Klaus Stranacher, Bernd Zwattendorfer - "Ein interoperabler Container für elektronische Dokumente" - D-A-CH Security 2012, pp. 421-431

Ein interoperabler Container für elektronische Dokumente

Klaus Stranacher[1], Bernd Zwattendorfer[2]

[1]Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie, Technische Universität Graz, Österreich
klaus.stranacher@iaik.tugraz.at

[1]Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie, Technische Universität Graz, Österreich
bernd.zwattendorfer@iaik.tugraz.at

Zusammenfassung

Die EU Dienstleistungsrichtlinie musste bis Ende 2009 von allen EU Mitgliedsstaaten umgesetzt werden. Ziel dieser Richtlinie ist es, Vereinfachungen im Handel mit Dienstleistungen zu erreichen. So soll es beispielsweise möglich sein, mittels elektronischer Verfahren eine Dienstleistung im Ausland anzubieten oder ein Geschäft zu eröffnen. Ein zentrales Element dieses Rahmenwerks sind elektronische Dokumente, die zwischen den betroffenen Parteien ausgetauscht werden. Dabei steigt der Bedarf an Interoperabilität zwischen den Mitgliedsstaaten vor allem im Bereich der elektronischen Dokumente und digitalen Signaturen. Der vorliegende Beitrag präsentiert ein mehrschichtiges Interoperabilitätskonzept für den grenzüberschreitenden Austausch von elektronischen Dokumenten entsprechend der Dienstleistungsrichtlinie. Der so genannte „Omnifarious Container for eDocuments“ (OCD) wurde im Zuge des EU Pilotprojekt SPOCS entwickelt und erfolgreich in den teilnehmenden Mitgliedsstaaten eingesetzt.

1 Einleitung

Am 28.Dezember 2009 ist die EU Dienstleistungsrichtlinie [EURO06] in Kraft getreten. Hauptziel der Richtlinie ist, *„die rechtlichen und administrativen Hindernisse für den Handel im Dienstleistungssektor zu beseitigen, damit das ungenutzte Wachstumspotenzial der Dienstleistungsmärkte in Europa freigesetzt wird“* [EURO12]. Speziell Artikel 8 der Direktive, der sich mit der elektronischen Verfahrensabwicklung befasst, ist ein essentieller Bestandteil um dieses Ziel zu erreichen. Artikel 8 und die damit verbundenen Artikel 5, 6, 7 und 21 sind dabei auf folgende Themen fokussiert:

- Identifikation und Authentifikation von Dienstleistungserbringern in einem grenzüberschreitenden Umfeld
- Gegenseitige Anerkennung von Dokumenten
- Sicherheit des Datenaustausches zwischen EU Mitgliedsstaaten
- Prüfung und Validierung von Dokumente

Dabei spielt der Austausch von elektronischen Dokumenten eine zentrale Rolle. Das führt unmittelbar zur Frage der Interoperabilität im Bereich der elektronischen Dokumente und der digitalen Signaturen. Des Weiteren wurde im E-Government Aktionsplan der Europäischen Union [EURO10a] ein starker Fokus auf eine Erhöhung der Interoperabilität zwischen den Mitgliedsstaaten gelegt. Aus diesem Grund präsentieren wir in diesem Beitrag ein mehrschichtiges Interoperabilitätskonzept für den grenzüberschreitenden Austausch von elektronischen Dokumenten, wie es von der EU Dienstleistungsrichtlinie gefordert ist. Das Ergebnis dieses Konzept ist der so genannte „Omnifarious Container for eDocuments“ (OCD), der im Zuge des EU Erprobungsprojekts SPOCS[1] entwickelt wurde.

Der Rest dieses Beitrags ist wie folgt strukturiert: Abschnitt 2 behandelt grundlegende Hintergrundinformationen zu elektronischen Dokumenten sowie dem EU Rahmenwerk. Der darauf folgende Abschnitt 3 gibt einen kurzen Überblick über das EU Pilotprojekt SPOCS. In Abschnitt 4 stellen wir den interoperablen OCD Container vor. Abschnitt 5 erläutert die entwickelten Open Source Software Module, die derzeit in den teilnehmenden Mitgliedsstaaten eingesetzt werden. Abschließend geben wir einen Ausblick auf die Evaluierung der Software Module und die weitere Arbeit.

2 Hintergrundinformationen

Dieser Abschnitt liefert entsprechende Hintergrundinformationen zum besseren Verständnis des weiteren Beitrags. Im Speziellen werden elektronische Dokumente und das Europäische Rahmenwerk wie das Europäische Interoperabilitäts-Rahmenwerk und die EU Dienstleistungsrichtlinie behandelt.

2.1 Elektronische Dokumente

Im Allgemeinen stellen elektronische Dokumente das digitale Pendant zu Papier-Dokumenten dar. Dabei kann dieselbe Information wie bei Papier-Dokumenten ausgetauscht werden, nur können diese einfacher digital verarbeitet und problemloser und rascher übertragen werden.

Prinzipiell können elektronische Dokumente in folgende drei Kategorien eingeteilt werden:

- Strukturierte Formate
- Unstrukturierte Formate
- Container Formate

Strukturierte Dokumente bzw. deren Formate sind Dokumente, deren Inhalt einem bestimmten Schema entspricht. Aus diesem Grund sind solche Formate üblicherweise maschinenlesbar und damit zur automatischen Weiterverarbeitung geeignet. Der bekannteste Vertreter dieses Formattyps ist wohl XML.

Im Gegensatz zu strukturierten Formaten kann der Inhalt von unstrukturierten Formaten nicht automatisch weiterverarbeitet werden. Solche Formate werden hauptsächlich zur (besseren) visuellen Darstellung genutzt. Das meist verwendete Format dieses Typs ist PDF.

Container Formate beinhalten normalerweise unterschiedliche Arten von Daten (wie Texte, Bilder, etc.). Das Container Format spezifiziert dabei, wie diese Daten im Container gespeichert werden. Im Allgemeinen sind solche Formate in sich abgeschlossen, d.h. sämtliche notwendige Informationen und Daten für die Verarbeitung des Dokuments sind im Container

[1] Simple Procedures Online for Cross- Border Services, http://www.eu-spocs.eu/

enthalten. Beginnend mit MIME, als eines der ersten Container Formate, haben diese Formate in den letzten Jahren immer mehr an Popularität erlangt, wie beispielsweise das Open-Document Format ODF[2] oder Office Open XML OOXML[3].

2.2 EU Rahmenwerk

Im Dezember 2012 wurde von der Europäischen Kommission das Europäische Interoperabilitäts Rahmenwerk (European Interoperability Framework - EIF) in der Version 2 veröffentlicht [EURO10b]. Dieses Rahmenwerk legt Designprinzipen fest und enthält Empfehlungen wie Verwaltungen, Unternehmen und Bürger grenzüberschreitend kommunizieren sollten. Dieses Rahmenwerk war die fundamentale Basis für die Entwicklung des interoperablen Dokumente Containers, welcher in Abschnitt 4 im Detail beschrieben wird.

Die EU Dienstleistungsrichtlinie wurde durch das Europäische Parlament und dem Europäischen Rat am 12. Dezember 2006 verabschiedet und wurde in den nationalen Systemen der Mitgliedsstaaten bis zum 28. Dezember 2009 umgesetzt. Die Richtlinie befasst sich mit Handelsbarrieren und legt allgemeine Bestimmungen zur Ausübung von Dienstleistungen sowie den freien Verkehr von Dienstleistung bei Beibehaltung der hohen Qualität innerhalb der Europäischen Union fest. Das Hauptziel der Dienstleistungsrichtlinie ist daher, die rechtlichen und administrativen Hindernisse im Dienstleistungssektor zu reduzieren. Die Richtlinie sieht auch eine erhöhte Transparenz für KMUs und Verbraucher vor.

Die Einrichtung von sogenannten Einheitlichen Ansprechpartnern (EAP) in den Mitgliedsstaaten ist eine Hauptanforderung der Richtlinie. Durch diese EAPs erhalten Dienstleister sämtliche Informationen von einer Stelle und können auch administrative Formalitäten zentral und elektronisch erledigen, ohne der Notwendigkeit weitere Behörden aufzusuchen.

3 EU Pilotprojekt SPOCS

Der vollständige Beitrag enthält in diesem Kapitel eine Beschreibung des EU Erprobungsprojekts (Large Scale Pilot) SPOCS inkl. Ziele des Projekts, entwickelte Spezifikationen und Software Module zu elektronischen Dokumenten, elektronische Dienste, Content Syndizierung[4], elektronische Zustellung und elektronischer Safe. Zusätzlich wird kurz auf die Pilotierung eingegangen, in dessen Rahmen in den teilnehmenden Mitgliedsstaaten die in SPOCS entwickelte Lösung in den Echtanwendungen der EAPs eingesetzt und evaluiert werden.

Dienstleistungsanbieterinnen und –anbieter sind bei der Aufnahme und Ausübung ihrer Dienste mit vielen bürokratischen Regulierungen konfrontiert. Dies trifft insbesondere dann zu, wenn sie grenzüberschreitend tätig sein wollen. Als Antwort auf diese Hindernisse wurde im Mai 2009 das EU Pilotprojekt SPOCS gestartet. Das Hauptziel des Projekts ist die Entwicklung einer Interoperabilitäts-Schicht zur Förderung des Dienstleistungsangebots, indem die grenzüberschreitende Geschäftseröffnung erleichtert wird. Dabei baut die Interoperabilitäts-Schicht auf den existierenden nationalen Lösungen auf.

Hierzu wurden in SPOCS Spezifikationen und Open Source Software Module entwickelt, die auf öffentlichen Standards basieren. Hierbei wurden sowohl die Spezifikationen als auch die

[2] Spezifiziert im ISO-Standard ISO/IEC 26300

[3] Spezifiziert im ISO-Standard ISO/IEC 29500

[4] Der, in diesem Fall grenzüberschreitende, Austausch von Informationen

Software Module einem öffentlichem Publikum (bestehend aus Vertretern der EU Mitgliedsstaaten und der privaten Wirtschaft) vorgestellt und deren Feedback eingearbeitet. Folgende technischen Lösungen wurden entwickelt:

- Content Syndizierung[5]
- Elektronische Zustellung und elektronische Safes
- Elektronische Dienst
- Elektronische Dokumente

Alle diese Module wurden bzw. werden noch in einer Pilotierungsphase[6] erprobt. Dabei werden diese Module in den Produktivsystemen der EAPs der teilnehmenden Pilotierungsländer eingesetzt und stehen den Dienstleistungsanbieterinnen und –anbietern zur Verfügung. Insgesamt erfolgt der Pilotbetrieb mit acht Mitgliedsstaaten[7], die fünf unterschiedliche Berufe[8] pilotieren.

Die folgenden Abschnitte erläutern Details zur Spezifikation und Implementierung der elektronischen Dokumente.

4 OCD – ein interoperabler Dokumente Container

4.1 Überblick

Mit Blick auf die EU Dienstleistungsrichtlinie und der Anforderung der Verbesserung von grenzüberschreitenden elektronischen Verfahren ist Interoperabilität eines der wichtigsten Themen aktueller E-Government Entwicklungen. Um die Interoperabilität zwischen allen betroffenen Parteien in solchen Verfahren zu steigern, wurde ein Interoperabilitäts-Rahmenwerk für den grenzüberschreitenden elektronischen Austausch von elektronischen Dokumenten spezifiziert (siehe Abschnitt 2.2).

Wenn man die E-Government Landschaft innerhalb Europas betrachtet, so ist ersichtlich, dass elektronische Dokumente in einer Vielzahl von Formaten erzeugt werden. Zusätzlich werden diese Dokumente von einer großen Menge an unterschiedlichen öffentlichen Verwaltungen, privaten Organisationen und Firmen, sowie Bürgern ausgestellt. Des Weiteren existieren verschiedenste Mechanismen, um die Integrität und die Authentizität des Ausstellers zu gewährleisten. Dabei kann zwischen Mechanismen, die eng an das jeweilige Dokumentenformat gebunden sind, wie beispielsweise PDF Signaturen, bzw. Mechanismen, die auf mehrere Dokumentenformate angewendet werden können, wie beispielsweise XML Signaturen unterschieden werden. Basierend auf diesen Fakten haben wir folgende Hauptanforderungen an einen interoperablen Dokument-Container formuliert [SPOC11a]. Das Container Format…

- … soll ein mehrschichtiges interoperables Modell für den grenzüberschreitenden Austausch von elektronischen Dokumenten einführen.
- … soll sich nicht darauf beschränken, nur ausgewählte Formate oder Technologien zu unterstützen.

[5] Der, in diesem Fall grenzüberschreitende, Austausch von Informationen

[6] Gestartet mit 1.Juli 2011, siehe auch: http://www.eu-spocs.eu/pilots/index.php

[7] Deutschland, Griechenland, Italien, Litauen, Österreich, Polen, Portugal und Slowenien

[8] Architekt, Baumeister, Immobilienmakler, Reisekauffrau bzw. Reisekaufmann und Tourist-Animation

- … soll alle elektronischen Dokumente unterstützen, die derzeit in Verwendung sind, und auch offen gegenüber neuen Formaten und Technologien sein.
- … soll semantische Interoperabilität unterstützen.
- … soll eine Integrität und Authentizität unterstützen, zusätzlich zu den Authentifizierungs-Mechanismen der enthaltenen Dokumente.

Also Antwort auf diese Forderungen wurde ein mehrschichtiger, interoperabler Container für elektronische Dokumente, der so genannte „Omnifarious Container for eDocuments“ (kurz: OCD) entwickelt. Der OCD Container ist in [SPOC11b] spezifiziert. Obschon der Container in Bezug auf die Dienstleistungsrichtlinie entwickelt wurde, ist er nicht auf diesen Anwendungsfall limitiert. Aufgrund seines generischen Konzepts kann er in allen Fällen des Informationsaustausches basierend auf elektronischen Dokumenten zum Einsatz gebracht werden.

Für den OCD Container wurde in der Spezifikation eine logische und eine physikalische Struktur definiert. Diese Strukturen definieren Kernelemente des OCDs und Methoden bzw. Prozesse, die auf diese Kernelemente angewendet werden können. In den folgenden Abschnitten werden die Strukturen und Methoden näher beleuchtet.

4.2 Logische Struktur

Die logische Struktur des OCD Containers definiert mehrere Schichten und Kernelemente, die mit den entsprechenden Daten gefüllt sind. Ein OCD Container besteht dabei aus folgenden Schichten (siehe auch Abb. 1)

- Payload Schicht
- Metadaten Schicht
- Authentifizierungs Schicht

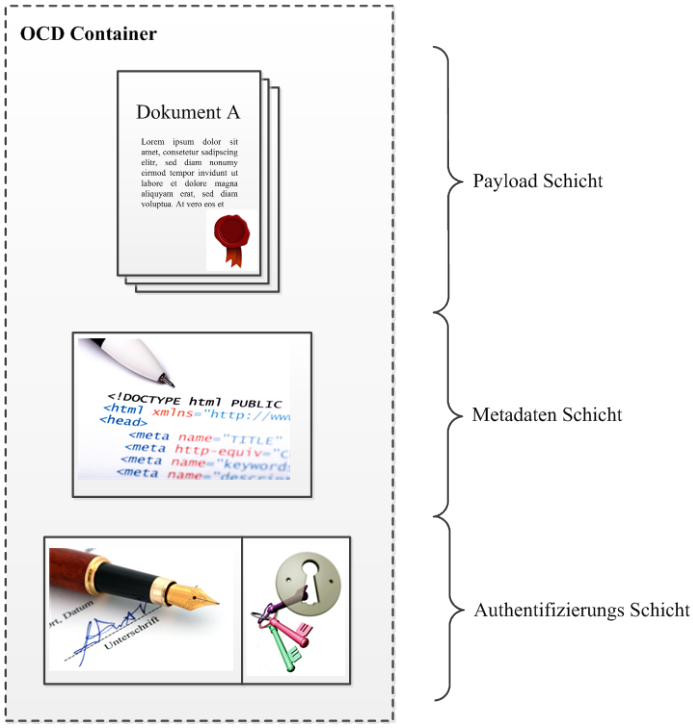


Abb. 1: Die Schichten des OCD Containers.

In der *Payload Schicht* können sämtliche Dokumente, die übertragen werden sollen, dem OCD Container hinzugefügt werden. Hierbei kann diese Schicht alle elektronischen Daten, unabhängig davon ob diese signiert/nicht signiert, verschlüsselt/nicht verschlüsselt, etc. sind, beinhalten. Dies gewährleistet, dass jedes existierende Dokument in einem OCD Container transportiert werden kann.

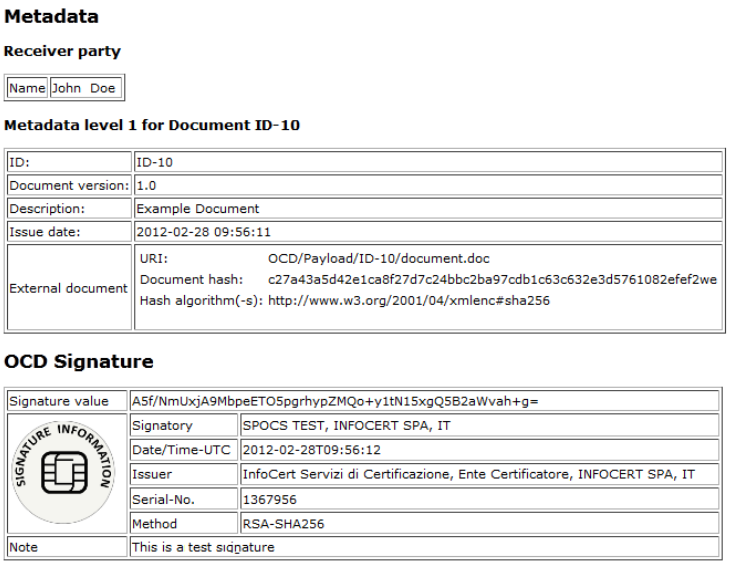
Die *Metadaten Schicht* ermöglicht das automatische Verarbeiten von elektronischen Dokumenten durch das Speichern von Metainformation. Hierbei werden zwei unterschiedliche Metadaten Level unterschieden:

- Metadaten Level 1: Beschreibung der Payload Schicht
- Metadaten Level 2: Beschreibung des Containers

Metadaten Level 2 beinhaltet eine Beschreibung des gesamten OCD Containers, wie beispielsweise den Absender und den Empfänger des Containers. Metadaten Level 1 umfasst hingegen eine einheitliche Beschreibung der Dokumente in der Payload Schicht. Abhängig von der Verfügbarkeit dieser Daten, kann eine Vielzahl von unterschiedlichen Metadaten angegeben werden. Zusätzlich (und im besten Fall) kann auch der extrahierte Inhalt des Dokuments in maschinenlesbarer Form angegeben werden. Beide Metadaten Level sind hierbei in einer XML Datei angegeben, die einen spezifiziertem XML Schema entspricht (siehe [SPOC11b]).

Die optionale *Authentifizierungs Schicht* stellt einen Mechanismus dar, mit dem der Container inklusive aller beinhaltenden Elemente signiert werden kann. Diese Signatur wird jedoch nur zur Integritätsprüfung herangezogen und hat keinerlei rechtliche Gültigkeit. Die rechtliche Gültigkeit wird alleine von den vorhandenen Signaturen der beinhaltenden Dokumente bestimmt.

Des Weiteren wurde eine visuelle Darstellung der Metadaten und Authentifizierungs Schicht spezifiziert. Mittels eines XSL Stylesheet werden Metadaten und Signaturdaten in eine menschenlesbare Darstellung transformiert. Ein Beispiel einer solchen Transformation ist in Abb. 2 gegeben.



Metadata

Receiver party

Name	John Doe

Metadata level 1 for Document ID-10

ID:	ID-10
Document version:	1.0
Description:	Example Document
Issue date:	2012-02-28 09:56:11
External document	URI: OCD/Payload/ID-10/document.doc Document hash: c27a43a5d42e1ca8f27d7c24bbc2ba97cdb1c63c632e3d5761082efef2we Hash algorithm(-s): http://www.w3.org/2001/04/xmlenc#sha256

OCD Signature

Signature value	A5f/NmUxjA9MbpeETO5pgrhypZMQo+y1tN15xgQ5B2aWvah+g=	
SIGNATURE INFORMATION	Signatory	SPOCS TEST, INFOCERT SPA, IT
	Date/Time-UTC	2012-02-28T09:56:12
	Issuer	InfoCert Servizi di Certificazione, Ente Certificatore, INFOCERT SPA, IT
	Serial-No.	1367956
	Method	RSA-SHA256
Note	This is a test signature	

Abb. 2: Visuelle Darstellung der Metadaten und Authentifizierungs Schicht.

4.3 Physikalische Struktur

Die physikalische Struktur definiert die physikalische Implementierung der logischen Struktur des OCD Containers, d.h. welches Datenformat wird für die Speicherung des Containers verwendet. Derzeit sind zwei unterschiedliche Formate definiert:

- ZIP basierter OCD Container
- PDF basierter OCD Container

Die ZIP Variante basiert hauptsächlich auf dem ETSI Standard für Associated Signature Containers (ASiC) [ETSI12a]. ASiC spezifiziert dabei eine Container-Struktur um signierte Daten gemeinsam mit fortgeschrittenen elektronischen Signaturen bzw. Zeitstempeln in einem Container zu speichern. Dabei werden für die Authentifizierungs Schicht XAdES Signaturen, wie sie in [ETSI09] spezifiziert sind, eingesetzt. Die Intention hinter dieser ZIP basierten Variante ist der hauptsächliche Einsatz im BackOffice-Bereich.

Die PDF basierte Variante nutzt den Mechanismus „PDF with attachments“, wie er in [ISO308] definiert ist. Dabei dient die visuelle Darstellung der OCD Metadaten als Hauptdokument. Alle weiteren Objekte, wie die hinzuzufügende Dokumente oder die Metadaten-Datei, werden als Anhang dem Hauptdokument hinzugefügt. Für die Authentifizierungs Schicht werden PAdES Signaturen, wie in [ETSI12b] spezifiziert, eingesetzt. Der Haupteinsatzzweck für PDF basierte OCD Container besteht in allen Fällen, in denen Bürgerinnen und Bürger direkt beteiligt sind.

4.4 Methoden

Dieser Abschnitt beschreibt die Methoden, die auf den OCD Container bzw. dessen Kernelemente angewandt werden können. Diese Methoden werden benötigt, um den OCD Container auch in Real-Life Szenarien einsetzen zu können. Folgende Methoden sind definiert:

- Erzeugung von OCD Containern:

  In einem schrittweisen Prozess wird aus den Eingangsdaten ein OCD Container erzeugt.
- Validierung und Verifikation von OCD Containern:

  Hierbei werden sämtliche Daten im Container einer Validierung bzw. Verifikation unterzogen (Metadaten, Signaturen des Containers und der allenfalls signierten Dokumente in der Payload Schicht, etc.)

Der folgende Abschnitt gibt einen Überblick über die implementieren Software-Module basierend auf den definierten Methoden.

5 Open Source Module

5.1 Überblick

Basierend auf den definierten Methoden wurden entsprechende Open Source Software Module implementiert. Lizensiert sind diese Module unter EUPL[9], um den Einsatz der Module in den EU Mitgliedsstaaten zu vereinfachen. Alle Module stehen dabei als Java API und als SOAP Web-Service zur Verfügung. Folgende Module wurden implementiert:

[9] European Union Public Licence, http://joinup.ec.europa.eu/software/page/eupl

- OCD Erzeugung
- OCD Validierung und Verifikation

Nachfolgend werden diese beiden Module näher erläutert – inklusive einer Architektur- und Schnittstellen-Beschreibung.

5.2 OCD Erzeugung

Das Modul OCD Erzeugung ist verantwortlich für die Erstellung von OCD Container entsprechend der Spezifikation. Nachfolgend werden die Schnittstellen und die Architektur des Moduls beschrieben (siehe auch Abb. 3 bzw. [SPOC12a]).

Schnittstelle. Als Moduleingang dienen die Dokumente, die dem OCD Container hinzugefügt werden sollen, sowie die entsprechenden Metadaten. Zusätzlich, so ein signierte OCD Container erzeugt werden soll, ein bestimmter Signaturschlüssel kann aus einer Menge an vorkonfigurierten Schlüsseln ausgewählt werden[10]. Modulausgang ist der jeweilig erzeugte OCD Container.

Architektur. Abb. 3 bietet einen Überblick über die Architektur des Moduls. Die Erzeugung eines OCD Containers erfolgt hierbei Schritt für Schritt. In der ersten Phase wird die Payload Schicht erstellt. Anschließend wird die Metadaten Schicht erzeugt, basierend auf den Eingangsdaten und den Dokumenten in der Payload Schicht. Im optionalen letzten Schritt wird der OCD Container mittels des selektieren Schlüssels signiert.

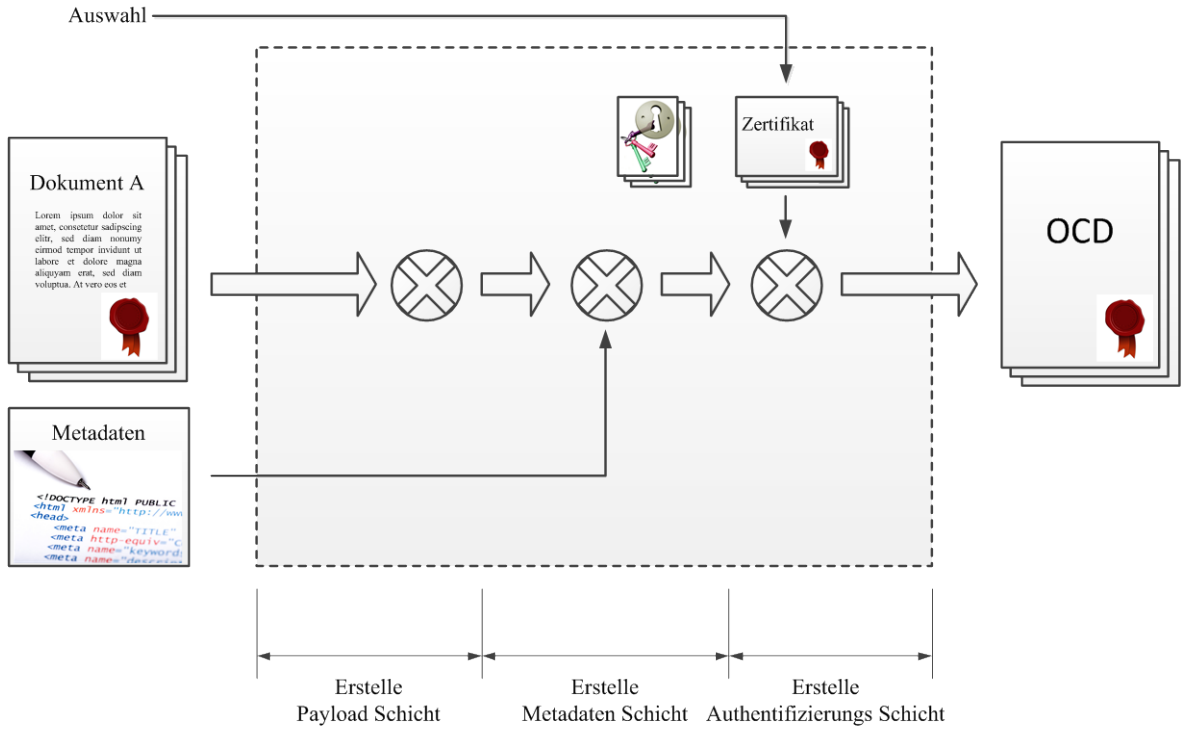


Abb. 3: Modul zu OCD Erzeugung.

[10] Die Modul-Konfiguration bietet die Möglichkeit mehrere unterschiedliche Signaturschlüssel zu konfigurieren.

5.3 OCD Validierung und Verifikation

Dieses Software-Modul ist verantwortlich für die Validierung und Verifikation von OCD Container. Nachfolgend werden die Schnittstellen und die Architektur des Moduls beschrieben (siehe auch Abb. 4 bzw. [SPOC12b]).

Schnittstelle. Der Moduleingang besteht aus einem verpflichtenden OCD Container und einem optionalen Prüfzeitpunkt[11]. Ein XML basierter Validierungs- und Verifikations-Bericht, der sämtliche Resultat der Validierung und Verifikation umfasst, dient als Ausgang.

Architektur. Abb. 4 bietet einen Überblick über die Architektur des Moduls und zeigt die unterschiedlichen Validierungs- und Verifikationsschritte. Zu Beginn wird eine Basis-Validierung durchgeführt. Diese Validierung umfasst verschiedene Überprüfung ob der übermittelte OCD Container der Spezifikation entspricht. Anschließend werden sämtliche Signaturen (Signaturen auf Ebene der Payload-Dokumente und auf Ebene des Containers) verifiziert. Diese Verifikationen umfassen sowohl die kryptographische Signaturüberprüfung als auch die Zertifikats-Validierung. Dabei kann die Signatur-Verifikation auf zwei Arten erfolgen:

1. *Mittels des internen Signatur-Verifikations-Mechanismus*
   Dieser Mechanismus unterstützt alle Signaturformat, wie sie im Beschluss der Europäischen Kommission über „Mindestanforderungen für die grenzüberschreitende Verarbeitung von Dokumenten, die gemäß der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates über Dienstleistungen im Binnenmarkt von zuständigen Behörden elektronisch signiert worden sind“ definiert sind (siehe [EURO11]). Die Zertifikats-Validierung basiert auf Trust-Services-Status Listen (TSL) inklusive der Möglichkeit zusätzliche Vertrauenseinstellungen vorzunehmen.
2. *Mittels externer Verifikationsdienste*
   Das Modul bietet die Möglichkeit sich zu externen Verifikationsdienst zu verbinden, um dort die Signatur-Verifikation vorzunehmen. Diese Möglichkeit ist insbesondere dafür gedacht um die Verifikation von proprietären Dokumentenformaten, die nicht vom internen Verifikationsmechanismus unterstützt werden, zu ermöglichen. Einige EU Mitgliedsstaaten nutzen (auch) solche proprietären Formate, wie beispielsweise Österreich oder Litauen. Üblicherweise betreiben diese Länder Verifikationsdienste, die an das OCD Validierungs und Verifikations Modul angebunden werden können.

In einem vorletzten Schritt findet die (optionale) Verifikation der Metadaten statt. Diese Verifikation bietet Möglichkeit zu überprüfen ob der OCD Container eine bestimmte Menge an Metadaten beinhaltet (z.B. die Überprüfung, ob ein Aussteller und Empfänger des OCD Containers in den Metadaten angegeben ist). Abschließend werden im Bericht-Generator sämtliche Resultate der Validierungs- und Verifikationsprozesse gesammelt und in einem – XML basierten – Validierungs- und Verifikations-Bericht zusammengefasst.

[11] Ist kein expliziter Prüfzeitpunkt angegeben, wird abhängig vom jeweiligen Signaturschema die in der Signatur gegebene Signaturzeit oder die aktuelle Zeit herangezogen.

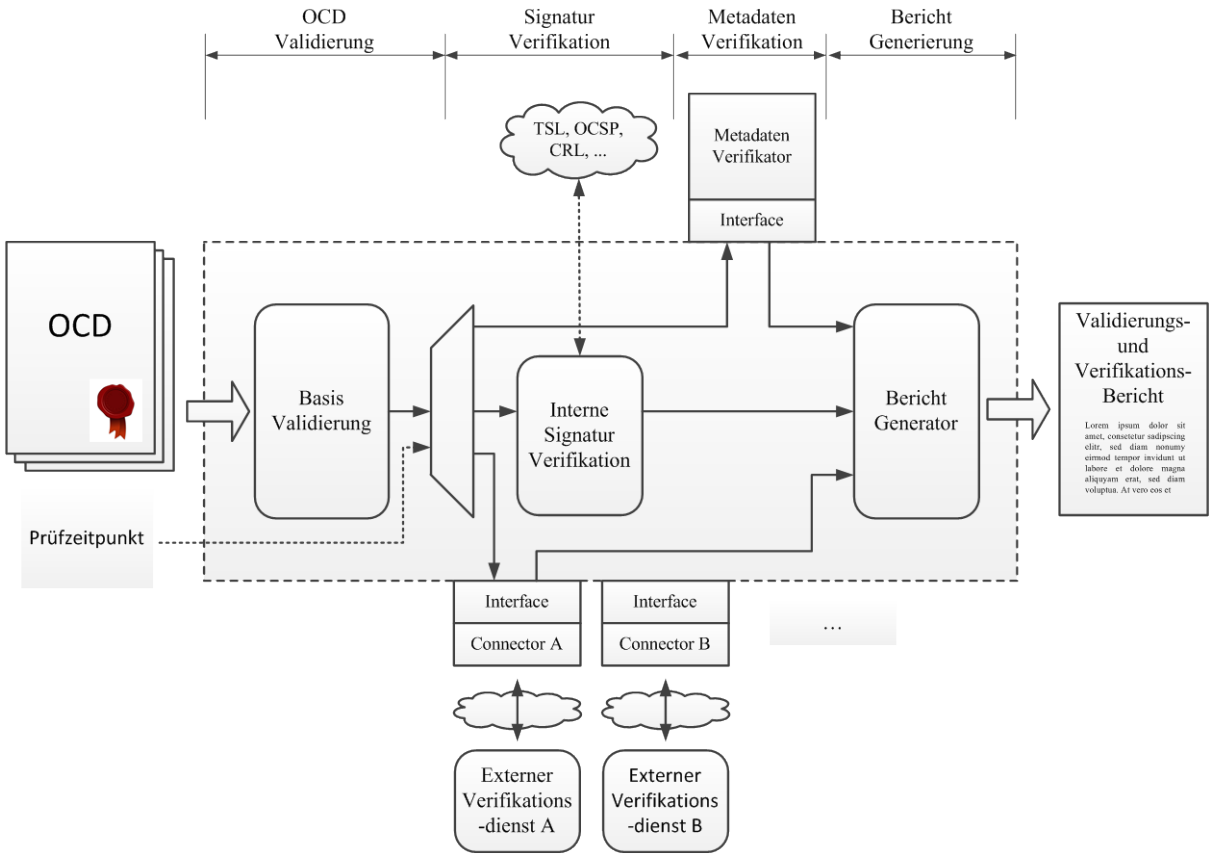


Abb. 4: Modul zu OCD Validierung und Verifikation.

6 Zusammenfassung und Ausblick

Dieser Beitrag präsentierte ein interoperables, mehrschichtiges Rahmenwerk für den grenzüberschreitenden Austausch von elektronischen Dokumenten (Omnifarious Container for e-Documents) in Hinblick auf die Umsetzung der EU Dienstleistungsrichtlinie. Während der Pilotierungsphase[12] im EU Pilotprojekt SPOCS wurden (und werden) die entwickelten Module in den Echtanwendungen der teilnehmenden Mitgliedsstaaten eingesetzt. Dabei werden Szenarien umgesetzt, in denen Immobilienmakler, Architekten, Baumeister oder Reisebüros ein Geschäft in einem anderen Mitgliedsstaat eröffnen können und das mit alleiniger Verwendung elektronischer Mittel. Derzeit befinden sich die OCD Module in der Evaluierung, aktuelle Ergebnisse zeigen aber bereits einen erfolgreichen Einsatz in Echtanwendungen.

Parallel zur Evaluierung werden die OCD Module mit zusätzlichen Funktionen ausgestattet, wie beispielsweise einem Verschlüsselungs-Mechanismus für den gesamten Container oder das automatische Erfassen von Metadaten aus den zu übermittelnden Dokumenten. Zusätzlich wurde eine enge Liaison mit dem Standardisierungsgremium ETSI aufgenommen. Dies hat bereits zu einer Zusammenarbeit im Rahmen der Spezifikation ETSI TS 102 918 (Associated Signature Containers ASiC) geführt.

[12] Die Pilotierungsphase startete am 1.Juli 2011 und endet am 31.Dezember 2012.

Literatur

[ETSI09] ETSI, ETSI TS 101 903, XML Advanced Electronic Signatures (XAdES), Version 1.4.1, June 2009

[ETSI12a] ETSI, ETSI TS 102 918, Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC), Version 1.2.1, February 2012

[ETSI12b] ETSI, ETSI TS 102 778-3, Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles, Version 1.2.1, July 2010

[EURO06] Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt.

[EURO10a] Europäische Kommission, Europäischer eGovernment-Aktionsplan 2011–2015 - Einsatz der IKT zur Förderung intelligent, nachhaltig und innovativ handelnder, COM(2010) 743, 2010

[EURO10b] Europäische Kommission, European Interoperability Framework (EIF) for European public services, COM(2010) 744 final (nur in Englisch verfügbar).

[EURO11] Europäische Kommission, Richtlinie über Dienstleistungen im Binnenmarkt, http://ec.europa.eu/internal_market/services/services-dir/index_de.htm (zuletzt abgerufen am 28.Juni 2012).

[EURO12] Beschluss der Europäischen Kommission, Mindestanforderungen für die grenzüberschreitende Verarbeitung von Dokumenten, die gemäß der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates über Dienstleistungen im Binnenmarkt von zuständigen Behörden elektronisch signiert worden sind, Bekannt gegeben unter Aktenzeichen K(2011) 1081, 2011/130/EU, 25. Februar 2011.

[ISO308] ISO 32000-1, Document management - Portable document format - Part 1: PDF 1.7, First Edition, 1 July 2008.

[SPOC11a] SPOCS, Deliverable D2.1: Inventory of standard documents and relations to open specifications, Version 1.1, 26. Juli 2011 (nur in Englisch verfügbar).

[SPOC11b] SPOCS, Deliverable D2.2: Standard Document and Validation Common Specifications, Version 1.4.0, 9 September 2011 (nur in Englisch verfügbar).

[SPOC12a] SPOCS, Deliverable D2.3: Open Source Standard Document Processing Module, Version 1.2, 24 January 2012 (nur in Englisch verfügbar).

[SPOC12b] SPOCS, Deliverable D2.4: Open Source Authentication Module, Version 1.1, 24 January 2012 (nur in Englisch verfügbar)