DITEC
Data Information Technology & Expert Consulting

Integračná príručka
D.Signer/XAdES Java - PDF Plugin, v2.0

Copyright

Popisné charakteristiky dokumentu

Projekt	GOV_ZEP		A3019_002
Dokument	Integračná príručka		
Podnázov	D.Signer/XAdES Java - PDF Plugin, v2.0		
Ref. číslo	GOV_ZEP.209	Verzia	5

Vypracoval	Vittek Robert	Podpis	Dátum 12. 11. 2023
Preveril		Podpis	Dátum
Schválil		Podpis	Dátum

Formulár	Dokument		
Ref. číslo	Fo 11	Dátum poslednej aktualizácie	Dátum 14. 10. 2005

Akceptované dňa : <Dátum akceptácie>

Za <Objednávateľa>: Za <Dodávateľa>.:

<Meno zodpovednej osoby> < Meno zodpovednej osoby >

Projekt	GOV_ZEP		A3019_002
Dokument	Integračná príručka		
Referencia	GOV_ZEP.209	Verzia	5

Záznamy o zmenách

Autor	Popis zmien	Dátum	Verzia

Pripomienkovanie a kontrola

Autor	Stanovisko	Dátum	Verzia

Rozdeľovník

	Priezvisko Meno	Firma, Funkcia
Originál		
Kópia		
Kópia		
Kópia		

Obsah

1. Úvod

Tento dokument popisuje funkcionalitu a integračné API komponentu D.Signer/XAdES Java – PDF Plugin[1] a tvorí prílohu Integračnej príručky aplikácie D.Signer/XadES Java.

Aplikácia D.Signer/XAdES Java predstavuje riešenie pre vytváranie zaručeného/kvalifikovaného elektronického podpisu (ZEP/KEP) vo formátoch XAdES_ZEP/XAdES_ZEPbp nad množinou rôznych formátov dokumentov, resp. typov dát (XML dokumenty, PDF dokumenty atď.), prípadne nad ľubovoľnou kombináciou podporovaných formátov dát, ktoré spolu vytvárajú tzv. *multipart* dokument. Funkcionalita SCA je v rámci aplikácie D.Signer/XAdES Java rozdelená do samostatných modulov, ktoré je možné pri nasadení aplikácie kombinovať podľa požiadaviek zákazníka. Aplikáciu D.Signer/XAdES Java tvorí sada knižníc, ktoré poskytujú pre klientské aplikácie nasledujúce integračné rozhrania:

- Java applet API – umožňuje volanie služieb komponentu D.Signer/XAdES Java priamo z prostredia webového prehliadača,
- Java API – umožňuje volanie služieb komponentu D.Signer/XAdES Java z Java aplikácií bežiacich v JRE.

Aby bolo možné postupne budovať podporu pre ďalšie typy dátových objektov, medzi hlavným modulom D.Signer/XAdES Java a pluginmi bolo takisto navrhnuté abstraktné API, ktoré musí každý plugin implementovať. Hlavný modul komunikuje s jednotlivými pluginmi prostredníctvom tohto rozhrania. Architektúra aplikácie D.Signer/XAdES Java je podrobne popísaná v Integračnej príručke D.Signer/XAdES Java.

Každý plugin aplikácie D.Signer/XAdES Java musí pre typ dátového objektu, pre ktorý je určený, definovať triedu, ktorá predstavuje integračné API pluginu. Všeobecné požiadavky na integračné API pluginov, ktoré vyplývajú z architektúry aplikácie D.Signer/XAdES Java, sú definované v Integračnej príručke D.Signer/XAdES Java. Trieda integračného API pluginu môže navyše poskytovať svojmu okoliu ďalšie metódy a atribúty, ktoré sú špecifické pre príslušný typ podporovaného dátového objektu.

[1] PDF technology in D.Signer/XAdES Java - PDF Plugin is powered by PDFNet SDK copyright © PDFTron™ Systems Inc., 2001-2016, and distributed by DITEC a.s. under license. All rights reserved.

2. Zoznam použitých skratiek

DHC – Data Hashing Component

DTBS – Data To Be Signed

DTBSF – Data To Be Signed Formatted, resp. komponent Data To Be Signed Formatter

DTBSR – Data To Be Signed Representation

KEP – kvalifikovaný elektronický podpis

NBÚ – Národný bezpečnostný úrad

PDF – Portable Document Format

QSCD – Qualified Signature Creating Device

SAC – Signer's Authentication Component

SCA – Signature Creation Application

SCDev – Signature Creating Device

SCVA – Signature Creation and Validation Application

SDOC – Signed Data Object Composer

SDP – Signer's Document Presentation

SIC – Signer Interaction Component

SLC – Signature Logging Component

SSA – SCDev/SCA Authenticator

SSC – SCDev/SCA Communicator

SSCD – Secure Signature Creating Device

SVA – Signature Validation Application

XML – eXtended Markup Language

XSD – XML Schema Definition

XSL – eXtensible Stylesheet Language

XSLT – XSL Transformation

XAdES – XML Advanced Electronic Signatures

XAdES_ZEP – profil formátu elektronického podpisu XAdES pre ZEP

XAdES_ZEPbp – profil formátu kvalifikovaného elektronického podpisu na báze XAdES baseline profile

ZEP – Zaručený elektronický podpis

3. Referencie

[1] W3C/IETF Recommendation: "XML-Signature Syntax and Processing" v2002-02-12 (XMLDSIG)

[2] ETSI TS 101 733 – CMS Advanced Electronic Signatures (CAdES) v2.2.1

[3] ETSI TS 101 903 – XML Advanced Electronic Signatures (XAdES) v1.4.2

[4] RFC 3125 – Electronic Signature Policies

[5] RFC 3161 – Internet X.509 Public Key Infrastructure Time-Stamp Protocol

[6] RFC 3279 – Algorithms and Identifiers for the Internet X.509 PKI

[7] RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[8] RFC 3548 – The Base16, Base32, and Base64 Data Encodings

[9] RFC 5652 – Cryptographic Message Syntax (CMS)

[10] RFC 4051 – Additional XML Security Uniform Resource Identifiers

[11] Zákon č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (novelizovaný zákonom č. 275/2006 Z.z.)

[12] Vyhláška NBÚ č. 131/2009 Z.z. o certifikátoch a kvalifikovaných certifikátoch

[13] Vyhláška NBÚ č. 134/2009 Z.z. o produktoch elektronického podpisu

[14] Vyhláška NBÚ č. 135/2009 Z.z. o vyhotovení a overovaní elektronického podpisu a časovej pečiatky

[15] Vyhláška NBÚ č. 136/2009 Z.z. o spôsobe a postupe používania elektronického podpisu v obchodnom styku a administratívnom styku

[16] NBÚ Formáty certifikátov a kvalifikovaných certifikátov, v4.0 (2014-07-10)

[17] NBÚ Formáty zoznamu zrušených kvalifikovaných certifikátov, v3.0 (2010-01-17)

[18] NBÚ Formáty zaručených elektronických podpisov, v3.0 (2009-08-12)

[19] NBÚ Upresnenia obsahu a formálne špecifikácie formátov dokumentov pre ZEP, v1.0 (2007-07-24)

[20] Zákon č. 272/2016 Z.z. o dôveryhodných službách

[21] CWA 14170:2004 E – Security requirements for signature creation applications

[22] CWA 14171:2004 D/E/F – General guidelines for electronic signature verification

[23] XMLENC – XML Encryption Syntax and Processing", J. Reagle, D. Eastlake, December 2002. http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

[24] Koncepcia všeobecného formátu XML podpisu a aplikácie SCVA, DITEC, a.s., 2006

[25] Profil XAdES_ZEP – formát ZEP na báze XAdES, v1.0, DITEC, a.s., 2008

[26] Profil XAdES_ZEP – formát ZEP na báze XAdES, v1.1, DITEC, a.s., 2009

[27] Profil XAdES_ZEP – formát ZEP na báze XAdES, v2.0, DITEC, a.s., 2011

[28] Profil XAdES_ZEPbp – formát ZEP na báze XAdES baseline profile, v1.0, DITEC, a.s., 2016

[29] Formát dátových objektov pre PDF dokument v rámci profilu XAdES_ZEP, v1.0, DITEC, a.s., 2013

[30] Formát dátových objektov pre PDF dokument v rámci profilu XAdES_ZEP, v1.1, DITEC, a.s., 2013

[31] Integračná príručka D.Signer/XAdES Java, v2.0, DITEC, a.s., 2016

[32] PDF Reference, Second Edition, version 1.3, Adobe Incorporated/Addison Wesley, ISBN 0-201-61588-6

[33] PDF Reference, Third edition, version 1.4, Adobe Incorporated/Addison Wesley, ISBN 0-201-75839-3

[34] PDF Reference, Sixth Edition, version 1.7, Adobe Incorporated

[35] Document management – Electronic document file format for long-term preservation – Use of PDF 1.4 (PDF/A-1), ISO 19005-1:2005(E)

[36] Document management – Electronic document file format for long-term preservation – Use of PDF 1.4 (PDF/A-1), TECHNICAL CORRIGENDUM 1, ISO 19005-1:2005/Cor.1:2007(E)

[37] Rozhodnutie komisie 2011/130/EU, ktorým sa ustanovujú minimálne požiadavky na cezhraničné spracovanie dokumentov elektronicky podpísaných príslušnými orgánmi v zmysle smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu

[38] Rozhodnutie komisie 2014/148/EÚ zo 17. marca 2014, ktorým sa mení rozhodnutie 2011/130/EÚ, ktorým sa ustanovujú minimálne požiadavky na cezhraničné spracovanie dokumentov elektronicky podpísaných príslušnými orgánmi v zmysle smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu

[39] Nariadenie Európskeho Parlamentu a Rady EÚ č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES

[40] Rozhodnutie komisie 2015/1506/EU, ktorým sa ustanovujú špecifikácie týkajúce sa formátov zdokonalených elektronických podpisov a zdokonalených elektronických pečatí, ktoré môžu subjekty verejného sektora uznávať

[41] ETSI TS 103 171 – Electronic Signatures and Infrastructures (ESI) XAdES Baseline Profile, v2.1.1

[42] ETSI TS 102 918 – Electronic Signatures and Infrastructures (ESI);. Associated Signature Containers (ASiC), v1.3.1

[43] ETSI TS 103 174 – Electronic Signatures and Infrastructures (ESI);. ASiC Baseline Profile, v2.2.1

[44] Zákon č. 305/2013 o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov

[45] Výnos MF SR č. 55/2014 Z.z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov

4. Formát PDF

Formát PDF bol vytvorený v roku 1993 firmou Adobe Systems pre účely *desktop publishing* a v súčasnosti predstavuje rozšírený a podporovaný štandard pre publikovanie a distribúciu tlačiteľných *device independent* a *display resolution independent* dokumentov. V súčasnosti je aktuálna verzia 1.7 špecifikácie formátu PDF.

Po celom svete používajú firmy, rôzne organizácie, archívy a vládne inštitúcie formát PDF na ukladanie rôznych dôležitých informácií. Množstvo z týchto informácií musí byť archivovaných veľmi dlhý čas (rádovo roky až desiatky rokov, prípadne permanentne) a PDF súbory, v ktorých sú uložené, musia byť použiteľné počas niekoľkých generácií IT technológií. Použiteľnosť týchto súborov v budúcnosti závisí na dlhodobom zabezpečení ich vizualizácie a čitateľnosti (teda reprodukovateľnosti) a uchovaní ich logickej štruktúry ako aj ďalších dôležitých popisných atribútov.

Vzhľadom na bohatosť vlastností a čŕt PDF formátu je dôležité pre zabezpečenie dlhodobej reprodukovateľnosti PDF dokumentov definovať obmedzenia na jednotlivé črty tohto formátu, ktoré je možné použiť v rámci konkrétneho PDF dokumentu. ISO štandard PDF/A-1 (ISO 19005-1:2005 E a ISO 19005-1:2005/Cor.1:2007 E) definuje takéto obmedzenia pre PDF dokumenty verzie 1.4, pričom stanovuje dve úrovne súladu PDF dokumentu so špecifikáciou PDF/A-1:

- Level A Conformance – úplný súlad so špecifikáciou PDF/A-1, teda súlad zabezpečujúci dlhodobú reprodukovateľnosť správnej vizualizácie PDF dokumentu vrátane jeho štrukturálnych a sémantických vlastností,
- Level B Conformance – súlad so špecifikáciou PDF/A-1 zabezpečujúci dlhodobú reprodukovateľnosť správnej vizualizácie daného PDF dokumentu.

Formát PDF má taktiež oporu v legislatíve ako jeden z dátových formátov, nad ktorými je možné vytvárať zaručený/kvalifikovaný elektronický podpis (ZEP/KEP). Vyhláška č. 136/2009 Z.z. NBÚ SR umožňovala používať pre administratívny styk PDF dokumenty, ktoré sú v súlade so špecifikáciami PDF, verzie 1.3 a 1.4, prípadne vo formáte PDF/A-1. Výnos MFSR č. 55/2014 o štandardoch [45] definuje ako jeden zo štandardov pre prijímanie a čítanie podpísaných elektronických dokumentov aj formát PDF/A-1, Level 1A.

4.1. Vizualizácia PDF dokumentov

Dokumenty vo formáte PDF je možné podľa CWA 14170:2004 E (kapitola 8.2) zaradiť do skupiny *Presentation Sensitive SDs*, pretože ich sémantika je závislá na presnosti prezentácie dokumentu podpisovateľovi, resp. overovateľovi. Špecifikácia bezpečnostných požiadaviek na SCA stanovuje ďalšie požiadavky na podpisované dokumenty, ktorých cieľom je zabezpečiť jednoznačnosť interpretácie sémantiky podpisovaných dokumentov.

Naplnenie týchto požiadaviek pre PDF dokumenty realizuje špecifikácia PDF/A-1 (ISO 19005-1:2005 E a ISO 19005-1:2005/Cor.1:2007 E), ktorá poskytuje mechanizmus pre takú reprezentáciu elektronických dokumentov vo formáte PDF, ktorá umožňuje zabezpečenie ich vizualizácie a čitateľnosti (teda reprodukovateľnosti) v rámci dlhého časového obdobia a bez ohľadu na použitú technológiu ich reprodukcie.

Kľúčovým prvkom tejto reprodukovateľnosti PDF/A dokumentov je požiadavka na ich 100% sebestačnosť, teda aby všetky informácie potrebné pre zobrazenie PDF dokumentu vždy rovnakým spôsobom boli zahrnuté v samotnom dokumente.

PDF plugin pre aplikáciu D.Signer/XAdES Java poskytuje pre profily XAdES_ZEP možnosť vizualizácie PDF dokumentov vo formátoch PDF v1.3, v1.4, prípadne vo formáte PDF/A-1 a pre profil XAdES_ZEPbp možnosť vizualizácie PDF dokumentov vo formáte PDF/A-1 prostredníctvom knižnice PDFNet SDK.

Pozor! Pre zabezpečenie jednoznačnosti interpretácie sémantiky podpisovaných PDF dokumentov, a teda ich presnej a výstižnej vizualizácie a čitateľnosti (reprodukovateľnosti) v rámci dlhého časového obdobia odporúčame požadovať úroveň súladu so špecifikáciou PDF/A-1 aspoň na úrovni Level 1B. V opačnom prípade je potrebné zabezpečiť naplnenie uvedenej požiadavky inými prostriedkami v rámci klientskej aplikácie, ktorá využíva služby aplikácie D.Signer/XAdES Java a PDF pluginu.

4.2. Spracovanie PDF dokumentov

Napriek tomu, že požadovanie súladu so špecifikáciou PDF/A-1 umožňuje zabezpečiť dlhodobú reprodukovateľnosť správnej vizualizácie PDF dokumentu, prípadne vrátane jeho štrukturálnych a sémantických vlastností, špecifikácia PDF/A-1 nevyžaduje pri validácii formátu vstupného dokumentu kontrolu prekrývania textu obrázkami alebo inými objektami, ani kontrolu farieb textu a pozadia v rámci dokumentu. Preto je možné vytvoriť PDF súbor, ktorý je v súlade so špecifikáciou PDF/A-1 a pritom text má rovnakú farbu ako pozadie dokumentu (napr. "biely text na bielom pozadí") alebo kde je text prekrytý obrázkom bez predchádzajúceho upozornenia podpisovateľa.

Rovnako PDF plugin pri validácii PDF dokumentu neupozorňuje na vloženie obrázkov, prípadne iných objektov, ktoré môžu prekrývať text, a teda nad takýmto PDF dokumentom je možné vytvoriť platný elektronický podpis. Pri následnom automatickom spracovaní obsahu PDF dokumentu môže takto dôjsť k nežiaducemu automatickému spracovaniu textov, ktoré neboli pri vytváraní ani overovaní elektronického podpisu viditeľné. Z tohto dôvodu nesmie byť dátový obsah takto podpísaného PDF dokumentu na strane overovateľa automaticky spracovávaný.

V prípade potreby vizualizácie podpísaného PDF dokumentu na strane overovateľa odporúčame použiť taký nástroj pre zobrazenie formátu PDF, ktorý dokáže spracovať a vizualizovať PDF dokumenty, ktoré sú v súlade so špecifikáciami PDF Reference 1.3 alebo 1.4, prípadne PDF/A-1.

4.3. Upozornenie ohľadom konverzie PDF dokumentov do formátu PDF/A-1

Cieľom konverzie vstupného PDF dokumentu do formátov definovaných v ISO štandarde PDF/A-1 [35][36] je zabezpečenie dlhodobej reprodukovateľnosti správnej vizualizácie PDF dokumentu, vrátane jeho štrukturálnych a sémantických vlastností.

Konverzia na úroveň PDF/A-1, Level 1B je jednoduchšia, keďže konverzia na túto úroveň zabezpečuje len naplnenie požiadaviek potrebných pre dlhodobú reprodukovateľnosť správnej vizualizácie daného PDF dokumentu (ako napríklad vloženie všetkých požadovaných fontov do výsledného PDF dokumentu).

Konverzia na úroveň PDF/A-1, Level 1A vyžaduje okrem naplnenia všetkých podmienok pre Level 1B aj množstvo sémantických informácií, ktoré nemusia byť vo vstupnom PDF dokumente prítomné. Splnenie požiadaviek štandardu PDF/A-1, Level 1A môže dokonca v niektorých prípadoch vyžadovať manuálne spracovanie vstupného PDF dokumentu. Automatická konverzia vstupného PDF dokumentu do formátu PDF/A-1, Level 1A teda nemusí byť vždy úspešná, keďže vstupný PDF dokument nemusí obsahovať potrebné sémantické informácie, ktoré požiadavky špecifikácie PDF/A-1 pre Level 1A vyžadujú.

Ďalším problémom môže byť použitie rôznych nástrojov pre konverziu a pre validáciu PDF dokumentov v súlade s požiadavkami štandardu PDF/A-1, pretože ich implementácie nemusia byť navzájom kompatibilné. Odporúčame preto využiť pre konverziu do formátu PDF/A-1 funkciu convertToPDFA alebo nastavenie parametra convert na hodnotu True v rámci funkcií createObject, ktoré tvoria API komponentu PDF Plugin pre aplikáciu D.Signer/XAdES Java.

5. Architektúra PDF Pluginu

V rámci tejto kapitoly je popísaná architektúra PDF Pluginu pre aplikáciu D.Signer/XAdES Java, ktorá vychádza z dokumentov:

- Koncepcia všeobecného formátu XML podpisu a aplikácie SCVA [24]
- CWA14170:2004 E – Security requirements for signature creation applications [21].

Pre účely validácie PDF dokumentov voči špecifikácii PDF/A-1 využíva PDF Plugin pre aplikáciu D.Signer/XAdES Java služby knižnice PDFNet.jar od firmy PDFTron.

5.1. Postavenie komponentu v rámci prevádzkového prostredia a aplikácie D.Signer/XAdES Java

PDF Plugin pre aplikáciu D.Signer/XAdES Java je realizovaný ako samostatný komponent, ktorý môže byť nasadený ako súčasť aplikácie D.Signer/XAdES Java v rámci rozsiahlejších systémov, napr. pre elektronickú výmenu dokumentov medzi rôznymi subjektami, v rámci ktorých je potrebné zabezpečiť:

- jednoznačnú identifikáciu pôvodcu dokumentu a neodmietnuteľnosť autorstva,
- integritu (prenášaných) dokumentov.

V rámci aplikácie D.Signer/XAdES Java zabezpečuje PDF Plugin činnosti potrebné pre spracovanie a vizualizáciu dát typu PDF dokument pred spustením procedúry vytvorenia ZEP/KEP a vytvorenie príslušných XML štruktúr pre formát podpisu v súlade s profilmi XAdES_ZEP/XAdES_ZEPbp.

Komponent PDF Plugin poskytuje pre klientské aplikácie nasledujúce integračné rozhrania – API:

- integračné Java API – umožňuje volanie služieb komponentu PDF plugin z Java aplikácií,
- integračné Java applet API – umožňuje volanie služieb komponentu PDF Plugin priamo z prostredia webového prehliadača.

Pre interakciu s podpisovateľom poskytuje komponent PDF Plugin GUI rozhranie, v rámci ktorého je realizované:

- zobrazenie obsahu podpisovaných PDF dokumentov,
- zobrazenie obsahu verifikačných údajov pre podpisované PDF dokumenty (úroveň súladu so špecifikáciou PDF/A-1),
- zobrazenie ostatných relevantných parametrov ZEP/KEP (napr. použité algoritmy pre digitálne odtlačky a ich hodnoty)

pred spustením procedúry vytvorenia ZEP/KEP.

Komponent PDF Plugin zároveň poskytuje implementáciu abstraktného API rozhrania pre integráciu s aplikáciou D.Signer/XAdES Java, ktoré je definované v rámci dokumentu Integračná príručka D.Signer/XAdES Java [31].

Komponent PDF Plugin nevykonáva kryptografické operácie ani nekomunikuje s SSCD zariadením. Pre tento účel volá funkcie rozhrania samostatnej knižnice, ktorá takisto tvorí súčasť aplikácie D.Signer/XAdES Java.

5.2. Funkčná dekompozícia komponentu

Vnútorná architektúra komponentu PDF Plugin pre D.Signer/XAdES Java vychádza a je v súlade s funkčným komponentovým modelom dokumentu CWA14170:2004 E – Security requirements for signature creation applications [21].

Z pohľadu funkčného komponentového modelu SCA sú v rámci komponentu PDF Plugin pre D.Signer/XAdES Java implementované nasledujúce dôveryhodné komponenty:

- SDP – Signer's Document Presentation Component – zabezpečuje zobrazenie podpisovaných PDF dokumentov podpisovateľovi, pre túto funkcionalitu využíva PDF Plugin služby knižnice PDFNet.jar,
- SAV – Signature Attributes Viewer – zabezpečuje zobrazenie príslušných verifikačných údajov pre podpisované PDF dokumenty a ďalších atribútov vytváraného ZEP/KEP podpisovateľovi,
- DTBSF – Data To Be Signed Formatter – zabezpečuje validáciu vstupného PDF dokumentu voči špecifikácii PDF/A-1, sformátovanie a tranformáciu verifikačných údajov vstupného PDF dokumentu do kanonickej formy a vytvorenie štruktúry DTBSF,
- SIC – Signer Interaction Component – GUI rozhranie pre vizualizáciu PDF dokumentov a ďalších atribútov ZEP/KEP a pre interakciu medzi podpisovateľom a aplikáciou D.Signer/XAdES Java, pre túto funkcionalitu využíva PDF Plugin služby knižnice PDFNet.jar.

PDF Plugin pre D.Signer/XAdES Java obsahuje nasledujúce aplikačne závislé komponenty všeobecnej architektúry SCA:

- SDOC – Signed Data Object Composer – modul pre spracovanie a transformáciu PDF dokumentu do base64 a vytvorenie príslušných XML fragmentov výsledného ZEP/KEP vo formáte XAdES_ZEP, resp. XAdES_ZEPbp zo vstupného PDF dokumentu a príslušných verifikačných parametrov.

Obrázok funkčnej dekompozície aplikácie D.Signer/XAdES Java na jednotlivé komponenty SCA ako aj pohľad na jednotlivé vrstvy architektúry sa nachádza v dokumente Integračná príručka D.Signer/XAdES Java, kapitola 6.2 [31].

6. Špecifikácia funkčnosti

6.1. Popis činnosti

Komponent PDF Plugin pre aplikáciu D.Signer/XAdES Java zabezpečuje nasledujúce činnosti:

- vytvorenie dátového objektu typu PDF dokument pre aplikáciu D.Signer/XAdES Java,
- spracovanie vstupných dátových objektov typu PDF dokument, validácia PDF dokumentu voči špecifikácii PDF/A-1, spracovanie verifikačných parametrov a aplikovanie príslušných transformácií pre vytyvorenie DTBSF,
- vizualizácia PDF dokumentu a ďalších atribútov vytváraného ZEP/KEP podpisovateľovi,
- spracovanie a transformácia PDF dokumentu do base64 a vytvorenie príslušných fragmentov výslednej štruktúry ZEP/KEP podľa profilu XAdES_ZEP a prílohy Formát dátových objektov pre PDF dokument, resp. podľa profilu XAdES_ZEPbp a ich poskytnutie aplikácii D.Signer/XAdES Java.

Popis činnosti komponentu v rámci aplikácie D.Signer/XAdES Java je špecifikovaný v rámci dokumentu Integračná príručka D.Signer/XAdES Java, kapitola 7 [31].

7. Špecifikácia API

Komponent PDF Plugin pre D.Signer/XAdES Java tvorí JAR knižnica, ktorá poskytuje pre klientské aplikácie nasledujúce integračné rozhrania:

- Java API – umožňuje volanie služieb komponentu XML plugin z Java aplikácií,
- Java applet API – umožňuje volanie služieb komponentu XML Plugin priamo z prostredia webového prehliadača.

Princípy návrhu integračných rozhraní Java API a Java applet API sú popísané v rámci integračnej príručky SCA aplikácie D.Signer/XAdES Java [31], kapitoly 8.1.1 a 8.1.2.

PDF Plugin definuje v rámci integračného API triedy pre typ dátového objektu PDF dokument, ktoré reprezentujú:

- podpisovaný PDF dokument,
- verifikačné údaje pre daný PDF dokument – požadovaná úroveň súladu so špecifikáciou PDF/A-1.

PDF Plugin pre D.Signer/XAdES Java implementovať abstraktné API IPlugin pre komunikáciu s hlavnou aplikáciou D.Signer/XAdES Java.

V nasledujúcich kapitolách je popísané integračné rozhranie PDF Pluginu.

7.1. Integračné API pluginu

PDF Plugin pre aplikáciu D.Signer/XAdES Java publikuje pre Java aplikácie nasledujúce rozhranie:

Package:
sk.ditec.zep.dsigner.xades.plugins.pdfplugin

Triedu:
PdfPlugin

Metódy a premenné:
```
public DataObject createObject
(     String objectId
,     String objectDescription
,     String sourcePdfBase64
,     String password
,     String objectFormatIdentifier
,     int reqLevel
,     boolean convert
);

public int checkPDFACompliance
(     String sourcePdfBase64
,     String password
,     int reqLevel
);

public int convertToPDFA
(     String sourcePdfBase64
,     String password
,     int reqLevel
);

public static final int CONFORMANCE_LEVEL_1A = 0;
public static final int CONFORMANCE_LEVEL_1B = 1;
public static final int CONFORMANCE_LEVEL_NONE = 2;

public String getErrorMessage();

public String getConvertedPDFA();
```

Package:
sk.ditec.zep.dsigner.xades.bp.plugins.pdfplugin

Triedu:
PdfBpPlugin

Konštanty:
```
public static final int CONFORMANCE_LEVEL_1A = 0;
public static final int CONFORMANCE_LEVEL_1B = 1;
public static final int CONFORMANCE_LEVEL_NONE = 2;
```

Metódy a premenné:

```
public DataBpObject createObject
(     String objectId
,     String objectDescription
,     String sourcePdfBase64
,     String password
,     String objectFormatIdentifier
,     final int reqLevel
,     final boolean convert
)ô
```

```
public int checkPDFACompliance
(     String sourcePdfBase64
,     String password
,     int reqLevel
);
```

```
public int convertToPDFA
(     String sourcePdfBase64
,     String password
,     int reqLevel
);
```

```
public String getErrorMessage();

public String getConvertedPDFA() {
```

Package:

```
sk.ditec.zep.dsigner.xades.plugins.pdfplugin.applet
```

Triedu:

```
PdfPluginApplet
```

Konštanty:

```
public static final int CONFORMANCE_LEVEL_1A = 0;
public static final int CONFORMANCE_LEVEL_1B = 1;
public static final int CONFORMANCE_LEVEL_NONE = 2;
```

Metódy a premenné:

```
public boolean createObject
(     final Object objectId
,     final Object objectDescription
,     final Object sourcePdfBase64
,     final Object password
,     final Object objectFormatIdentifier
,     final int reqLevel
,     final boolean convert
,     final JSObject callback
);
```

```
public boolean checkPDFACompliance
(     final Object sourcePdfBase64
,     final Object password
,     final int reqLevel
,     final JSObject callback
);

public boolean convertToPDFA
(     final Object sourcePdfBase64
,     final Object password
,     final int reqLevel
,     final JSObject callback
);

public boolean getErrorMessage(final JSObject callback);

public boolean getConvertedPDFA(final JSObject callback);
```

Package:

```
sk.ditec.zep.dsigner.xades.bp.plugins.pdfplugin.applet
```

Triedu:

```
PdfBpPluginApplet
```

Konštanty:

```
public static final int CONFORMANCE_LEVEL_1A = 0;
public static final int CONFORMANCE_LEVEL_1B = 1;
public static final int CONFORMANCE_LEVEL_NONE = 2;
```

Metódy a premenné:

```
public boolean createObject
(     final Object objectId
,     final Object objectDescription
,     final Object sourcePdfBase64
,     final Object password
,     final Object objectFormatIdentifier
,     final int reqLevel
,     final boolean convert
,     final JSObject callback
);

public boolean checkPDFACompliance
(     final Object sourcePdfBase64
,     final Object password
,     final int reqLevel
,     final JSObject callback
);
```

```
public boolean convertToPDFA
(     final Object sourcePdfBase64
,     final Object password
,     final int reqLevel
,     final JSObject callback
);

public boolean getErrorMessage(final JSObject callback);

public Object getConvertedPDFA(final JSObject callback);
```

7.1.1. Popis funkcií a premenných API pluginu

7.1.1.1. createObject (trieda PdfPlugin, PdfPluginApplet)

Preťažená metóda. Umožňuje vytvoriť dátový objekt typu PDF dokument v rámci profilu XAdES_ZEP pre aplikáciu D.Signer/XAdES Java.

Parametre:

objectId – XML Id daného objektu v rámci výslednej XML štruktúry podľa XAdES_ZEP, povolené znaky: a..z, A..Z, 0..9, „.“ (bodka), „-“ (pomlčka), „_“ (podčiarkovník); XML Id musí začínať písmenom alebo podčiarkovníkom,

objectDescription – popis obsahu daného PDF dokumentu, napr: "Všeobecné zmluvné podmienky",

sourcePdfBase64 – samotný vstupný PDF dokument, kódovaný v base64,

password – heslo pre prístup k PDF dokumentu, ak je chránený heslom,

objectFormatIdentifier – hodnota elementu ObjectIdentifier, ktorý sa nachádza v elemente xades:DataObjectFormat (pozri dokumenty [29][30]),

reqLevel – požadovaná úroveň súladu so špecifikáciou PDF/A-1:

- CONFORMANCE_LEVEL_1A – požadovaná úroveň súladu Level 1A,
- CONFORMANCE_LEVEL_1B – požadovaná úroveň súladu Level 1B,
- CONFORMANCE_LEVEL_NONE – nie je požadovaná validácia úrovne súladu so špecifikáciou PDF/A-1 (v tomto prípade musia byť bezpečnostné požiadavky definované v dokumente [21], kapitola 8.2 naplnené pomocou iných prostriedkov),

convert – ak je True, vykoná sa pred validáciou voči špecifikácii PDF/A-1 a zobrazením PDF dokumentu podpisovateľovi konverzia dokumentu na PDF dokument, ktorý spĺňa požadovanú úroveň súladu so špecifikáciou PDF/A-1.

callback – viď dokument [31], kapitola 8.1.2.

Všetky podpisované informácie o dátovom objekte budú pred vytvorením podpisu zobrazené používateľovi a pri overení podpisu budú overené voči referenčným údajom evidovaným v rámci IS spracovateľa elektronického podpisu.

7.1.1.2. createObject (triedy PdfBpPlugin, PdfBpPluginApplet)

Umožňuje vytvoriť dátový objekt typu PDF dokument v rámci profilu XAdES_ZEPbp pre aplikáciu D.Signer/XAdES Java.

Parametre:

objectId – názov súboru s dátovým objektom typu PDF dokument (odporúča sa názov vrátane prípony .pdf); zakázané sú znaky < > : " / \ | ? *,

objectDescription – popis obsahu daného PDF dokumentu, napr: "Všeobecné zmluvné podmienky", môže byť null

sourcePdfBase64 – samotný vstupný PDF dokument, kódovaný v base64,

password – heslo pre prístup k PDF dokumentu, ak je chránený heslom,

objectFormatIdentifier – hodnota elementu ObjectIdentifier, ktorý sa nachádza v elemente xades:DataObjectFormat (pozri dokument [28]), môže byť null

reqLevel – požadovaná úroveň súladu so špecifikáciou PDF/A-1:

- 0 – požadovaná úroveň súladu Level 1A,
- 1 – požadovaná úroveň súladu Level 1B,
- 2 – nie je požadovaná validácia úrovne súladu so špecifikáciou PDF/A-1 (v tomto prípade musia byť bezpečnostné požiadavky definované v dokumente [21], kapitola 8.2 naplnené pomocou iných prostriedkov).

convert – ak je True, vykoná sa pred validáciou voči špecifikácii PDF/A-1 a zobrazením PDF dokumentu podpisovateľovi konverzia dokumentu na PDF dokument, ktorý spĺňa požadovanú úroveň súladu so špecifikáciou PDF/A-1,

callback – viď dokument [31], kapitola 8.1.2.

Všetky podpisované informácie o dátovom objekte budú pred vytvorením podpisu zobrazené používateľovi a pri overení podpisu budú overené voči referenčným údajom evidovaným v rámci IS spracovateľa elektronického podpisu.

7.1.1.3. checkPDFACompliance

Preťažená metóda. Umožňuje validáciu dátového objektu typu PDF dokument voči špecifikácii PDF/A-1.

Funkcia vracia:

- 0 – ak validácia vstupného PDF dokumentu voči špecifikácii PDF/A prebehla úspešne,
- inak vráti číslo chyby a príslušnú chybovú správu je možné získať pomocou metódy getErrorMessage.

Parametre:

sourcePdfBase64 – samotný vstupný PDF dokument, kódovaný v base64,

password – heslo pre prístup k PDF dokumentu, ak je chránený heslom,

reqLevel – požadovaná úroveň súladu so špecifikáciou PDF/A-1:

- CONFORMANCE_LEVEL_1A – požadovaná úroveň súladu Level 1A,
- CONFORMANCE_LEVEL_1B – požadovaná úroveň súladu Level 1B,

- CONFORMANCE_LEVEL_NONE – žiadna požadovaná úroveň súladu so špecifikáciou PDF/A-1; v tomto prípade sa skontroluje len verzia vstupného PDF dokumentu na hodnoty v1.3 alebo v1.4 (v súlade s požiadavkami dokumentov [29][30]), resp. hodnotu v1.4 (v súlade s požiadavkami dokumentu [28])
- callback – viď dokument [31], kapitola 8.1.2.

7.1.1.4. convertToPDFA

Umožňuje konverziu dátového objektu typu PDF dokument na PDF dokument, ktorý spĺňa požadovanú úroveň súladu so špecifikáciou PDF/A-1.

Funkcia vracia:

- 0 – ak konverzia prebehla úspešne, výsledný PDF/A dokument v base64 je možné získať pomocou metódy getConvertedPDFA,
- inak vráti číslo chyby a príslušnú chybovú správu je možné získať pomocou metódy getErrorMessage.

Parametre:

sourcePdfBase64 – samotný vstupný PDF dokument, kódovaný v base64,

password – heslo pre prístup k PDF dokumentu, ak je chránený heslom,

reqLevel – požadovaná úroveň súladu so špecifikáciou PDF/A-1:

- CONFORMANCE_LEVEL_1A – požadovaná úroveň súladu Level 1A,
- CONFORMANCE_LEVEL_1B – požadovaná úroveň súladu Level 1B,
- callback – viď dokument [31], kapitola 8.1.2.

7.1.1.5. getErrorMessage

V prípade výskytu chyby v rámci procesu vytvárania dátového objektu typu PDF dokument bude vracať príslušnú chybovú správu uloženú v premennej ErrorMessage.

Parametre:

callback – viď dokument [31], kapitola 8.1.2

7.1.1.6. getConvertedPDFA

V prípade úspešnej konverzie vstupného PDF dokumentu do požadovanej úrovne súladu s PDF/A-1, bude vracať výsledný PDF/A dokument uložený v premennej ConvertedPDFA v base64.

Parametre:

callback – viď dokument [31], kapitola 8.1.2

8. Návratové kódy PDF pluginu

V nasledujúcej tabuľke sú uvedené návratové kódy funkcie checkPDFACompliance (všetky triedy).

Návratový kód	Popis
0	Pdf je validné vzhľadom na požadovanú úroveň.
-1	Odchytená výnimka v aplikácii. Popis chyby je možné získať pomocou funkcie getErrorMessage.

V nasledujúcej tabuľke sú uvedené návratové kódy funkcie convertToPDFA (všetky triedy), pozri tiež kapitolu 4.3.

Návratový kód	Popis
0	Konverzia prebehla úspešne.
-1	Odchytená výnimka v aplikácii. Popis chyby je možné získať pomocou funkcie getErrorMessage.

Ostatné funkcie vrátia v prípade chyby prázdny string, resp. hodnotu Null (v závislosti od typu návratovej hodnoty).

9. Trademarks