Informations- und Beweiswerterhaltung in a Nutshell – Übersicht über Lösungsoptionen für Archivinformations-pakete.

- Tomasz Kusber, Fraunhofer FOKUS [tomasz.kusber@fokus.fraunhofer.de]
- Dr. Ulrike Korte, Bundesamt für Sicherheit in der Informationstechnik [ulrike.korte@bsi.bund.de]
- Steffen Schwalm, Fraunhofer FOKUS [steffen.schwalm@fokus.fraunhofer.de]

Beitragsvorschlag

Im Zuge der Implementierung der [eIDAS-VO] werden mit Hilfe der korrespondierenden Durchführungsrechtsakten (vgl. z.B. 2015/1506/EU) bestimmte technische Standards und Normen (z.B. für die vollständige und durchgehende Abwicklung der elektronischen Prozesse/Transaktionen) festgelegt. Die Verbreitung dieser Spezifikationen findet auch außerhalb der EU[1] und EFTA[2] ihre Geltung. Die elektronischen Dokumente, sowohl in Behörden als auch in Unternehmen, unterliegen dabei den gleichen regulatorischen Vorgaben, wie in der papierbasierten Form, so dass stets die Nachvollziehbarkeit und Prüfbarkeit der zugrundeliegenden elektronischen Geschäftsprozesse gegenüber Dritten (z.B. Gerichten oder Prüfbehörden) lückenlos und über nicht selten sehr lange Periode der Zeit (bis 100 Jahren und mehr) nachgewiesen werden müssen. Die Integrität, Authentizität, Verfügbarkeit sowie Verkehrsfähigkeit der Unterlagen ist dementsprechend über die gesamthafte Aufbewahrungszeit zu gewährleisten. Neben den Nachweispflichten (insbes. Beweiswerterhaltung) müssen die aufbewahrten Unterlagen verfügbar und lesbar sein – als die Informationserhaltung gewährleistet werden. Insbesondere die Visualisierung und Nutzung von lange aufbewahrten Unterlagen stellt eine weitere Herausforderung der Langzeitspeicherung dar, für die tragfähige Lösungen bereitzustellen sind. Gem. dem Stand der Technik werden die Authentizität und Integrität der Daten mit Hilfe kryptographischer Signaturtechniken, z.B. mittels elektronischer Signaturen bzw. Siegel, Zeitstempel, Evidence Records (vgl. ISO14533, EN319{122,132,142,162}, RFC4998, RFC6283) sowie zugehörigen beweiswerterhaltenden Maßnahmen (vgl. TR03125, DIN31647, , SR019510 etc.) ausreichend umgesetzt. Die Informationserhaltung dagegen wird primär durch die Verwendung geeigneter Dateiformate für die aufzubewahrenden Primärdaten die kontinuierliche Umsetzung definierten Erhaltungsmaßnahmen, wie z.B. wohldefinierte und dokumentierte Transformation von alten „aussterbenden“ in die neuen zukunftsträchtigen Formate realisiert (vgl. ISO14721). Hinzu kommen die notwendigen fachlichen wie technischen Metadaten. Die beiden genannten Stränge, Beweiswerterhaltung und Informationserhaltung, sind dabei komplementär und Inhaltsdaten incl. der zugehörigen Metadaten, beweisrelevanten Daten und technischen Beweisdaten müssen in einem untrennbaren Zusammenhang als selbsttragende Archivinformationspakete aufzubewahren (vgl.

[1] Europäische Union
[2] Europäische Freihandelsassoziation

ISO14721, DIN 31647, TR03125). Die wesentlichen Anforderungen an AIP zur Informations- und Beweiswerterhaltung ergeben umfassen dabei: z.B.:

- Aufnahme von beliebigen elektronischen Daten (Formatneutralität),
- Unterstützung von verschiedenen kryptographischen Sicherungstechniken (elektronische Signatur bzw. Siegel, Zeitstempel, Evidence Records etc.),
- Nachträgliche Anpassungen der Inhalts-, Meta- und Beweisdaten und sowie der damit verbundenen Versionierung der aufbewahrten Daten,
- Definition der Verknüpfungen zwischen den einzelnen Teilen der aufbewahrten Daten,
- Vorgabe der geschützten und nicht geschützten Teile im Paket,
- Unterstützung für Umgang mit sehr großen Datenmengen (Inhaltsdaten von mehrehren Gigabytes Dateigröße),
- Selbstragende Form – Beinhaltung aller notwendigen Daten,
- Basierend auf offenen und anerkannten Standards so insbesondere ISO-14721, DIN 31644, DIN 31647, BSI TR-ESOR

Gegenwärtig definiert die TR03125 ein XML-basiertes Informationspaket (vgl. TR03125-F), das auf XFDU[3] (vgl. ISO13527) aufsetzt, die o.g. Anforderungen erfüllt und mit Hilfe von XBARCH, XDOMEA und PREMIS einen Mechanismus für die Ablage der zugehörigen fachlichen und technischen Metadaten anbietet – das XAIP[4]-Paket. Langzeitspeicher gem. BSI TR-ESOR werden branchenübergreifend als verfahrensübergreifende IT-Dienste im Sinne digitaler Langzeitarchive gem. OAIS, DIN 31644, DIN 31647 eingesetzt (u.a. digitales Zwischenarchiv, Airbus, Generali, Mecklenburg-Vorpommern, Bayern). Die Praxis hatte u.a. gezeigt, dass der Umgang mit sehr großen Datenmengen mit Hilfe dieses XML-basierten Pakets zum einen aufgrund der XML-immanenten Base64-Codierung zum anderen der WebService-Schnittstellen, der Module zur Beweiswerterhaltung gem. TR-03125 nicht genügend performant umgesetzt werden konnte, was die Suche nach geeigneten Alternativen initiiert hat. In einem engen Auswahl der Betrachtung sind folgenden Ansätze gerückt:

- Logisches XAIP – eine Möglichkeit der Aufbewahrung der Inhaltsdaten außerhalb des Pakets mit entsprechend eindeutigen Referenzierungen und einer Möglichkeit, bei Bedarf die Daten in das Paket einbetten zu können (somit keine Verletzung der selbstragenden Form),
- Profilierung des ASiC[5] – Containers (vgl. EN319162), wobei die Verwendung von Komprimierungsalgorithmus inbegriffen ist, da ASiC auf ZIP aufbaut (vgl. ISO21320),
- Verwendung eines PDF/A-3 Containers (vgl. ISO19005-3), der bereits als ISO-Standard weltweite Anerkennung genießt.

Wir würden gerne im Rahmen des Papiers eine Diskussion der kurz dargestellten Ideen als Lösungsoptionen für ein selbstragendes Archivinformationspaket, geeignet für die beweiswerterhaltende Langzeitspeicherung der elektronischen Unterlagen, darlegen, die identifizierten Vor- und Nachteile der einzelnen Ansätze vorstellen, sowie kurz die Ideen für die geplante Umsetzung in der kommenden Version der TR03125 skizzieren. Ergänzt werden die Darstellungen durch konkrete Praxisbeispiele aus Behörden sowie der Privatwirtschaft.

[3] XML Formatted Data Unit Standard
[4] XML formatted Archival Information Package
[5] Associated Signature Container

Referenzen

[2015/1506/EU] DURCHFÜHRUNGSBESCHLUSS (EU) 2015/1506 DER KOMMISSION 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, 8. September 2015

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

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

[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

[EN319122] ETSI EN 319 122 – {1,2,3}, Electronic Signatures and Infrastructers (ESI); CAdES digital signatures, ETSI V1.1.1, (2016-04)

[EN319132] ETSI EN 319 132 – {1,2}, Electronic Signatures and Infrastructures (ESI); XAdES digital signatures, ETSI V1.1.1, (2016-04)

[EN319142] ETSI EN 319 142 – {1,2}, Electronic Signatures and Infrastructeres (ESI); PAdES digital Signatures, ETSI V1.1.1 (2016-04)

[EN319162] ETSI EN 319 162 – {1,2}, Electronic Signatures and Infrastrucutres (ESI); Associated Signature Containers (ASiC), ETSI V1.1.1 (2016-04)

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

[ISO14533] ISO 14533 – {1,2,3}, Processes, data elements and documents in commerce, industry and administration – Long term signature profiles

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

[Ko13] U. Korte, S. Schwalm, D. Hühnlein: Vertrauenswürdige und beweiswerterhal-tende Langzeitspeicherung auf Basis von DIN 31647 und BSI TR-03125, In-formatik 2013, GI-LNI, P220, ISBN 978-3-88579-614-5, S. 550-566, 2013

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

[PREMIS] http://www.loc.gov/standards/premis/. Library of Congress: Preservation Metadata Maintenance Activity, Version 2.3

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

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

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

[TR03125] BSI TR 03125, Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR), https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html, 2014

[TR03125-F] BSI TR 03125, Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage TR-ESOR-F: Formate, Version 1.2, 2015

[XBARCH] https://www.bundesarchiv.de/fachinformationen/00895/index.html.de, Version 1.4.3

[XDOMEA] https://www.xrepository.de/Inhalt/urn:uuid:0e13664e -6df5-4d1f-8397-elee-d87a0d4a.xhtml, Version 2.2.0