langzeitarchivs (dLZA), während die [DIN31647] die notwendigen Funktionen und Informationen zur Beweiswerterhaltung in einem OAIS-konformen dLZA beschreibt und damit die Verbindung zu den technischen Normen zur Beweiswerterhaltung bildet (vgl. [ISO14533, EN319122, EN319132, EN319142, EN319162, RFC4998, RFC6283]). Die [TR03125] wiederum beschreibt eine mögliche Referenzarchitektur eines Systems zur Beweis- und Informationserhaltung elektronischer Unterlagen mit daraus abgeleiteten Anforderungen. Sie integriert die Anforderungen aus ETSI[1] und IETF ([RFC 4998/6293]). Im praktischen Fall des betrachteten Unternehmens war diese Referenzarchitektur ein integraler Bestandteil des dLZA – als eigenständiges Modul zur Beweiswerterhaltung gem. OAIS.

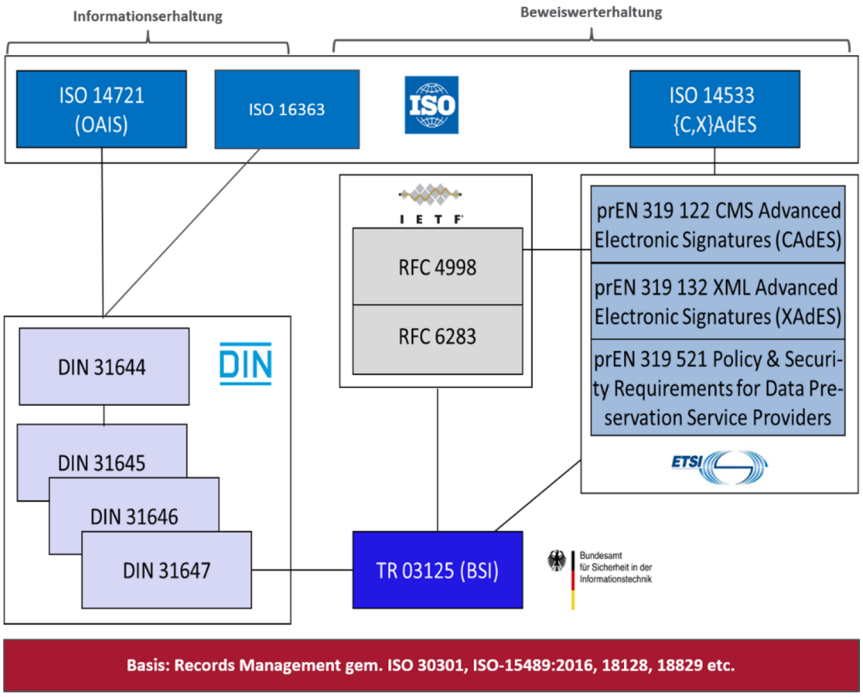

Abb. 1: Standards und Normen zur beweissicheren Aufbewahrung

[1] Empfehlung für Verwendung von {C,X,P}AdES als Signaturformat zu verwenden.

1.2 Rechtlicher Rahmen in Deutschland und Europa

Mit der eIDAS-Verordnung liegt eine EU- und EFTA-weit einheitliche Vorgabe für vertrauenswürdige elektronische Geschäftsprozesse vor. Deren Umsetzung wird einerseits durch weitere EU-Vorgaben wie z.B. die [EU-DLR], andererseits durch Branchenvorgaben determiniert, so z.B. FDA[2] oder GxP[3] im Gesundheitswesen und Pharma, [EuroSOX] sowie Vorgaben von EASA[4], FAA[5] bzw. Luftfahrtbundesamt und z.B. Vorgabe zum Haftungsrecht [BGB]. Diese erfordern jeweils die Nachvollziehbarkeit und mögliche Prüfbarkeit der erzeugten Unterlagen durch Prüfbehörden und Dritte wie z.B. Gerichte.

In Deutschland ist eine weitgehende Digitalisierung der Bundesbehörden bis das Jahr 2020 (z.B. Einführung einer führenden E-Akte, Umsetzung vom rechtsicheren ersetzenden Scannen oder Implementierung von beweiswerterhaltenden Aufbewahrungsdienste) durch das sog. E-Government Gesetz (vgl. [EGovG]) festgeschrieben. Äquivalentes ist für die Behörden der Länder und Kommunen bereits umgesetzt oder zu erwarten. Gleichzeitig besteht zum einen weiterhin die Verpflichtung, behördliche Entscheidungen prüfbar und damit bis zum Ablauf der geltenden Aufbewahrungsfristen gerichtsfest zu halten, zum anderen gilt die TR-03125 des BSI als Stand der Technik zur Beweiswerterhaltung.

Insbesondere die eIDAS-Verordnung, mit ihrer unmittelbaren Wirkung auf der nationalen Ebene sowie den verbindlichen technischen Standards harmonisiert zum einen die europäischen Lösungen für z.B. Signaturen, Zeitstempel, Siegel und stellt zum anderen Weichen für die Interoperabilität der Lösungen im Bereich eID, was, verbunden mit Erleichterungen bei der Signaturerzeugung (Serversignaturen, Siegel), absehbar die Menge signierter Dokumente spürbar erhöhen wird. Die eIDAS-Verordnung war ein wesentlicher Grund zur Etablierung eines konzernweit einheitlichen Vorgehens zur beweissicheren Archivierung auf Basis europaweit verbindlicher Standards und Normen im betroffenen europäischen Unternehmen.

1.3 Typische Ansätze für die Beweiswerterhaltung

Hinsichtlich der Beweiswerterhaltung elektronischer Unterlagen können grundsätzlich zwei unterschiedliche Ansätze genannt werden.

- der AdES/ASiC basierte, der entsprechend durch korrespondierende europäische Normen gegeben wird (vgl. Abbildung 1, rechts):
  - ein separates Vorgehen für jede Art von elektronischen Signaturen bzw. Siegeln[6]
  - mehrheitlich ein Archivzeitstempel pro zu erhaltender Signatur bzw. zu erhaltendem Siegel, außer beim ASIC-Ansatz [EN319162]
- ein RFC-basierter Ansatz, der auch im Rahmen der technischen Richtlinie des BSI [TR03125] verwendet wird (vgl. Abbildung 1 Mitte)

---

[2] FDA – Food and Drug Administration

[3] Sammlung von Guten Arbeitspraxis Richtlinien, z.B. GCP – Good Clinical Practice oder GLP – Good Laboratory Practice etc.

[4] EASA – European Aviation Safety Agency

[5] FAA – Federal Aviation Administration

[6] Da elektronische Signaturen und Siegel sich technisch faktisch nur dadurch unterscheiden, ob sich das zugrundeliegende Zertifikat auf eine natürliche Person (elektronische Signatur) oder eine juristische Person (elektronisches Siegel) bezieht, sind die Maßgaben zur Beweiswerterhaltung faktisch gleich. Beide kryptographische Mittel werden insofern unter dem Begriff „elektronische Signatur“ zusammen betrachtet.

- ein Vorgehen für alle Arten von elektronischen Signaturen/Siegeln
- ein Archivzeitstempel für beliebig viele zu erhaltende Signaturen/Siegel

Die erste Variante ist Gegenstand, der bisher bei ETSI entwickelten Standards[7], auf der zweiten Variante basieren die IETF-Standards [RFC4998] und [RFC6283], die [TR3125] des BSI sowie zahlreiche internationale Produkte und Implementierungen für die Beweiswerterhaltung. [ISO14533] unterstützen beide Ansätze.

Die beiden Ansätze wurden im Zuge der Case Study verglichen und eine Lösung zur weitgehenden technischen Interoperabilität beider Optionen entwickelt. Darüber hinaus entstand eine allgemeingültige, wie übertragbare Handlungsempfehlung, die so derzeit vom erwähnten Unternehmen umgesetzt wird. Dabei ist zu beachten, dass das Unternehmen eine hohe Anzahl elektronischer Unterlagen verarbeitet – im aktuellen dLZA werden über 180 Mio. Datenobjekte mit jeweils mehreren Dateien aufbewahrt – eine Datenmenge, wie sie auch bei anderen internationalen Konzernen entsteht (z.B. Bankwesen, Versicherungswesen etc.).

2 Lösungswege zur Beweiswerterhaltung

2.1 Grundsatz

Grundsätzlich umfasst die praktische Umsetzung der Beweiswerterhaltung kryptographisch gesicherter Dokumente die folgenden Schritte:

- Beilegung aller Informationen, die für die Offline-Prüfung der zugrundeliegenden Signatur notwendig sind (Zertifikate und Sperrmaterial), also der beweisrelevanten Daten
- Erzeugung der technischen Beweisdaten
- Zeitliche Erneuerung der kryptographischen Mechanismen im Falle des drohenden Verlusts der Sicherheitseignung der zugrundeliegenden Signatur- und Hashalgorithmen:
  - Signaturerneuerung – im Falle, dass der zugrundeliegende Signaturalgorithmus in absehbarer Zeit schwach wird,
  - Hashwerterneuerung – im Fall, dass der verwendete Hashalgorithmus in absehbarere Zeit schwach wird.

2.2 Beweiswerterhaltung nach ETSI

Gemäß ETSI und den hierauf verweisenden Ausführungsbestimmungen der eIDAS entstehen aktuell für die folgenden vier unterschiedlichen Signaturarten jeweils sogenannte Basis Profile, die von den Mitgliedsstaaten der EU verbindlich zu unterstützen sein werden:

- CMS-basierte Signaturen gem. [EN319122] – CAdES
- XML-basierte Signaturen gem. [EN319132] – XAdES
- PDF-basierte Signaturen gem. [EN319142] – PAdES
- ZIP-basierter Signaturcontainer für CAdES, XAdES sowie Zeitstempel (gem. [RFC3161]) und Evidence Records (gem. [RFC4998] und [RFC6283]) gem. [EN319162] – ASiC.

[7] Kürzlich wurde durch ETSI eine Arbeitsgruppe gegründet, die gegenwärtig untersucht, ob und wie man ggf. die zweite Variante ebenfalls in {C/X}AdES integrieren kann (siehe hierzu z.B. Abschnitt. 2.4).

Die auch durch [eIDAS] geforderte Erneuerung der Signaturen zur Beweiswerterhaltung im Rahmen der Langzeit-Verfügbarkeit und -Integrität erfolgt bei ETSI im Rahmen der aktuellen Basis-Profile mit einem Archivzeitstempel je Signatur – es muss also zwingend eine Signatur vorhanden sein. Bei hohen Datenmengen entsteht also ein vergleichsweise hoher Aufwand zur Beweiswerterhaltung.

2.2.1 CAdES – Beweiswerterhaltung

Gem. CAdES-Basis-Profil-Vorschriften für die Beweiswerterhaltung muss jede einzelne CAdES-Signatur mit Hilfe eines sog. Archive Timestamp Version 3 (ATSv3) abgesichert werden (vgl. [EN319122] und Abbildung 2). Daneben kann jede CAdES-Signatur zu einer CAdES-A-Signatur erweitert werden. Dieses Profil ist notwendig, da nur eine CAdES-A-Signatur die Maßgaben zur Beweiswerterhaltung erfüllt und die Ablage der Verifikationsdaten und Sperrinformationen in den Signaturinformationen ermöglicht. In der Abbildung 1 wird eine beispielhafte Anwendung der CAdES-Beweiswerterhaltung-Regel auf eine TIFF-Datei gezeigt, die dreifach abgesetzt signiert wurde. Es müssen drei ATSv3-Instanzen erzeugt werden.

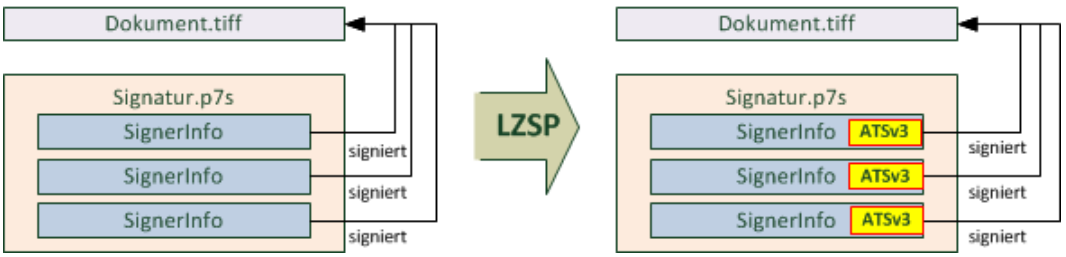

Abb. 2: Beweiswerterhaltung gem. CAdES

Eine erneute Sicherung der Signaturen (Signatur-/Hasherneuerung) würde das Anbringen von weiteren drei ATSv3-Instanzen nach sich ziehen.

Sollten mehrere signierte Dokumente behandelt werden, so ist das Vorgehen für jedes Dokument zu wiederholen. Dabei ist zu beachten, dass das Format ATSv3 nicht vollständig abwärtskompatibel ist – eine zusätzliche Komplexität bei teilweise jahrzehntelangen Aufbewahrungsfristen. Im Rahmen einer CAdES-A-Signatur können aktuell auch Evidence Records außerhalb des Basis-Profils eingesetzt werden, allerdings sind dafür spezielle Bedingungen im Anhang B des [EN319122-1] definiert.

2.2.2 XAdES – Beweiswerterhaltung

Eine analoge Situation zu CAdES ist im Falle der XAdES-Signaturen vorzufinden. Einzelne Signaturen müssen mit Hilfe jeweils eines Archivzeitstempels pro Signatur, sog. *xadesv141:ArchiveTimeStamp* (vgl. [EN319142] und Abbildung 3), zwecks Beweiswerterhaltung versiegelt werden. Ebenso besteht mit XAdES-A ein Profil zur Ablage der Verifikationsdaten und Sperrinformationen je Signatur.

Auch hier müssen im Falle einer Signatur-/Hasherneuerung die einzelnen Instanzen des Zeitstempels erneut separat mit jeweils einem Archivzeitstempel/Signatur versiegelt werden. Gleiches gilt für die Signaturen je Dokument. Es wird also wiederum je Signatur ein eigener Archivzeitstempel angebracht, mit dem entsprechenden Aufwand. Unter speziellen Bedingungen[7] sind aktuell im Rahmen einer XAdES-A-Signatur auch Evidence Records einsetzbar, aber ebenfalls außerhalb des Basis-Profils.

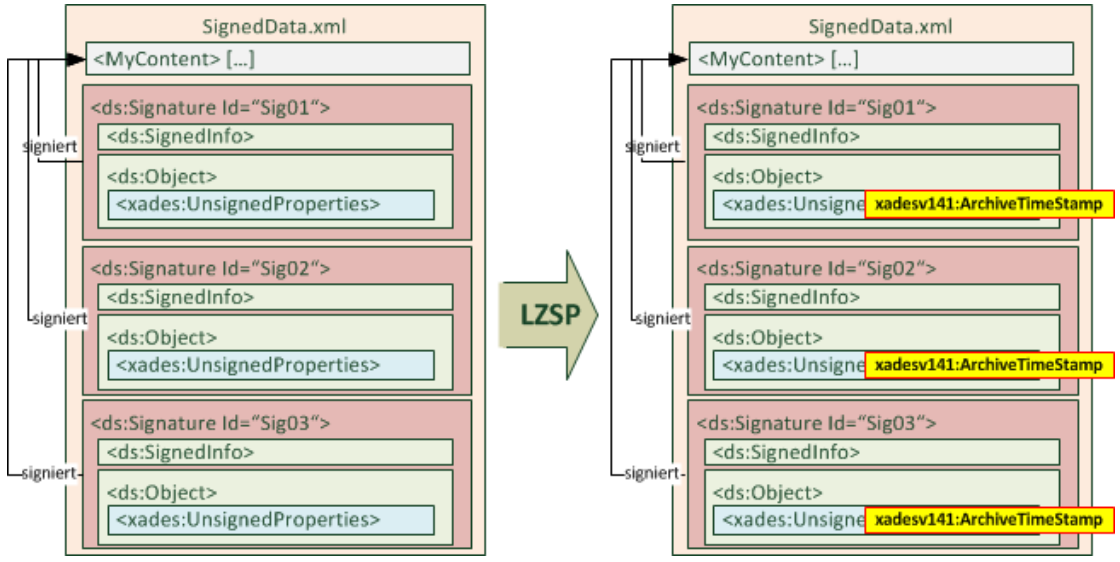

Abb. 3: Beweiswerterhaltung gem. XAdES

2.2.3 ASiC – Beweiswerterhaltung

Die ASiC-Spezifikation [EN319162] definiert einen ZIP-basierten Signaturcontainer, der sowohl CAdES- als auch XAdES-Signaturen, Zeitstempel und Evidence Records (gem. [RFC4998] und [RFC6283]) integrieren kann. Die [EN319162] ermöglicht zur Beweiswerterhaltung die Ablage eines Evidence Records nach [RFC4998/6283] und damit die Nutzung von Hashbäumen zur Beweiswerterhaltung. Dabei ist zu beachten, dass ASiC-S (simple) nur ein Dokument enthalten kann und ASiC-E (extended) die Aufnahme von mehreren Dokumenten ermöglicht. ASiC unterstützt damit als derzeit einziges von ETSI entwickeltes Format explizit die Beweiswerterhaltung auf Basis von Merkle-Hashbäumen (vgl. Absatz 2.3), in dem der in einem RFC4998/6283-konformen System erzeugte und reduzierte Evidence Record im META/INF-Folder des ASIC-Container ebenso abgelegt werden kann, wie Signaturen und Zeitstempel, neben den Inhaltsdaten. Die Langzeit-Validität wird dabei mit den inhärenten Mechanismen gemäß RFC4998/6283 sichergestellt.

2.3 Beweiswerterhaltung gem. IETF RFC4998 / RFC6283

2.3.1 Grundsatz

Beide IETF-Standards zur Beweiswerterhaltung [RFC4998] und [RFC6283] basieren auf den sog. Merkle-Hashbäumen und unterscheiden sich lediglich durch die ausgewählte Technologie für die Abbildung des Evidence Record. Während [RFC4998] ASN.1 nutzt, basiert [RFC6283] auf XML. Im weiteren Verlauf wird ausschließlich die ASN.1 Struktur gem. [RFC4998] betrachtet, da die XML-basierte Variante ähnlich strukturiert ist und in der Praxis derzeit kaum angewendet wird. Die Ergebnisse der Untersuchung lassen sich bei analog auf die Evidence Records gem. [RFC6283] übertragen. Im Gegensatz zu den Format-spezifischen Ansätzen in den ETSI-Spezifikationen kann der RFC4998-basierte Mechanismus für alle Signaturformate sowie auch für unsignierte Dokumente angewendet werden.

2.3.2 RFC4998

Gemäß [RFC4998] werden die zu schützenden Dokumente in einer festgelegten Art und Weise in einem sog. Merkle-Hashbaum gruppiert und anschließend nur der Wurzel-Hashwert mit

einem Zeitstempel[8] (sog. Archivzeitstempel) versiegelt (vgl. [RFC4998], Abschnitt 4.2 und Abbildung 4). Auf dieser Weise kann eine beliebige Anzahl von Dokumenten und Datenobjekten beliebiger Art mit einem einzigen Zeitstempel geschützt werden. Die Beweisdaten werden durch einen sog. Evidence Record (ER), der einen reduzierten Hashbaum und korrespondierten Archivzeitstempel beinhaltet (vgl. [RFC4998], Abschnitt 3) repräsentiert.

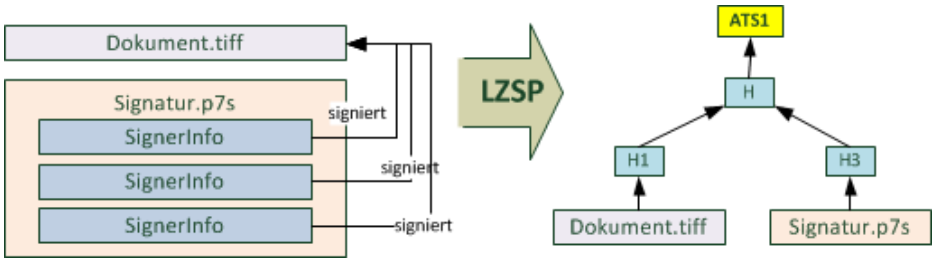

Abb. 4: Beweiswerterhaltung gem. RFC4998

Droht der Signaturalgorithmus des Archivzeitstempels die Sicherheitseignung zu verlieren, so muss einen neuen Archivzeitstempel, der die in der Signatur bereits vorhandenen Zeitstempel umfasst, eingeholt werden – Signaturerneuerung (vgl. [RFC4998], Abschnitt 5.2). Im Falle, dass die Sicherheitseignung des dem Hashbaum zugrundeliegenden Hashalgorithmus in Kürze abläuft, muss ein neuer Hashbaum unter Verwendung eines neuen sicherheitsgeeigneten Hashalgorithmus erzeugt und mit einem neuen Archivzeitstempel versiegelt werden – Hashbaumerneuerung (vgl. [RFC4998], Abschnitt 5.2). Die IETF-Standards [RFC4998] und [RFC6283] ermöglichen so die Beweiswerterhaltung einer beliebigen Anzahl an Signaturen sowie signierter als auch unsignierter Daten mit einem einzigen Archivzeitstempel.

2.3.3 Beweiswerterhaltung gem. BSI TR-03125

Die [TR03125] des BSI integriert die Mechanismen zur Beweiswerterhaltung gem. [RFC4998] bzw. [RFC6283] und kombiniert diese mit grundlegenden Maßgaben zur Informationserhaltung. Sie deckt also grundsätzlich beide Aufgabenbereiche einer beweissicheren Langzeitspeicherung ab (vgl. Absatz 1.1). Die Technische Richtlinie definiert darüber hinaus im Wesentlichen eine Referenzarchitektur für einen vertrauenswürdigen Langzeitspeicher, ein korrespondierendes Format für ein selbsttragendes Archivinformationspaket (AIP) als Container für Meta-, Inhalts- und Beweisdaten (XAIP auf Basis von [XFDU,ISO13527] und [VERS]) sowie Anforderungen an die Funktionen und Prozesse der einzelnen Module innerhalb der Referenzarchitektur. Hinsichtlich der Signaturformate lässt die [TR03125] alle Signaturformate nach ETSI zu. Durch die Möglichkeit zur Zertifizierung von Marktlösungen gegen die [TR03125] in mehreren Konformitätsstufen wird zudem eine Überprüfbarkeit und Vergleichbarkeit entsprechender Produkte und damit Sicherheit für die anwendenden Unternehmen wie Behörden geschaffen.

2.4 Fazit – Beweiswerterhaltung

Wie die Ausführungen in den Abschnitten 2.2 und 2.3 gezeigt haben, unterscheiden sich die Mechanismen zur Beweiswerterhaltung seitens der ETSI- und IETF-Standards erheblich voneinander.

[8] Es handelt sich dabei um einen gem. [RFC3161] ausgestellten Zeitstempel, der den Wurzelhashwert in „message imprint“ trägt.

Während die ETSI-Standards sich stets weitgehend an den Spezifika des jeweiligen Signaturformats orientieren und somit auch die Menge der einzusetzenden Zeitstempel direkt proportional zu der Anzahl der abzusichernden Signaturen ansteigen lässt, abstrahiert das durch [RFC4998] bzw. [RFC6283] definierte Verfahren grundsätzlich vollständig von der Art der abzusichernden elektronischen Dokumente und ermöglicht damit eine Absicherung einer beliebigen Menge an Daten und Signaturen mit einem einzelnen Zeitstempel. Weiterhin gilt es auch, dass in der ETSI-Welt nur signierte Dokumente geschützt werden können, wogegen gem. [RFC4998] bzw. [RFC6283] eine Signatur dafür nicht zwingend notwendig ist, was die Praxistauglichkeit des Standards mit Blick auf aktuelle Anwendungsfälle (z.B. IT-Dienste zur Langzeitspeicherung) spürbar erhöht.

Darüber hinaus erzeugen die Verfahren nach ETSI durch ihren Fokus auf das jeweilige Signaturformat sowie die einzelne Signatur eine erhebliche Komplexität, um selbsttragende AIPs zu erzeugen und damit die Basis für eine langfristige Erhaltung der digitalen Daten unter Wahrung von deren Authentizität, Integrität, Verkehrsfähigkeit und Verfügbarkeit zu schaffen. Dies gilt umso mehr, sofern die Daten im Entstehungszusammenhang aufzubewahren sind, wie dies z.B. für behördliche Akten, wissenschaftliche Studien oder Konstruktionsunterlagen in Forschung und Unternehmen der Fall ist.

Die Verwendung eines gem. [TR03125] aufgebauten Systems führt die Vorteile des [RFC4998] bzw. [RFC6283] basierten Ansatzes, mit den Maßgaben zur Informationserhaltung gem. [ISO14721, ISO16363] und [DIN31647] etc. durch wohldefinierte Mechanismen wie den o.g. selbstragenden Archivcontainer sowie definierte Prozesse für Ablage, Abruf und Löschung logisch zusammen und ermöglicht so den Aufbau eines ganzheitlichen, vertrauenswürdigen dLZA zur Informations- und Beweiswerterhaltung.

Im Kontext der neuen eIDAS-Verordnung galt es, für das betroffene europäische Unternehmen jedoch eine konzernweit einheitliche Lösung zu finden, die zum einen die Vorgaben der eIDAS und den hieraus basierenden ETSI-Normen berücksichtigt als auch eine wirtschaftliche wie OAIS-konforme beweissichere Aufbewahrung ermöglicht. Dazu war es demgemäß notwendig, die Ansätze von ETSI und IETF im Kontext von [eIDAS] zu einer Lösung zu kombinieren. Weiterhin mussten vice-versa Migrationspfade definiert werden, da ja künftig nur noch ein Weg zur Beweiswerterhaltung (ETSI oder [RFC4998]) konzernweit Anwendung finden sollte.

Zwar definiert eIDAS gegenwärtig keine konkreten Ansätze für die Umsetzung von LZSP, stellt aber die Notwendigkeit einer Implementierung von beweiskrafterhaltenden Mechanismen für die kryptographisch geschützter Dokumente fest (vgl. Art. 34 eIDAS). Im Rahmen des Projekts galt es, einen adäquaten Mechanismus für die Beweiswerterhaltung zu finden, der in keinerlei Widerspruch zu eIDAS-Bestimmung gegenwärtig steht und der eine zukunftsträchtige Alternative darstellt.

3 Kombination/Migration ETSI und RFC4998/6283

3.1 Grundsatz

Wie in Abschnitt 2 beschrieben, unterscheiden sich die Verfahren zur Beweiswerterhaltung von ETSI und IETF durch ihre verschiedenen Betrachtungsgegenstände (vgl. Abbildung 5):

- ETSI: Fokus auf die zu erhaltende Signatur, nicht die Daten
- IETF: Fokus auf die zu erhaltenden Datenobjekte – unabhängig davon, ob es sich um Nutzdaten, Signaturen, Zertifikate o.ä. handelt.

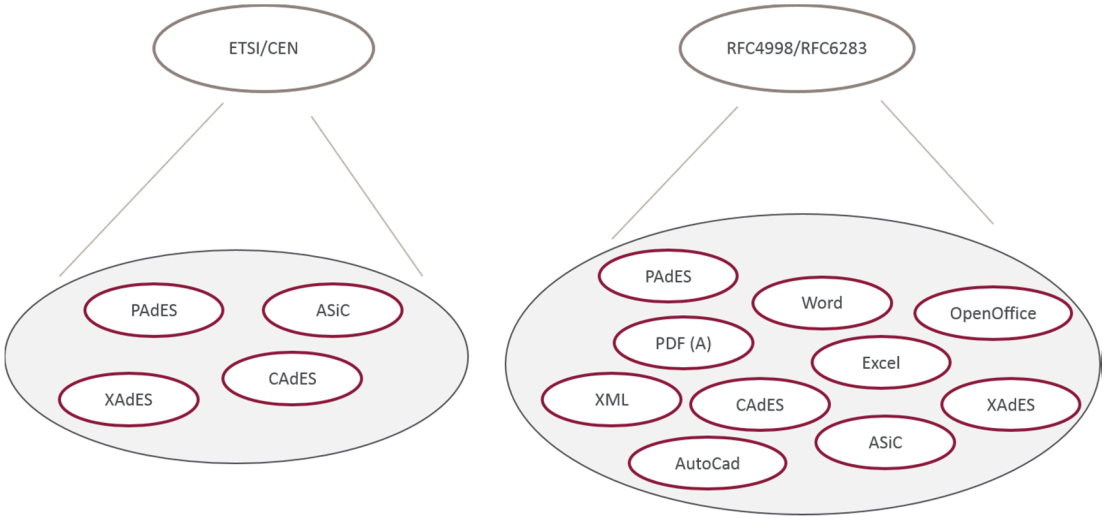

Abb. 5: Betrachtungsgegenstand ETSI vs. RFC 4998/6283

Einzig durch die Spezifikation der Möglichkeit zur Ablage von Evidence Records in ASiC-E nimmt ETSI aktuell eine Durchbrechung des o.g. Prinzips vor (vgl. Absatz 2.2.3). Die nachfolgend vorgestellten Lösungswege zur Kombination und Interoperabilität beziehen sich ausschließlich auf die RFC4998- und CAdES-basierten Anwendungsfälle. Das hier vorgestellte Procedere kann auf die übrigen ETSI-Signaturformate entsprechend übertragen werden. Die Lösung ist im Rahmen der durchgeführten Case Study entstanden und zeigt die Vor- sowie Nachteile der einzelnen Ansätze.

3.2 Migration zwischen RFC4998- und ETSI-Systemen

3.2.1 Ansatz für die Migration

Der Ausgangspunkt stellt ein durch einen Archivzeitstempel nach [RFC3161] abgesicherter Merkle-Hashbaum dar (vgl. Absatz 2.3.2), der durch Einbringen eines ATSv3 an die Signatur des Zeitstempels in die CAdES-Welt übertragen wurde (vgl. *ATSv3_1* in Abbildung 6).

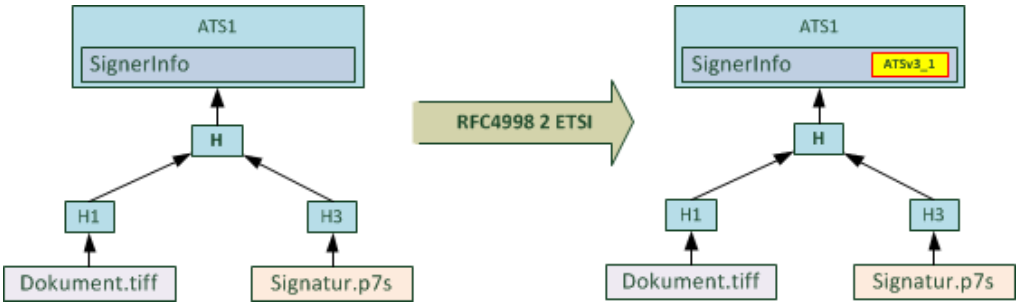

Abb. 6: Migration eines RFC4998-Hashbaums in ein ETSI-System

3.2.2 Signaturerneuerung

Im Falle der Signaturerneuerung wird der dafür vorgesehene CAdES-Mechanismus angewandt (vgl. Absatz 2.1 und 2.2.1) und ein neuer ATSv3 für die Signatur des Archivzeitstempels eingeholt wird (vgl. ATSv3_2 in Abbildung 7).

Es ist nur ein ATSv3 notwendig um den ganzen Hashbaum erneut abzusichern, was dem puren [RFC4998]-Vorgehen vom Aufwand her genau entspricht.

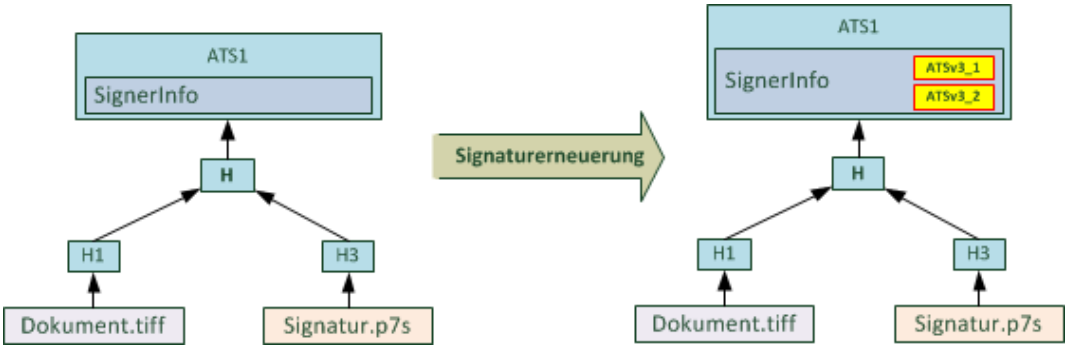

Abb. 7: Signaturerneuerung eines RFC4998-Hashbaums in einem ETSI-System

3.2.3 Hashwerterneuerung

Die anstehende Hashwerterneuerung kann grundsätzlich nicht mit alleinigen CAdES-Beweiskrafterhaltungsmitteln durchgeführt werden. Eine gem. CAdES vorgesehene Signaturerneuerung würde die Signatur des Archivzeitstempels aber nicht die Hashwerte des Hashbaums schützen. Da der Algorithmus schwach ist, können somit u. U. Kollisionen erstellt werden und manipulierte Dokumente in den Blättern des Hashbaums abgelegt werden, ohne dass die Integrität des Hashbaums verletzt wird. Eine Alternative besteht darin, den Hashbaum gem. [RFC4998] mit Hilfe eines neuen geeigneten Hashalgorithmus aufzubauen, mit einem neuen Archivzeitstempel (vgl. *ATS2* in Abbildung 8) zu versiegeln und die Signatur des Archivzeitstempels mit Hilfe eines ATSv3 abzusichern (vgl. *ATSv3_2* in Abbildung 8).

Es ist zu bedenken, dass die neuberechnete Hashwerte gem. [RFC4998] auch die vorherigen ATS-Instanzen mit einbeziehen müssen. Somit ergibt sich z.B. *H1'=Ha(Ha(Dokument.tiff)+Ha(atsc1))*, wobei *Ha* der neu gewählte sichere Hashalgorithmus ist und *atsc1* eine Konkatenation der für betrachteten Dokument relevanten vorherigen Archivzeitstempel in chronologischer Reihenfolge darstellt (vgl. [RFC4998], Abschnitt 5.2). Es ist notwendig die Hashwerterneuerung mit Hilfe des ursprünglichen RFC4998-basierten Systems durchzuführen. Eine o.g. abwechselnde Verwendung von Archivzeitstempel gem. [RFC4998] und ATSv3 gem. [EN319122] hat zur Folge, dass solcher Konstrukt gegenwärtig durch keine Prüfkomponente on-the-fly geprüft werden könnte.

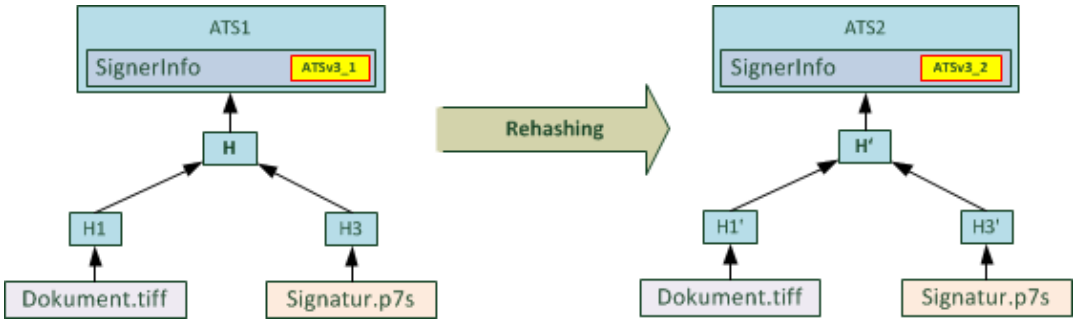

Abb. 8: Hasherneuerung eines RFC4998-Hashbaums in einem ETSI-System

3.3 Migration aus CAdES- zu RFC4998-basierten System

3.3.1 Ansatz für die Migration

Die Migration aus einem CAdES-konformen System in ein RFC4998-konformes System gestaltet sich wesentlich unkomplizierter. Die involvierte CAdES-Signatur wurde bereits mit

CAdES-Mechanismen versiegelt (vgl. Absatz 2.2.1 und *ATSv3_{1-3}* in Abbildung 9) und wird gem. Beweiskrafterhaltungsregeln aus [RFC4998] in ein Merkle-Hashbaum überführt sowie anschließend mit einem Archivzeitstempel entsprechend abgesichert (vgl. Absatz 2.3.2 und *ATS1* in Abbildung 9). Selbstverständlich können auch weitere beliebige Dokumente beim Hashbaumaufbau mitberücksichtigt werden und somit unabhängig von der betrachtenden CAdES-Signatur mitabgesichert werden.

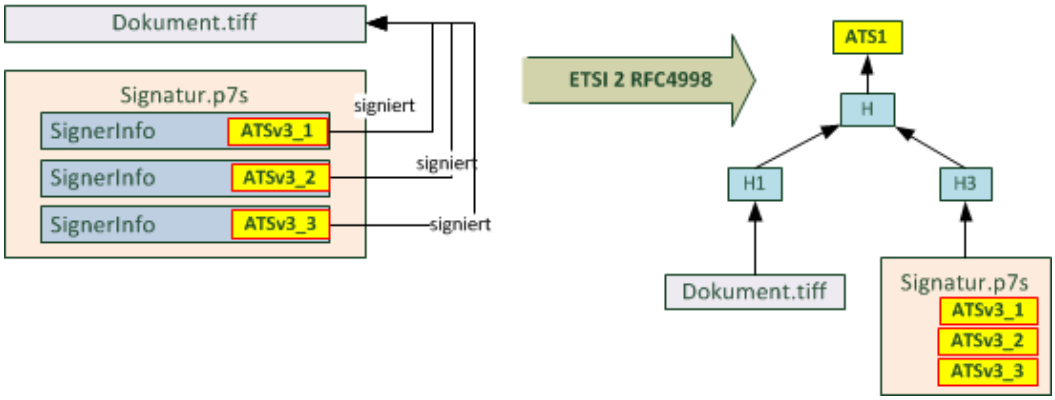

Abb. 9: Migration von CAdES-A-Signaturen in ein RFC4998-System

3.3.2 Signaturerneuerung

Die Signaturerneuerung bezogen auf die Signatur des bestehenden Zeitstempels, dessen Sicherheitseignung abzulaufen droht, wird gem. [RFC4998] durch das Einbringen von neuen Archivzeitstempel vollbracht (vgl. Absatz 2.3.2 und *ATS2* in Abbildung 10).

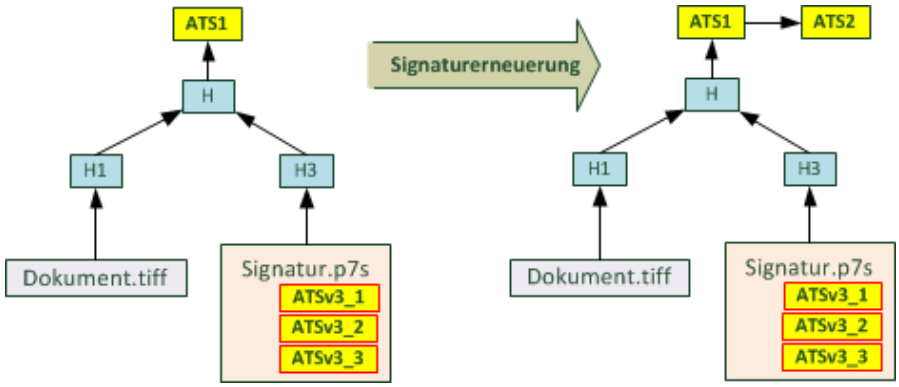

Abb. 10: Signaturerneuerung von in einem RFC4998-System migrierten CAdES-A-Signaturen

Mit Hilfe von einem einzigen Archivzeitstempel werden alle zu schützenden Daten, unabhängig vor deren Art, gleichzeitigt versiegelt.

3.3.3 Hashwerterneuerung

Analog, im Falle der dem aufgebauten Hashbaum zugrunde liegenden Hashwerteerneuerung, müssen die durch [RFC4998] festgelegten Mechanismen verwendet werden (vgl. hierzu Absatz 2.3.3 und Abbildung 11).

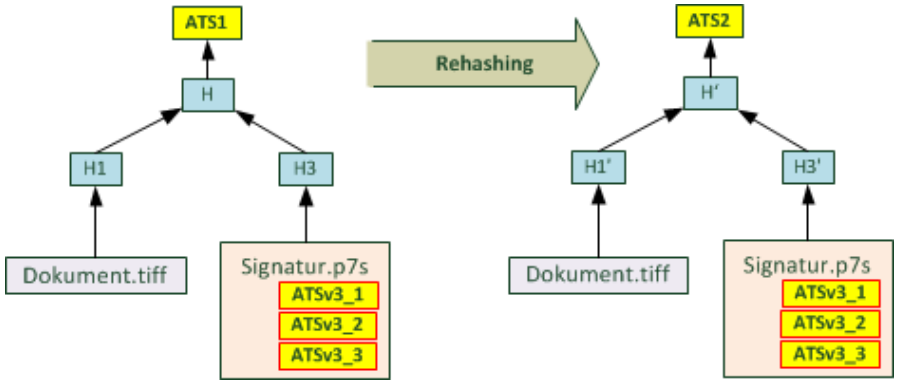

Abb. 11: Hashbaumerneuerung bei in einem RFC4998-System migrierten CAdES-A-Signaturen[9]

Es erfolgt keine Vermischung der Ansätze (ETSI/RFC4998), die Umsetzung basiert vollumfänglich auf den Mechanismen definiert durch [RFC4998].

3.4 Fazit – Kombination und Migration

Wie in den Abschnitten 3.3 und 3.4 gezeigt wurde, ist die Kombination, Interoperabilität und somit die grundsätzliche Migration von Dokumenten, die beweiswerthaltenden Maßnahmen nach ETSI oder RFC 4998/6283 unterzogen wurden, von ETSI nach RFC 4998/6283 und umgekehrt technisch möglich. Damit war für das betrachtete europäische Unternehmen ein standardkonformer Migrationspfad für die technischen Beweisdaten geschaffen, unabhängig davon, für welches Verfahren zur Beweiswerterhaltung – einzelsignaturbezogen oder hashbaumbaumbasiert – sich der Konzern entscheiden würde. Der Weg der Migration aus einem ETSI-basierten in ein RFC4998-basiertes System stellt dabei eine weniger aufwändige und sinnvollere Alternative dar.

4 Zusammenfassung

Mit der eIDAS-Verordnung wurde eine einheitliche wie verbindliche Rechtsgrundlage für vertrauenswürdige und nachvollziehbare elektronische Geschäftsprozesse in Europa geschaffen. Angesichts der hierauf basierenden, verbindlichen ETSI-Normen und den hierin definierten Verfahren zur Beweiswerterhaltung elektronischer, insbesondere kryptographisch signierter Unterlagen, die scheinbar konträr zu etablierten Mechanismen nach IETF [RFC4998] bzw. [RFC6283] standen, ergab sich für das im konkreten Projekt betroffene europäische Unternehmen die Notwendigkeit zur Konsolidierung der unterschiedlichen Verfahren, um rechtliche wie technische Risiken zu vermeiden.

Ziel des Projekts war es, eine standardisierte, eIDAS-konforme Lösung auf Basis der aktuell zur Verfügung stehenden ETSI-Signatur-Standards zu finden, die konzernweit verwendet wird und parallele Verfahren ablöst. Aufgrund der teilweise jahrzehntelangen Aufbewahrungsfristen galt es zudem die, Beweiswert- und Informationserhaltung für die geschäftsrelevanten Unterlagen des Unternehmens auf Basis geltender Standard (vgl. Absatz 1.1) zu gewährleisten. Ähnliche Herausforderungen stellen sich für alle Behörden und Unternehmen, die bislang die Beweiswerterhaltung ihrer elektronischen Unterlagen auf Basis von Merkle-Hashbäumen durchführen.

[9] Entsprechend gilt z.B. für H1‘=Ha(Ha(Dokument.tiff)+Ha(atsv1)), wobei Ha der neu gewählte sichere Hashalgorithmus ist und atsc1 gem. RFC4998, Abschnitt 5.2 entsprechend erstellt wurde.

Einen kritischen Vergleich der ETSI- bzw. RFC 4998/6283 basierten Verfahren Ansätze bezogen auf wesentliche Aspekte einer langfristigen wie wirtschaftlichen Aufbewahrung zeigt, dass insbesondere in folgenden Bereichen die Hashbaumbasierte Lösung auf Basis von RFC 4998/6283 im Vorteil liegt:

- Homogenität – vollständig vom Dokumententyp unabhängig
- Komplexität – ein Ansatz für alle Dokumente und Signaturarten
- Abwärtskompatibilität – vollumfänglich gewehrleistet
- Verbreitung – beachtliche Verbreitung wegen [TR03125]
- Standardisierungsgrad – gleichwertiger Grad der beiden Ansätze
- Kostenfaktor – rein mathematisch, aufgrund des niedrigeren Verbrauch von Zeitstempel, deutlich günstiger

Eine solche Konsolidierung der Beweiswerterhaltung ist aktuell nur dann möglich, wenn zwecks Migration der Daten entsprechende Mechanismen für die Interoperabilität der einzelnen Technologien untereinander entwickelt werden. Im Rahmen des Projekts wurde gezeigt, dass die gem. ETSI und gem. RFC4998/RFC6283 sowie im Besonderen gem. CAdES etc. und gem. [RFC4998] aufgesetzten Systeme für die Beweiswerterhaltung zueinander interoperabel sind, sofern bestimmte Anforderungen beachtet werden (vgl. Absatz 3). Die Verwendung von den RFC4998- und insbesondere TR-03125-basierten System ermöglicht jedoch, eine Reduktion der Komplexität sowie der damit verbundenen Kosten zur beweissicheren Aufbewahrung, da die Beweiswert- und Informationserhaltung aller elektronischen Unterlagen unabhängig vom Signaturformat, ob signiert oder unsigniert in selbsttragenden AIP gewährleistet wird.

Die geplanten ETSI-Spezifikationen für die dLZA sind derzeit in der Vorbereitung. Zur Reduktion der aktuell erforderlichen, in Absatz 3 beschriebenen Migrationsaufwände wird seitens ETSI derzeit eine Integration des Evidence Record gemäß RFC4998/6283 in {C/X}AdES erarbeitet. Die Erstellung eines ETSI-Standards für Bewahrungsdienste ist noch in der Planung.

Literatur

[BGB] Bürgerliches Gesetzbuch, Ausfertigungsdatum: 18.08.1896, zuletzt geändert durch Art. 1 G v. 22.7.2014 I 1218.

[DIN31644] DIN 31644:2012 Information und Dokumentation – Kriterien für vertrauenswürdige digitale Langzeitarchive, 2012.

[DIN31645] DIN 31645:2011 Information und Dokumentation – Leitfaden zur Informationsübernahme in digitale Langzeitarchive, 2011.

[DIN31646] DIN 31646:2013 Information und Dokumentation – Anforderungen an die langfristige Handhabung persistenter Identifikatoren (Persistent Identifier), 2013.

[DIN31647] DIN 31647:2015 Information und Dokumentation – Beweiswerterhaltung kryptographisch signierter Dokumente, 2015.

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

[eIDAS] 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.

[EN319122] ETSI EN 319 122 – {1,2}, Electronic Signatures and Infrastructers (ESI); CAdES digital signatures, ETSI Draft, V1.1.0 (2016-02)

[EN319132] ETSI EN 319 132 – {1,2}, Electronic Signatures and Infrastructures (ESI); XAdES digital signatures, ETSI Draft, V1.1.0 (2016-02)

[EN319142] ETSI EN 319 142 – {1,2}, Electronic Signatures and Infrastructeres (ESI); PAdES digital Signatures, ETSI Draft, V1.1.0 (2016-02)

[EN319162] ETSI EN 319 162 – {1,2}, Electronic Signatures and Infrastrucutres (ESI); Associated Signature Containers (ASiC), ETSI Draft, V1.1.0 (2016-02)

[EU-DLR] RICHTLINIE 2006/123/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über Dienstleistungen im Binnenmarkt“ vom 12.12.2006.

[EuroSOX] RICHTLINIE 2006/43/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates und zur Aufhebung der Richtlinie 84/253/EWG des Rates.

[ISO13527] ISO 13527:2010, Space data and information transfer systems – XML formatted data unit (XFDU) structure and construction rules, 2010.

[ISO14533] ISO 14533: Processes, data elements and documents in commerce, industry and administration – Long term signature profiles. 2014

[ISO14721] ISO 14721:2012, Space data and information transfer systems – Open archival information system (OAIS) -- Reference model, 2012

[ISO15489] ISO/FDIS 15489-1 "Information and documentation – Records management – Part 1: Concepts and principles". 08.12.2015

[ISO16363] ISO 16363:2012. Space data and information transfer systems – Audit and certification of trustworthy digital repositories. 2012

[ISO18829] ISO/DIS 18829. Document management – Assessing ECM/EDRM Implementation - Trustworthiness. 22.10.2015

[ISO30301] ISO 30301:2011, Information and documentation – Management systems for records - Requirements. 2011

[RFC4998] T. Gondrom, R. Brandner, U. Pordesch: Evidence Record Syntax, IETF (2007)

[RFC6283] A. J. Blazic, S. Saljic, T. Gondrom: Extensible Markup Language Evidence Record Syntax (XMLERS), IETF (2011)

[TR03125] BSI TR-03125: Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR), BSI (2014)

[XFDU] S. Nikhinson, L. Reich: XML formatted Data Unit (XFDU), Structure and construction rules, CCSDS 661.0-R-1, 2007, http://sindbad.gsfc.nasa.gov/xfdu

[VERS] Victorian Electronic Records Strategy, http://prov.vic.gov.au/government/vers