DITEC
Data Information Technology & Expert Consulting

Všeobecný popis produktu
D.Signer/XAdES Java, v2.0

Copyright

Popisné charakteristiky dokumentu

Projekt	GOV_ZEP		A3019_002
Dokument	Všeobecný popis produktu		
Podnázov	D.Signer/XAdES Java, v2.0		
Ref. číslo	GOV_ZEP.204	Verzia	9

Vypracoval	Vittek Róbert	Podpis	Dátum 27. 12. 2022
Preveril	Priezvisko Meno Preveril	Podpis	Dátum 31. 12. 2004
Schválil	Priezvisko Meno Schválil	Podpis	Dátum 30. 12. 2004

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	Všeobecný popis produktu		
Referencia	GOV_ZEP.204	Verzia	9

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. Všeobecný popis produktu

Aplikácia D.Signer/XAdES Java predstavuje riešenie pre vytváranie zaručeného/kvalifikovaného elektronického podpisu (ZEP/KEP) 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. Povolené formáty podpisovaných elektronických dokumentov v administratívnom styku špecifikuje Výnos MF SR č. 55/2014 o štandardoch pre IS VS [37]. Požiadavky na formát a obsah podpisovaných dát stanovuje dokument NBÚ SR – Upresnenia obsahu a formálne špecifikácie formátov dokumentov pre ZEP, v1.0.

Zaručený/kvalifikovaný elektronický podpis na druhej strane zabezpečuje integritu podpísaných dát a nepopierateľnosť podpisu. Aplikácia D.Signer/XAdES Java môže byť teda nasadená v rámci akéhokoľvek systému, kde je potrebné zabezpečiť jednak integritu prenášaných a spracovávaných dokumentov, ako aj nepopierateľnosť identity ich podpisovateľa.

Aplikácia D.Signer/XAdES Java pred samotnou procedúrou vytvorenia ZEP/KEP zabezpečí podpisovateľovi zobrazenie všetkých podpisovaných dát a zaručí, že dáta sa pri podpise nezmenia (v zmysle zákona č. 215/2002 Z.z. o elektronickom podpise).

Pre vytvorenie ZEP/KEP musí byť aplikácia použitá len v súlade s platnou podpisovou politikou pre ZEP/KEP, ktorá bola schválená NBÚ SR. Používateľ je pred vytvorením podpisu povinný presvedčiť sa, že podpisová politika, ktorú aplikácia používa, je stále platná a nebola zo strany vydavateľa predčasne zrušená. Výrobca, resp. integrátor aplikácie D.Signer/XAdES Java je povinný zabezpečiť také nastavenie konfigurácie aplikácie a parametrov volania metód rozhrania aplikácie, aby aplikácia vytvárala podpis v súlade so špecifikovanou podpisovou politikou.

Za obsah a sformátovanie vstupných dát (dokumentov), ako aj za dodržanie správneho postupu vytvorenia ZEP/KEP, definovaného v rámci podpisovej politiky, je zodpovedný podpisovateľ. Za správne vyhodnotenie platnosti vytvoreného ZEP/KEP a za špecifikovanie parametrov procesu verifikácie ZEP/KEP v súlade s podpisovou politikou je zodpovedný prijímateľ alebo prevádzkovateľ systému, ktorý tieto dáta spracováva.

Požiadavky NBÚ SR na vytváraný formát ZEP/KEP upravuje dokument – Formáty zaručených elektronických podpisov, v3.0. Minimálne požiadavky EÚ na cezhraničné spracovanie dokumentov elektronicky podpísaných príslušnými orgánmi v zmysle smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu stanovuje rozhodnutie komisie 2014/148/EU, ktoré nahrádza rozhodnutie komisie 2011/130/EU. Špecifikácie týkajúce sa formátov zdokonalených elektronických podpisov a zdokonalených elektronických pečatí, ktoré môžu subjekty verejného sektora uznávať ustanovuje Rozhodnutie komisie 2015/1506/EU.

Aplikácia D.Signer/XAdES Java vytvára ZEP v súlade so schválenými formátmi pre zaručený elektronický podpis XAdES_ZEP, v1.0 (http://www.ditec.sk/ep/signature_formats/xades_zep/v1.0), XAdES_ZEP, v1.1 (http://www.ditec.sk/ep/signature_formats/xades_zep/v1.1), XAdES_ZEP, v2.0 (http://www.ditec.sk/ep/signature_formats/xades_zep/v2.0) a KEP v súlade s profilom pre kvalifikovaný elektronický podpis XAdES_ZEPbp (http://www.ditec.sk/ep/signature_formats/xades_zepbp/v1.0). Aplikácia D.Signer/XAdES Java vytvára typ podpisu XAdES_ZEP-EPES (resp. XAdES_ZEPbp-EPES), teda elektronický podpis rozšírený o:

- informáciu o čase vzniku ZEP/KEP,
- explicitnú podpísanú referenciu podpisovej politiky,
- podpísané informácie o typoch a formátoch podpísaných dátových objektov

a tiež XAdES_ZEP-T, resp. XAdES_ZEPbp-T, teda elektronický podpis rozšírený o časovú pečiatku podpisu. Aplikácia D.Signer/XAdES .NET umožňuje vytvárať aj typ podpisu XAdES_ZEPbp-BES, to znamená typ elektronického podpisu bez explicitne uvedenej referencie podpisovej politiky, v súlade s príslušnými nariadeniami komisie [29][30][32] a príslušným baseline profilom pre XAdES [33].

Aplikácia D.Signer/XAdES Java môže byť použitá taktiež pre vytváranie tzv. obyčajného elektronického podpisu zmysle zákona č. 215/2002 Z.z. o elektronickom podpise.

Na vytvorenie štruktúr zložených elektronických podpisov v súlade s profilmi XAdES_ZEP, resp. XAdES_ZEPbp, prípadne štruktúr elektronických podaní Registration, resp. Message Container môžu byť použité komponenty D.Sig XAdES Extender a ASiC Factory.

V súlade s §4, odsek (5) zákona o e-Gov [36] je aplikácia D.Signer/XAdES Java implementovaná takým spôsobom, aby poskytovala funkcionalitu vytvorenia ZEP/KEP aj pre osoby so zdravotným postihnutím – pre slabozrakých a nevidiacich pomocou technológie NVDA (http://www.nvaccess.org/).

Aplikácia D.Signer/XAdES Java je lokalizovaná v slovenskom a v anglickom jazyku.

1.1. Architektúra aplikácie

Architektúra aplikácie D.Signer/XAdES Java zodpovedá architektúre SCA, popísanej v štandarde CWA 14170:2004 E – Security requirements for signature creation applications, pričom aplikácia zároveň spĺňa všetky jeho relevantné bezpečnostné požiadavky.

Aplikácia D.Signer/XAdES Java bude poskytovať pre klientské aplikácie nasledujúce integračné rozhrania – API:

- 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.

Pre interakciu s podpisovateľom bude aplikácia D.Signer/XAdES Java poskytovať GUI rozhranie, v rámci ktorého je realizované:

- zobrazenie obsahu podpisovaných dokumentov ako aj všetkých relevantných parametrov ZEP/KEP pred spustením procedúry vytvorenia ZEP/KEP,
- výber kvalifikovaného certifikátu pre vytvorenie ZEP/KEP,
- štandardné ovládacie prvky – potvrdenie procedúry vytvorenia ZEP/KEP, zrušenie procedúry vytvárania ZEP/KEP apod.

1.2. Systémové požiadavky

Systémové požiadavky aplikácie D.Signer/XAdES Java sú nasledujúce:

- operačný systém – MS Windows 7 / 8 / 10 / 11, Mac OS X: verzia 10.12 – 10.15, 11, 12, procesor (architektúra CPU): x86_64, arm (M1), prekladač Rosetta 2 – v prípade procesora arm (M1), GNU/Linux: Mint verzia 13, 17.x, 18, 19.x, 20.0, 20.1, 20.2, 20.3; Debian verzia 8, Mint Debian Edition 4, 5; Ubuntu verzia 12.04 LTS, 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS, 21.04, 21.10, 22.04; Fedora: verzia 23, 24, 25, 33, 34, 35, 36; Manjaro 21.0, 21.2.2,
- ak je aplikácia D.Signer/XAdES Java spúšťaná z web portálu pomocou aplikácie D.Launcher v1.x:
  - ⇒ Oracle Java 8 (https://www.java.com/en/download/manual.jsp), pozn. kombinácia OpenJDK a IcedTea nie je podporovaná,
  - ⇒ Java plugin do webového prehliadača, Java Web Start a Java FX verzia 2.1 a vyššia (súčasť inštalácie Oracle Java),
- občiansky preukaz s čipom alebo iné certifikované SSCD/QSCD zariadenie pre generovanie kľúčových párov a vytváranie elektronického podpisu + čítačka a ovládače podľa odporúčaní akreditovanej certifikačnej autority (ACA); prípadne PKCS#12 súbor ako úložisko podpisového certifikátu,
- príslušná CSP implementácia MS CryptoAPI (iba MS Windows) alebo implementácia PKCS #11 rozhrania (32 bit / 64 bit podľa platformy Java); súčasť softvéru dodávaného s SSCD/QSCD zariadením,
- web prehliadač podporujúci spúšťanie Java appletov[1] – MS Internet Explorer v7.0 alebo vyššia (len 32 bit), Mozilla Firefox, v45 – v45 – v51, resp. v59 ESR (len 32 bit, s podporou NP API), Safari 14, 15,
- prístup na internet (prípadne správne nastavenia pre proxy),
- správne nastavený aktuálny systémový dátum a čas.

Ak je aplikácia D.Signer/XAdES Java spúšťaná z web portálu pomocou aplikácie D.Launcher v1.x, tak požiadavky na web prehliadač zahŕňajú aj prehliadače:

[1] Ak je aplikácia D.Signer/XAdES Java spúšťaná ako Java applet.

- MS Internet Explorer verzia 10/11 (aj 64 bit), Mozilla Firefox, v45 a vyššia aj 64-bit, Google Chrome v51 alebo vyššia (prípadne Chromium), Opera v38 alebo vyššia, MS Edge v25 alebo vyššia.

V tomto prípade je Java plugin vyžadovaný pre MS Internet Explorer 7/8/9, voliteľný pre MS Internet Explorer 10/11; môže byť nutné ho v prehliadači MS Internet Explorer povoliť pomocou voľby Tools/Manage add-ons. Systémové požiadavky pre aplikáciu D.Launcher sú špecifikované v rámci používateľskej príručky pre aplikáciu D.Launcher.

Ak je aplikácia D.Signer/XAdES Java spúšťaná z web portálu pomocou aplikácie D.Launcher v2.x a rozšírenia D.Bridge 2:

- webový prehliadač – MS Internet Explorer 11 (len 32bit verzia), Mozilla Firefox 78, 89, 91, 101, Google Chrome 91, 100, 101, Chromium 91, 100, 101, Opera 76, 78, Microsoft Edge 91, 96, 97,
- vo webovom prehliadači nainštalované a povolené rozšírenie D.Bridge 2, pre MS Internet Explorer sa vyžaduje vypnutý chránený režim.

Pri vytváraní zaručeného/kvalifikovaného elektronického podpisu pomocou aplikácie D.Signer/XAdES Java sa predpokladá použitie certifikovaného zariadenia pre generovanie a uloženie privátneho kľúča a pre vytvorenie zaručeného/kvalifikovaného elektronického podpisu (SSCD/QSCD – napr. čipová karta, USB token ap.) a použitie kvalifikovaného certifikátu, vydaného akreditovanou certifikačnou autoritou. Aplikácia D.Signer/XAdES Java pristupuje k danému SSCD/QSCD zariadeniu prostredníctvom príslušného CSP providera (implementácia MS Crypto API pre dané SSCD/QSCD zariadenie) alebo príslušnej implementácie PKCS#11 rozhrania.

Pri vytváraní tzv. obyčajného elektronického podpisu pomocou aplikácie D.Signer/XAdES Java nie je potrebné použiť kvalifikovaný certifikát vydaný akreditovanou certifikačnou autoritou, ani certifikované SSCD/QSCD zariadenie. Použitá podpisová politika by mala jasne deklarovať, o aký elektronický podpis ide.

Podrobný popis prevádzkových požiadaviek aplikácie (teda napr. požiadaviek na SSCD/QSCD zariadenie, požiadaviek na prevádzkové prostredie aplikácie, bezpečnostných požiadaviek ap.), ako aj postup pri vytváraní ZEP/KEP, je špecifikovaný v rámci dokumentácie aplikácie.

2. Podporované normy a štandardy

Pri návrhu a implementácii aplikácie D.Signer/XAdES Java pre vytváranie ZEP/KEP sa autori aplikácie riadili nasledujúcimi dokumentami, normami a odporúčaniami:

[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

[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] 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

[30] 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

[31] 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

[32] 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

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

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

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

[36] 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

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

[38] Extensible Markup Language (XML) 1.0 (Fifth Edition) – http://www.w3.org/TR/2008/REC-xml-20081126/

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

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

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

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

[43] 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)

[44] Information technology -- Computer graphics and image processing -- Portable Network Graphics (PNG): Functional specification, ISO/IEC 15948:2004

3. Podporované kryptografické funkcie

Aplikácia D.Signer/XAdES Java podporuje všetky podpisové schémy profilu XAdES_ZEP [25][26][27] a profilu XAdES_ZEPbp [28]:

Názov	Identifikátor	Poznámka
DSA-SHA1 (DSS)	http://www.w3.org/2000/09/xmldsig#dsa-sha1	povinná v rámci XML Signature [1] povinná v rámci profilu XAdES_ZEP
RSA-SHA1	http://www.w3.org/2000/09/xmldsig#rsa-sha1	odporúčaná v rámci XML Signature [1] odporúčaná v rámci profilu XAdES_ZEP
RSA-SHA256	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256	voliteľná, RFC4051 [10] voliteľná v rámci profilu XAdES_ZEP odporúčaná v rámci profilu XAdES_ZEPbp
RSA-SHA384	http://www.w3.org/2001/04/xmldsig-more#rsa-sha384	voliteľná, RFC4051 [10] voliteľná v rámci profilu XAdES_ZEP voliteľná v rámci profilu XAdES_ZEPbp
RSA-SHA512	http://www.w3.org/2001/04/xmldsig-more#rsa-sha512	voliteľná, RFC4051 [10] voliteľná v rámci profilu XAdES_ZEP voliteľná v rámci profilu XAdES_ZEPbp

Aplikácia D.Signer/XAdES Java podporuje všetky algoritmy pre výpočet digitálneho odtlačku profilu XAdES_ZEP [25][26][27] a profilu XAdES_ZEPbp [28]:

Názov	Identifikátor	Poznámka
SHA-1	http://www.w3.org/2000/09/xmldsig#sha1	povinný v rámci XML Signature [1]

		povinný v rámci profilu XAdES_ZEP
SHA-256	http://www.w3.org/2001/04/xmlenc#sha256	odporúčaný, XMLENC [23] odporúčaný v rámci profilu XAdES_ZEP odporúčaný v rámci profilu XAdES_ZEPbp
SHA-384	http://www.w3.org/2001/04/xmldsig-more#sha384	voliteľný, RFC4051 [10] voliteľný v rámci profilu XAdES_ZEP voliteľný v rámci profilu XAdES_ZEPbp
SHA-512	http://www.w3.org/2001/04/xmlenc#sha512	voliteľný, XMLENC [23] voliteľný v rámci profilu XAdES_ZEP voliteľný v rámci profilu XAdES_ZEPbp

Podpisová schéma a algoritmus pre výpočet digitálneho odtlačku, ktorý bude použitý pri vytváraní ZEP/KEP, závisí od zvoleného podpisového certifikátu používateľa a zvolených parametrov volania funkcie pre vytvorenie ZEP/KEP aplikácie D.Signer/XAdES Java.

Tvorca klientskej aplikácie, v rámci ktorej je D.Signer/XAdES Java integrovaný musí zabezpečiť, že funkcia sign bude volaná s parametrom, ktorý zodpovedá algorimu digitálneho odtlačku, ktorý sa nachádza v rámci ETSI SR 002 176 a je schválený v rámci vyhlášky NBÚ č. 135/2009 Z.z.