Fortgeschrittene PDF Signaturen mit PAdES

Andreas Fitzek I Christian Maierhofer I Arne Tauber I Bernd Zwattendorfer

abstract

Fortgeschrittene PDF Signaturen sind sowohl im behördlichen als auch im privatwirtschaftlichen Bereich essentiell, wenn die Gewährleistung der Authentizität und Unversehrtheit von PDF Dokumenten gefordert ist. Österreich hat bereits 2006 in Eigenentwicklung das Signaturformat PDF-AS (PDF Amtssignatur) für fortgeschrittene PDF Signaturen eingeführt. Das PDF-AS Signaturformat entspricht allerdings keinem internationalen Standard, womit der zunehmenden Notwendigkeit der grenzüberschreitenden Akzeptanz von signierten PDF Dokumenten nicht nachgekommen werden kann. Aus diesem Grund setzt Österreich ab sofort nicht mehr auf PDF-AS, sondern auf den auch von der EU Kommission rechtlich abgesegneten Standard PAdES. Im Rahmen dieses Beitrags wird die aktuelle Open Source Library PDF-AS 4 vorgestellt, die anstatt des Signaturformats PDF-AS nur mehr den Standard PAdES implementiert. Zusätzlich werden konkrete Anwendungen der neuen PDF-AS Bibliothek aufgezeigt.

Einleitung. Digitale Signaturen garantieren Authentizität und Unversehrtheit von elektronischen Dokumenten. Österreich hat in seiner E-Government Voreiterrolle bereits früh mit der Einführung von digitalen Signaturen sowohl im behördlichen als auch im privaten Umfeld begonnen. Um die rechtlichen Anforderungen hinsichtlich Rückführbarkeit von ausgedruckten amtssignierten Dokumenten, speziell jenes des bekanntesten Dokumentenaustauschformats PDF, zu erfüllen, wurde 2006 im österreichischen E-Government das Signaturformat PDF-AS (PDF Amtssignatur) eingeführt. PDF-AS ist eine österreichische Eigenentwicklung, bei der das PDF Dokument mit einer fortgeschrittenen XML Signatur gemäß Signaturgesetz[1] versehen wurde, welche einerseits die Rückführbarkeit von Ausdrucken als auch die einfache visuelle Darstellung eines Signaturblocks ermöglicht. Das PDF-AS Signaturformat entspricht allerdings keinem internationalen Standard. Somit können mittels PDF-AS vom Bürger signierte oder von der Verwaltung amtssignierte Dokumente nur mit spezieller Software oder über spezielle Services geprüft werden, z.B. über das offizielle Signaturprüfservice der RTR[2].

Digital signierte Dokumente sollten aber nicht nur im eigenen Land, sondern möglichst überall und mit jeder Standardsoftware prüfbar sein. Dies ist auch ein großes Anliegen der EU Kommission, die bereits 2011 den rechtlichen Rahmen[3] für die Verarbeitung von Dokumenten mit standardisierten Signaturformaten im Rahmen der EU Dienstleistungsrichtlinie geschaffen hat. Dabei handelt es sich um die fortgeschrittenen Signaturformate XAdES, CAdES und PAdES (XML-, CMS- bzw. PDF-Advanced Electronic Signatures), die von dem European Telecommunications Standard Institute (ETSI) standardisiert wurden und den Anforderungen an fortgeschrittene Signaturen gemäß EU Signaturrichtlinie entsprechen. Mit der kürzlich in Kraft getretenen EU Verordnung über elektronische Identifikation und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS Verordnung)[4] wird der Einsatz dieser Formate aller Voraussicht nach auch über entsprechende delegierte Rechtsakte eine rechtliche Basis für sämtliche Transaktionen mittels elektronischer Signaturen im EU Raum erhalten.

PDF-AS vs. PAdES. PDF-AS basiert auf einer fortgeschrittenen XML-Signatur, wobei nicht die ganze Signatur, sondern nur die essentiellen Informationen der Signatur in ein spezielles PDF-Objekt in Dokument eingebettet werden. Für die Signaturprüfung wird die vollständige XML-Signatur auf Basis von „Templates“ und den im PDF-Objekt enthaltenen Informationen rekonstruiert und anschließend geprüft.[5] PAdES ist ein Profil der in ISO 32000-1 (PDF Standard)[6] spezifizierten PDF-Signatur. PAdES basiert im Gegensatz zu PDF-AS auf einer binären CMS-Signatur (PKCS7). Dabei wird die CMS-Signatur direkt in das PDF-Dokument eingebettet und eine Rekonstruktion ist für eine Signaturprüfung nicht mehr notwendig.[7]

PDF-AS 4. Mit PDF-AS wird jedoch nicht nur das in Österreich spezifizierte Signaturformat bezeichnet, sondern auch eine Open Source Software, die das Anbringen von PDF Signaturen auf Dokumenten erleichtert. Um ein hohes Level an Interoperabilität zu gewährleisten, wird mit der kürzlich erschienenen Version 4 der Open-Source Bibliothek PDF-AS[8] nicht mehr auf das veraltete und proprietäre Signaturformat PDF-AS, sondern auf den europäischen Signaturstandard PAdES im BES (Basic Electronic Signature) Profil gesetzt. Bekannte und positiv aufgenom-

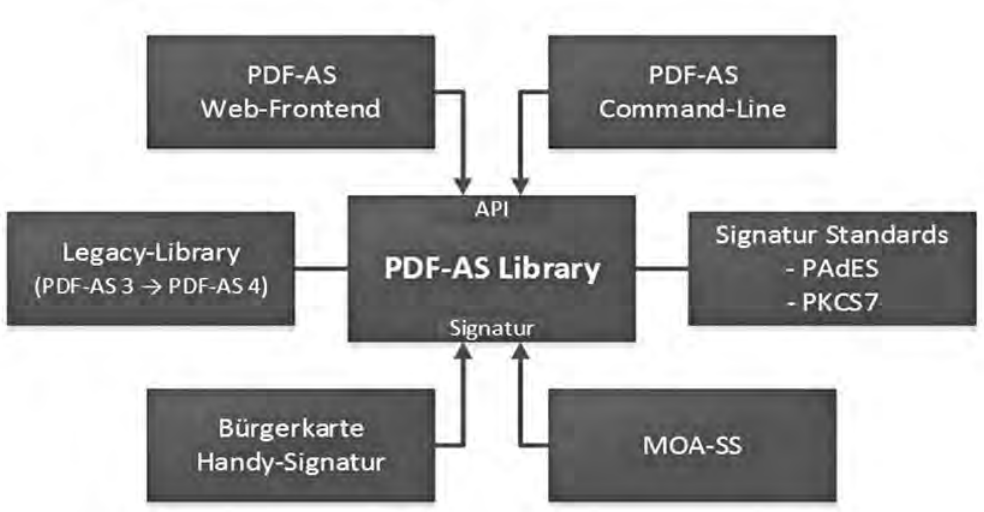

Abb. 1: PDF-AS 4 Architektur

mene Features von PDF-AS, wie z.B. der visuelle Signaturblock, bleiben auch weiterhin erhalten. Die Open-Source Bibliothek PDF-AS wurde dazu von Grund auf neu entwickelt. Es wurde darauf geachtet PDF-AS möglichst modular und erweiterbar zu entwickeln. Abbildung 1 zeigt die Architektur von PDF-AS 4. Durch die starke Modularisierung wird nicht nur die einfache Erweiterbarkeit sichergestellt, sondern auch die Codegröße verkleinert. Dies hat den Vorteil, dass, je nach Anwendungsfall, nicht alle Komponenten eingebunden und somit zur Laufzeit nicht zur Verfügung stehen müssen. Dies reduziert auch die Anzahl der Abhängigkeiten zu externen Software Bibliotheken. Eine kleinere Codebasis bietet neben geringerer Fehleranfälligkeit auch den Vorteil von weniger potenziell angreifbaren Komponenten.

Die Kernfunktionalität wurde in der PDF-AS Library-Komponente zusammengefasst. Die verwendeten Komponenten implementieren fest definierte Schnittstellen, wodurch sich konkrete Implementierungen einfach austauschen lassen. Die Kernfunktionalität gemäß der Signaturstandards PAdES und PKCS7 wird über eine öffentliche API angeboten. Anwendungen sollten ausschließlich diese API verwenden. Mit PDF-AS 4 werden zwei Anwendungen ausgeliefert. Eine kommandozeilenbasierte Anwendung (PDF-AS Command-Line) und eine webbasierte Anwendung (PDF-AS Web-Frontend). Mit beiden Anwendungen können PDF-Dokumente unterschrieben und verifiziert werden. Um den Umstieg auf die neue Version zu erleichtern wurde auch eine Legacy-Library entwickelt, welche die API von PDF-AS 3 auf die API von PDF-AS 4 übersetzt. Da sich die Signaturformate PAdES und PDF-AS allerdings stark voneinander unterscheiden, ist eine vollständige Übersetzung der APIs nicht möglich. Es wird daher empfohlen, dass Anwendungen, die bereits PDF-AS 3 verwenden, auf die API von PDF-AS 4 portiert werden. Die Signaturerstellung via PDF-AS Library kann entweder durch eine Bürgerin bzw. einen Bürger initiiert werden (via Bürgerkarte bzw. Handy-Signatur) oder über eine serverseitige Applikation wie MOA-SS (Modul für Online Applikationen – Server-Signatur)[9].

Anwendungen. Konkrete Anwendung findet die neue PDF-AS Bibliothek sowohl im Rahmen der Amtssignatur in der öffentlichen Verwaltung als auch in Applikationen für BürgerInnen und Unternehmen. Ein Beispiel ist die Java-basierte Anwendung PDF-Over[10]. Bei PDF-Over handelt es sich um eine Java-Applikation zum Signieren von PDF-Dokumenten unter Verwendung der österreichischen Bürgerkarte via Smartcard (z.B. eCard) oder Handy-Signatur. PDF-Over bietet die Möglichkeit, den Signaturblock in einer Voransicht beliebig zu platzieren und anschließend das Dokument zu signieren. Des Weiteren bietet PDF-Over umfangreiche Konfigurationsmöglichkeiten, wie die automatische Signaturblockplatzierung oder eine individuelle Gestaltung des visuellen Signaturblocks. PDF-Over wird vom E-Government Innovationszentrum (EGIZ) entwickelt und ist für die Betriebssysteme Linux, Windows und MacOS verfügbar. Ebenfalls verwendet wird PDF-AS 4 im webbasierten Signaturservice auf Bürgerkarte.at, welches auf der PrimeSign Technologie[11] basiert.

links

(1) https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10003685

(2) https://www.signaturpruefung.gv.at

(3) http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32014D0148

(4) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

(5) http://git.egiz.gv.at/pdf-as-3/plain/dok/Spezifikation/PDF-AS-Spezifikation-2.3.pdf

(6) http://www.adobe.com/devnet/acrobat/pdfs/PDF32000_2008.pdf

(7) http://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf

(8) https://joinup.ec.europa.eu/software/pdf-as/home

(9) https://joinup.ec.europa.eu/software/moa-idspss/home

(10) http://webstart.buergerkarte.at/PDF-Over/index.html

(11) https://www.prime-sign.com/

DI Andreas FITZEK
Wissenschaftlicher Mitarbeiter, E-Government Innovationszentrum (EGIZ); Andreas.Fitzek@egiz.gv.at

DI Christian MAIERHOFER
Wissenschaftlicher Mitarbeiter, E-Government Innovationszentrum (EGIZ); Christian.Maierhofer@egiz.gv.at

Dr. Arne TAUBER
Wissenschaftlicher Leiter, E-Government Innovationszentrum (EGIZ); Arne.Tauber@egiz.gv.at

Dr. Bernd ZWATTENDORFER
Wissenschaftlicher Mitarbeiter, E-Government Innovationszentrum (EGIZ); Bernd.Zwattendorfer@egiz.gv.at