

## Používateľská príručka D.Signer/XAdES Java, v2.0

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

### Copyright

Všetky práva vyhradené

Tento dokument je vlastníctvom spoločnosti DITEC, a. s. Žiadna jeho časť sa nesmie akýmkoľvek spôsobom (elektronickým, mechanickým) poskytnúť tretej strane, rozmnožovať, kopírovať, vrátane spätného prevodu do elektronickej podoby, bez písomného povolenia spracovávateľa.

#### Popisné charakteristiky dokumentu

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Podnázov	D.Signer/XAdES Java, v2.0		
Ref. číslo	GOV_ZEP.212	Verzia	6

Vypracoval	Vittek Róbert	Podpis	Dátum 14.2.2020
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	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

#### Záznamy o zmenách

Autor	Popis zmien	Dátum	Verzia

#### Pripomienkovanie a kontrola

Autor	Stanovisko	Dátum	Verzia

#### Rozdeľovník

	Priezvisko Meno	Firma, Funkcia
Originál		
Kópia		
Kópia		
Kópia		

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

### Obsah

1.	Úvod	5
2.	Zoznam použitých skratiek	6
3.	Popis aplikácie	7
4.	Systémové požiadavky	9
5.	Distribúcia a inštalácia	12
6.	Užívateľské nastavenia	15
6.1	Nastavenie jazyka aplikácie	15
6.2	Nastavenie spôsobu prístupu k SSCD a podpisov certifikátom	vým 16
7.	Vytvorenie ZEP používateľom	22
7.1	Načítanie vstupných parametrov	
7.2	Súhlas s licenčnou zmluvou	
7.3	Zobrazenie podpisovaných dát	
7 /	Nastavonio dátumu a času vytvoronia podnisu	25 <b>26</b>
7.5	Podpísanie dokumentu	
7.6	Zobrazenie parametrov podpisu	
8.	Trademarks	35

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

## 1. Úvod

Tento dokument je určený pre používateľov aplikácie D.Signer/XAdES Java, resp. pre používateľov informačných systémov a aplikácií, v rámci ktorých bude aplikácia D.Signer/XAdES pre zaručený elektronický podpis (ZEP) integrovaná.

Jednotlivé časti dokumentácie aplikácie D.Signer/XAdES Java je možné použiť pri tvorbe používateľských príručiek týchto informačných systémov po dohode s vlastníkmi autorských práv aplikácie D.Signer/XAdES Java.

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

## 2. Zoznam použitých skratiek

HTML – HyperText Markup Language; hypertextový značkový jazyk na vytváranie webových stránok

HTTPS – HyperText Transfer Protocol Secure; zabezpečený hypertextový prenosový protokol

NBÚ – Národný bezpečnostný úrad

PDF – formát dokumentov Portable Document Format

PNG – grafický formát Portable Network Graphics

SSCD – Secure Signature Creating Device; bezpečné zariadenie na vytváranie elektronického podpisu

TXT – formát textových súborov

XML – eXtensible Markup Language; rozšíriteľný značkovací jazyk pre štruktúrované dáta

XAdES – XML Advanced Electronic Signatures; formát pokročilého elektronického podpisu na báze XML

XAdES\_ZEP – profil formátu elektronického podpisu XAdES pre ZEP

XAdES\_ZEPbp – profil formátu zaručeného elektronického podpisu na báze XAdES baseline profile

ZEP – Zaručený elektronický podpis

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

### 3. Popis aplikácie

Aplikácia D.Signer/XAdES Java predstavuje riešenie pre vytváranie zaručeného elektronického podpisu (ZEP) 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. Požiadavky na formát a obsah podpisovaných dát stanovuje dokument NBÚ SR – Upresnenia obsahu a formálne špecifikácie formátov dokumentov pre ZEP, v1.0.

Zaručený 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 v zmysle zákona č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov:

- zabezpečí podpisovateľovi zobrazenie všetkých podpisovaných dát jednoznačným a adekvátnym spôsobom,
- zaručí, že dáta sa pri podpise nezmenia.

Pre vytvorenie ZEP musí byť aplikácia použitá len v súlade s platnou podpisovou politikou pre ZEP, 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, definovaného v rámci podpisovej politiky, je zodpovedný podpisovateľ. Za správne vyhodnotenie platnosti vytvoreného ZEP a za špecifikovanie parametrov procesu verifikácie ZEP v súlade s podpisovou politikou je zodpovedný prijímateľ alebo prevádzkovateľ systému, ktorý tieto dáta spracováva.

Požiadavky NBÚ SR na vytváraný formát ZEP 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,

Popis aplikácie

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

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 XAdES ZEPbp, (http://www.ditec.sk/ep/signature formats/xades zepbp/v1.0). 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, o explicitnú podpísanú referenciu podpisovej politiky a 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 2011/130/EU, 2014/148/EU, 2015/1506/EU a príslušným baseline profilom pre XAdES ETSI TS 103 171.

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.

V súlade s §4, odsek (5) zákona č. 305/2013 Z.z. o e-Governmente v znení neskorších predpisov je aplikácia D.Signer/XAdES Java implementovaná takým spôsobom, aby poskytovala funkcionalitu vytvorenia ZEP aj pre osoby so zdravotným postihnutím – pre slabozrakých a nevidiacich pomocou technológie NVDA (<u>http://www.nvaccess.org/</u>).

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

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

## 4. Systémové požiadavky

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

- operačný systém MS Windows Vista / 7 / 8 / 10, Mac OS X: verzia 10.12
   10.15, GNU/Linux: Mint verzia 13, 17.x, 18; Debian verzia 8; Ubuntu verzia 12.04 LTS, 14.04 LTS, 16.04 LTS; Fedora: verzia 23, 24, 25,
- procesor (architektúra CPU): x86, x86\_64,
- 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 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 zariadením,
- web prehliadač podporujúci spúšťanie Java appletov<sup>1</sup> MS Internet Explorer v7.0 alebo vyššia (len 32 bit), Mozilla Firefox, v45 – v51, resp. v59 ESR (len 32 bit, s podporou NP API), Safari 9,
- 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, tak požiadavky na web prehliadač zahŕňajú aj prehliadače:

 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.

Pri vytváraní zaručeného elektronického podpisu pomocou aplikácie D.Signer/XAdES Java sa vyžaduje použitie certifikovaného zariadenia pre generovanie a uloženie privátneho kľúča a pre vytvorenie zaručeného elektronického podpisu (SSCD – napr. čipová karta, USB token apod.) a použitie

<sup>&</sup>lt;sup>1</sup> Ak je aplikácia D.Signer/XAdES Java spúšťaná ako Java applet.

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

kvalifikovaného certifikátu, vydaného akreditovanou certifikačnou autoritou. Ak príslušný právny úkon vyžaduje autorizáciu mandátnym kvalifikovaným certifikátom, používateľ musí zvoliť mandátny kvalifikovaný certifikát s príslušným oprávnením pre daný úkon podľa osobitného predpisu. Zoznam zobrazených certifikátov, ktoré sú k dispozícii pre vytvorenie elektronického podpisu, je možné riadiť nastavením filtra certifikátov v okne pre výber certifikátu v aplikácii D.Signer/XADES Java. Aplikácia D.Signer/XAdES Java pristupuje k danému SSCD zariadeniu prostredníctvom príslušného CSP providera (implementácia MS Crypto API pre dané SSCD zariadenie) alebo prostredníctvom 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 zariadenie. Použitá podpisová politika by mala jasne deklarovať, o aký elektronický podpis ide.

Veľkosť distribučných súborov jednotlivých komponentov aplikácie D.Signer/XAdES Java je uvedená v nasledujúcej tabuľke.

Komponent	Veľkosť
D.Signer/XadES Java	10,5 MB
D.Signer/XAdES Java – XML Plugin	450 kB
D.Signer/XAdES Java – PDF Plugin <sup>2</sup>	11,3 MB (MS Windows)
	11,6 MB (GNU/Linux)
	20,4 MB (Mac OS X)
D.Signer/XAdES Java – TXT Plugin	40 kB
D.Signer/XAdES Java – PNG Plugin	45 kB

Tzn. že pre konkrétnu platformu (OS, 32/64-bit) je veľkosť distribučných súborov cca 22,5 – 32 MB; ak sú skomprimované, tak dokonca len 15 – 25 MB.

Aplikácia D.Signer/XAdES Java vyžaduje, aby bolo v nastaveniach Java povolené ukladanie dočasných súborov. Toto nastavenie je prístupné z Java Control Panel a prednastavená hodnota je povolené ukladanie dočasných súborov.

<sup>&</sup>lt;sup>2</sup> PDF technology in D.Signer/XAdES Java - PDF Plugin is powered by PDFNet SDK copyright © PDFTron<sup>™</sup> Systems Inc., 2001-2016, and distributed by DITEC a.s. under license. All rights reserved.

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

	Temporary Files Settings ×
V	eep temporary files on my computer.
Loc	ation
	Select the location where temporary files are kept:
	\Users\vittek\AppData\LocalLow\Sun\Java\Deployment\cache Change
Dis	<pre>c Space</pre>
	Select the compression level for JAR files:
	Set the amount of disk space for storing temporary files:
	32768 🜩 MB
	Delete Files Restore Defaults
	OK Cancel

Podrobný popis požiadaviek na prevádzku aplikácie D.Signer/XAdES Java, teda požiadaviek na SSCD zariadenie, požiadaviek na prevádzkové prostredie aplikácie, bezpečnostných požiadaviek apod. je špecifikovaný v rámci dokumentu Požiadavky na prevádzkové prostredie a SSCD.

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

### 5. Distribúcia a inštalácia

Aplikácia D.Signer/XAdES Java môže byť integrovaná ako applet v rámci web aplikácie alebo ako komponent v rámci klientskej Java aplikácie bežiacej v JRE. Ak je distribúcia a inštalácia aplikácie D.Signer/XAdES Java na PC používateľa zabezpečená pomocou technológie webstart, tak integritu súborov aplikácie overuje technológia webstart pri spustení aplikácie. Jednotlivé JAR knižnice sú podpísané certifikátom výrobcu aplikácie (spoločnosť DITEC, a.s.) a je na ne vyžiadaná časová pečiatka.

Na nasledujúcom obrázku je zobrazený náhľad na aktuálny podpisový certifikát spoločnosti DITEC, a.s.

sertificate	×
General Details Certification Path	
Certificate Information	
This certificate is intended for the following purpose(s):	
<ul> <li>Ensures software came from software publisher</li> <li>Protects software from alteration after publication</li> <li>1.3.6.1.4.1.6449.1.2.1.3.2</li> </ul>	
* Refer to the certification authority's statement for details.	
Issued to: DITEC, a.s.	
Issued by: Sectigo RSA Code Signing CA	
Valid from 21.5.2019 to 21.5.2022	
Install Certificate Issuer Statement	
OK	

Používateľ si môže skontrolovať podrobnosti a platnosť certifikátu výrobcu kliknutím na link "More information" (prekl. Viac informácií) a potvrdiť spustenie aplikácie kliknutím na tlačidlo "Run" (prekl. Spustiť).

Distribúcia a inštalácia

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

Do you want	to run this	s application?
	Name:	D.Signer/XAdES Java
<b>S</b>	Publisher:	DITEC, a.s.
	Location:	
This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the location and publisher above.		
Do not show this again for apps from the publisher and location above		
More Infor	mation	Run Cancel

(Pozn. opätovnému zobrazovaniu tohto okna pri každom spustení aplikácie D.Signer/XAdES Java je možné zamedziť zaškrtnutím poľa: Do not show this again for apps from the publisher and location above; prekl. Nezobrazovať opäť pre hore uvedeného vydavateľa a miesto distribúcie aplikácie.)

Pri komunikácii webového prehliadača s Java Runtime môže byť tiež potrebné najprv povoliť prístup webového prehliadača k aplikácii D.Signer/XAdES Java kliknutím na tlačidlo "Allow" (prekl. Povoliť).

Security Warning
Allow access to the following application from this web site?
Web Site: http://java.ditec.sk
Application: D.Signer/XAdES Java Publisher: DITEC, a.s.
This web site is requesting access and control of the Java application shown above. Allow access only if you trust the web site and know that the application is intended to run on this site.
Do not show this again for this app and web site. Allow Do Not Allow
More information

(Pozn. opätovnému zobrazovaniu tohto okna pri každom spustení aplikácie D.Signer/XAdES Java je možné zamedziť zaškrtnutím poľa: Do not show this

Distribúcia a inštalácia

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

again for this app and web site; prekl. Nezobrazovať opäť pre túto aplikáciu a web.)

Alternatívnou možnosťou je distribúcia aplikácie D.Signer/XAdES Java spolu s klientskou aplikáciou, v rámci ktorej je integrovaná, z dôveryhodného zdroja napr. na CD médiu v rámci inštalačných súborov klientskej aplikácie. V tomto prípade je integrita súborov aplikácie D.Signer/XAdES Java zabezpečená samotným spôsobom distribúcie.

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

### 6. Užívateľské nastavenia

Obrazovka s užívateľskými nastaveniami aplikácie D.Signer/XAdES Java je prístupná z hlavného okna aplikácie D.Signer/XAdES Java prostredníctvom tlačidla Nastavenia.

D.Signer/XAdES Java	- 🗆 🗙				
🔃 Dokument nie je podpísaný 🛛 📄 💢 🔽 25.05.2016 17:45:13					
Pozor! Do ZEP sú zahrnuté všetky zobrazované dátové objekty (dokumenty) a parametre elektronického podpisu. Vzhľadom k tomu, že vytvorením ZEP používateľ vyjadruje svoj súhlas s obsahom jednotlivých dokumentov, je v jeho záujme, aby sa dôkladne oboznámil s obsahom všetkých zobrazených dátových objektov. Žiadosť o prihlásenie vozidla do evidencie					
Žiadosť o prihlásenie vozidla do evidencie Identifikačné údaje vozidlaBL869FY vin: 1234567878896987 Údaje o žiadateľovi priezviskoNazov: Test Udajeoziad_Priezvisko21: Testovaci datumNarodeniaICO: 2013-11-06 rodneCislo: 8510094565 Udajeoziad_Obchodneme21: obchodne meno Údaje o držiteľovi uvednom pri prevode drživ vozidla					
Zalomiť text	Xml dáta Verifikačné dáta				
	Podpísať OK Storno				

### 6.1. Nastavenie jazyka aplikácie

V rámci nastavení aplikácie D.Signer/XAdES Java môže používateľ zmeniť nastavenie jazyka aplikácie. Nastavenie nového jazyka sa aplikuje pri ďalšom spustení aplikácie D.Signer/XAdES Java.

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

¢.	Nastavenia	×
Jazyk aplikácie ———	$\sim$	
	Slovenský 🔻	
Spôsob prístupu k certi	ifikátom	
	CryptoAPI OPKCS#11/PKCS#12	
	ок	Zrušiť

V prípade vynútenia jazyka aplikácie D.Signer/XAdES Java z prostredia klientskej aplikácie nebudú konfiguračné nastavenia jazyka aplikácie pre používateľa prístupné.

# 6.2. Nastavenie spôsobu prístupu k SSCD a podpisovým certifikátom

Aplikácia D.Signer/XAdES Java využíva pri vytváraní zaručeného elektronického podpisu certifikované SSCD zariadenie pre generovanie kľúčových párov a vytváranie elektronického podpisu, ku ktorému pristupuje pomocou CSP implementácie MS Crypto API alebo príslušnej PKCS#11 knižnice. Zároveň umožňuje vytvoriť aj obyčajný elektronický podpis napr. pomocou certifikátu uloženom v rámci PKCS#12 súboru. Predvolený spôsob prístupu k SSCD, resp. k PKCS#12 súboru (a teda aké podpisové certifikáty bude mať používateľ k dispozícii), je uložený v rámci konfigurácie aplikácie.

Po vytvorení inštancie modulu D.Signer/XAdES Java sa aplikácia v rámci inicializácie pokúsi načítať nastavenia pre prístup k SSCD a podpisovým certifikátom, ktoré sú uložené v rámci konfigurácie. Ak takéto nastavenia ešte neexistujú, tak otvorí používateľovi dialóg, v ktorom mu umožní nastaviť:

Užívateľské nastavenia

-16/35-

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

- buď prístup k SSCD pomocou MS Crypto API v tomto prípade bude mať používateľ pri výbere certifikátu k dispozícii všetky platné certifikáty uložené v MS Personal Certificate Store, ku ktorým existuje privátny kľúč,
- alebo pomocou PKCS#11 knižnice používateľ bude môcť špecifikovať cestu k PKCS#11 knižnici, ktorú má nainštalovanú v systéme. V tomto prípade bude mať používateľ pri výbere certifikátu k dispozícii všetky platné certifikáty uložené na príslušnom SSCD zariadení, ktoré je prístupné pomocou špecifikovanej PKCS#11 knižnice a ku ktorým existuje privátny kľúč,
- alebo prístup k PKCS#12 (PFX) súboru, ktorý má uložený na disku. V tomto prípade bude mať používateľ pri výbere certifikátu k dispozícii všetky platné certifikáty uložené v špecifikovanom PFX súbore, ku ktorým existuje privátny kľúč.

Na platforme Windows sa dialóg pre nastavenie prístupu k SSCD neotvorí, ale sa štandardne nastaví prístup k SSCD prostredníctvom MS Crypto API.

Po potvrdení konfigurácie prístupných SSCD zariadení a podpisových certifikátov aplikácia D.Signer/XAdES Java uloží tieto nastavenia v rámci konfigurácie aplikácie. Správa prístupných SSCD zariadení a podpisových certifikátov je používateľovi k dispozícii takisto z prostredia aplikácie D.Signer/XAdES Java prostredníctvom tlačidla Nastavenia.

Na nasledujúcom obrázku je zobrazený príklad nastavenia prístupu k SSCD pomocou MS Crypto API.

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

e	Nastavenia	×
<sub>–</sub> Jazyk aplikácie —		
	Slovenský 💌	
<sub>[</sub> Spôsob prístupu k	certifikátom	
	CryptoAPI     PKCS#11/PKCS#12	
	OK Z	Irušiť

Na nasledujúcom obrázku je zobrazený príklad nastavenia prístupu k SSCD pomocou PKCS#11 knižnice a prístup k certifikátom, ktoré sú uložené v rámci PKCS#12 (PFX) súborov (pozn. konkrétne pre prístup k SSCD prostredníctvom PKCS#11 knižnice poskytovateľa kryptografických služieb I.CA – SecureStore).

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

Nastavenia ×			
Jazyk aplikácie			
Slovenský 🔻			
Spôsob prístupu k certifikátom			
CryptoAPI • PKCS#11/PKCS#12			
Výber poskytovateľa kryptografických služieb			
Označte v zoznamoch všetkých poskytovateľov kryptografických služieb, ktorých si želáte používať. V prípade že sa želaný poskytovateľ v zozname nenachádza, je možné ho pridať pomocou tlačidla "+". Automatické označenie všetkých dostupných poskytovateľov je možné vykonať kliknutím na tlačidlo "Autokonfigurácia".			
Systémové Používateľské			
✓ eld klient ■ PSCA SafeNat Authenticat			
✓ I.CA- SecureStore			
Autokonfigurácia			
Slot-			
#1 9203030000013131 (9203030000013131)			
OK Zrušiť			

Aplikácia D.Signer/XAdES Java obsahuje konfiguráciu preddefinovaných systémových poskytovateľov kryptografických služieb a umožňuje tiež konfiguráciu používateľom definovaných poskytovateľov kryptografických služieb.

V rámci systémových poskytovateľov sú preddefinované nastavenia pre prístup k najbežnejšie používaným SSCD zariadeniam, ktoré sú distribuované používateľom akreditovanými certifikačnými autoritami pri zaobstaraní si kvalifikovaného certifikátu pre vytvorenie ZEP. Používateľ môže definovať zoznam povolených poskytovateľov kryptografických služieb<sup>3</sup> – stačí označiť tých

<sup>&</sup>lt;sup>3</sup> Teda tých poskytovateľov kryptografických služieb, ktorí budú k dispozícii pri výbere podpisového certifikátu.

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

systémových poskytovateľov kryptografických služieb, ktorých si želá používať (resp. systémových poskytovateľov kryptografických služieb k tým SSCD zariadeniam, na ktorých má uložené svoje kvalifikované certifikáty, ktoré si želá používať). Automatické označenie všetkých dostupných poskytovateľov je možné vykonať kliknutím na tlačidlo "Autokonfigurácia".

Definovanie predvoleného (default) poskytovateľa kryptografických služieb je možné označením jeho mena a výberom slotu (úložiska certifikátov na SSCD

zariadení). Kliknutím na tlačidlo s ikonou ie je možné aktualizovať zoznam slotov predvoleného poskytovateľa kryptografických služieb.

V prípade, že sa želaný poskytovateľ kryptografických služieb v zozname systémových a používateľských poskytovateľov nenachádza, je možné ho pridať do zoznamu používateľských poskytovateľov pomocou tlačidla "+". Nepotrebného poskytovateľa kryptografických služieb je možné odobrať zo zoznamu používateľských poskytovateľov pomocou tlačidla "-". Pomocou tlačidla s ikonou kľúča je možné zmeniť nastavenia pre používateľom definovaného poskytovateľa kryptografických služieb.

Na nasledujúcom obrázku je zobrazená obrazovka pre používateľom definovaného nového poskytovateľa kryptografických služieb.

e 🖉	Nový poskytovateľ kryptografických služieb		
Meno:	I.CA_SecureStore	Typ: PKCS11	•
Súbor:	C:\Windows\System32\SecureStorePkcs	:11.dll	
OS:	Windows	Architektúra: x86	
			OK Zrušiť

Pri definovaní nového poskytovateľa kryptografických služieb musí používateľ špecifikovať:

- meno poskytovateľa kryptografických služieb (používateľom špecifikované meno),
- typ poskytovateľa kryptografických služieb:
  - ⇒ PKCS#11, ak chce definovať poskytovaľa kryptografických služieb pre prístup k SSCD zariadeniu,
  - ⇒ PKCS#12, ak chce špecifikovať prístup k PKCS#12 (PFX) súboru s podpisovým certifikátom,
- cestu k PKCS#11 knižnici poskytovateľa kryptografických služieb alebo cestu k PKCS#12 (PFX) súboru s podpisovým certifikátom,

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

 hodnoty polí OS (operačný systém; možné hodnoty: "Windows", "Linux", "Mac OS X") a architektúra (možné hodnoty: "x86", "i386", "x86\_64", "amd64") budú nastavené automaticky na základe Java platformy, v rámci ktorej je aplikácia D.Signer/XAdES Java spustená.

Pri výbere PKCS#11 knižnice je potrebné zvoliť knižnicu, ktorá zodpovedá identifikovanému operačnému systému a architektúre Java Runtime.

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

## 7. Vytvorenie ZEP používateľom

### 7.1. Načítanie vstupných parametrov

Stiahnutie všetkých komponentov aplikácie D.Signer/XAdES Java pomocou technológie webstart môže vyžadovať istý čas, počas ktorého môže byť proces sťahovania aplikácie indikovaný na danej web stránke napríklad prostredníctvom nasledujúceho indikátora.

A.

### 7.2. Súhlas s licenčnou zmluvou

V prípade, že súčasťou distribúcie aplikácie D.Signer/XAdES Java je aj PDF Plugin, tak je potrebné potvrdiť licenčnú zmluvu pre použitie knižnice PDFNet SDK<sup>4</sup>, ktorá tvorí súčasť PDF Pluginu aplikácie D.Signer/XAdES Java.

e e	D.Signer/XAdES Java - PDF Plugin	×		
uzavretá podľa zákona č.	Licenčná zmluva . 618/2003 Z. z. o autorských právach a právach súvisiacich s autorským právom v úplnom zner (ďalej len "autorský zákon") (ďalej len "zmluva")	ní		
Táto Zmluva je uzatvorená	medzi spoločnosťou			
Obchodné meno:	DITEC, a.s.			
Sidlo:	Plynárenská 7/C, 821 09 Bratislava			
IČO:	31 385 401			
DRČ:	202 030 4198			
IČ pre DPH:	SK 202 030 4198			
Spoločnosť je zapisaná v OR Okresného súdu Bratislava I Oddiel: Sa; Vložka čislo: 769/B.				
(ďalej len "Poskytovateľ")				
a fyzickou osobou alebo právnickou osobou, ktorá Softvér inštaluje, sťahuje, kopiruje alebo používa (ďalej len "Používateľ"), pričom				
	Súhlasím Nesúhl	asím		

<sup>&</sup>lt;sup>4</sup> PDF technology in D.Signer/XAdES Java - PDF Plugin is powered by PDFNet SDK copyright © PDFTron<sup>™</sup> Systems Inc., 2001-2016, and distributed by DITEC a.s. under license. All rights reserved.

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

### 7.3. Zobrazenie podpisovaných dát

Pokiaľ všetky kontroly vstupných parametrov prebehli úspešne, na jednotlivých záložkách hlavného okna sú zobrazené časti podpisovaného *multipart* dokumentu. Používateľ má možnosť prezrieť všetky podpisované dátové objekty a ďalšie parametre podpisu.

Pozor! Do ZEP sú zahrnuté všetky zobrazované dátové objekty (dokumenty) a parametre elektronického podpisu. Vzhľadom k tomu, že vytvorením ZEP používateľ vyjadruje svoj súhlas s obsahom jednotlivých dokumentov, je v jeho záujme, aby sa dôkladne oboznámil s obsahom všetkých zobrazených dátových objektov.

🔱 Dokument nie je podpísaný 🛛 📓 💥 🔽 25.05.2016 16:51:39 🛛 🔀 🥥					
Pozor! Do ZEP sú zahrnuté všetky zobrazované dátové objekty (dokumenty) a parametre elektronického podpisu. Vzhľadom k tomu, že vytvorením ZEP používateľ vyjadruje svoj súhlas s obsahom jednotlivých dokumentov, je v jeho záujme, aby sa dôkladne oboznámil s obsahom všetkých zobrazených dátových objektov.					
PDF1 PNG1					
🗋 📄 🐵 🕢 🜗 🕨 🔲 🖬 💷 🖁 💾 Verifikačné dáta					
<pre></pre>					
Strana 1 z 1					
Podpisat OK Storno					

Pokiaľ sa vyskytli pri kontrole vstupných parametrov chyby, aplikácia D.Signer/XAdES Java zobrazí chybovú správu. V takomto prípade sa tiež zobrazí hlavné okno aplikácie D.Signer/XAdES Java, ale nebude možné uskutočniť vytvorenie podpisu (tlačidlo Podpísať bude neprístupné).

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

¢	D.Signer/XAdES Java	- 🗆 ×		
🔱 Dokument nie je podpísaný	25.05.2016 15:59:48	× 0		
Pozor! Do ZEP sú zahrnuté všetky zobr tomu, že vytvorením ZEP používateľ vy dôkladne oboznámil s obsahom všetkýc	azované dátové objekty (dokumenty) a parametre el jadruje svoj súhlas s obsahom jednotlivých dokumer :h zobrazených dátových objektov.	lektronického podpisu. Vzhľadom k ntov, je v jeho záujme, aby sa		
xmlObjectDescription				
HTML vizualizáciu XML dokumentu	nie je možné zobraziť! HTML vizualizácia obsa	ahuje zakázané elementy!		
Podpísanie nie je možné!				
		Podpísať OK Storno		

V rámci hlavného okna aplikcácie D.Signer/XAdES Java je tiež zobrazený stav podpisovaného dokumentu, ktorý môže nadobúdať nasledujúce hodnoty:

- Dokument nie je podpísaný
- Dokument bol podpísaný

V závislosti od stavu dokumentu sú jednotlivé tlačidlá hlavného okna aplikácie D.Signer/XAdES Java prístupné alebo neprístupné.

Aplikácia D.Signer/XAdES Java slúži na vytváranie (zaručeného) elektronického podpisu 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.

Pre jednotlivé požadované formáty dokumentov musí mať používateľ nainštalované príslušné plugin moduly aplikácie D.Signer/XAdES Java. Informácia o nainštalovaných plugin moduloch je používateľovi prístupná prostredníctvom tlačidla <sup>20</sup> "Pomoc".

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

e e	O aplikácii ×
d 🧷	Názov: D.Signer/XAdES Java Verzia: 2.0.0.0 Autor: Ditec, a.s.
Zoznan	n aktívnych pluginov:
1. sk.o 2. sk.o 3. sk.o 4. sk.o	ditec.zep.dsigner.xades.plugins.xmlplugin.XmlPlugin, 2.0.0.0 ditec.zep.dsigner.xades.plugins.txtplugin.TxtPlugin, 2.0.0.0 ditec.zep.dsigner.xades.plugins.pngplugin.PngPlugin, 2.0.0.0 ditec.zep.dsigner.xades.plugins.pdfplugin.PdfPlugin, 2.0.0.0
Zoznam	n použitých komponentov:
Apach jsoup JTatto Simple The A The A The L	e Santuario ( <u>http://santuario.apache.org</u> ) ( <u>http://jsoup.org</u> ) o ( <u>http://www.jtattoo.net</u> ) e Logging Facade for Java ( <u>http://www.slf4j.org</u> ) pache Xalan Project ( <u>http://xalan.apache.org</u> ) pache Xerces™ Project ( <u>http://xerces.apache.org</u> ) egion of the Bouncy Castle ( <u>https://www.bouncycastle.org</u> )
PDF to © PDI rights	echnology in D.Signer/XAdES Java - PDF Plugin is powered by PDFNet SDK copyright FTron™ Systems Inc., 2001-2016, and distributed by DITEC a.s. under license. All reserved.
	Systémové informácie Zavrieť

Zároveň sú na obrazovke zobrazené informácie o použitých komponentoch aplikácie D.Signer/XAdES Java a v prípade problémov je možné získať pre pracovníkov podpory ďalšie systémové informácie o prostredí aplikácie kliknutím na tlačidlo "Systémové informácie".

#### 7.3.1. Zobrazenie dokumentov

Zobrazenie dokumentov je realizované v rámci aplikácie D.Signer/XAdES Java pomocou príslušného pluginu pre daný typ dát, ktorý poskytuje aplikácii D.Signer/XAdES Java funkcie pre vizualizáciu dát daného typu. Jednotlivé podpisované dátové objekty (resp. dokumenty) sú zobrazené na samostatných záložkách, ktorých názov bližšie určuje obsah príslušného dokumentu.

Vytvorenie ZEP používateľom

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

Používateľ má takto možnosť pred vytvorením elektronického podpisu prezrieť obsah všetkých podpisovaných dokumentov.

Na nasledujúcom obrázku je príklad zobrazenia XML dokumentu v HTML vizualizácii v rámci aplikácie D.Signer/XAdES Java.

C.	D.Signer/XAdES Java	- 🗆 ×				
i) Dokument nie je podpísaný	🔊 📄 🗶 🔽 25.05.2016 16:05:25	] 🗶 🔞				
Pozor! Do ZEP sú zahrnuté všetky z tomu, že vytvorením ZEP používateľ dôkladne oboznámil s obsahom všel	<sup>3</sup> ozor! Do ZEP sú zahrnuté všetky zobrazované dátové objekty (dokumenty) a parametre elektronického podpisu. Vzhľadom k iomu, že vytvorením ZEP používateľ vyjadruje svoj súhlas s obsahom jednotlivých dokumentov, je v jeho záujme, aby sa dôkladne oboznámil s obsahom všetkých zobrazených dátových objektov.					
Žiadosť o prihlásenie vozidla	do evidencie					
Ziadostoprihlaseniev	ozidladoevidencie					
Ziadostoprihlasenie	vozidladoevidencie_Identifikacneudajevozidl	la				
Evidenčné číslo::	Evidenčné číslo:: BL869FY					
VIN::	1234567878896987					
Xml dáta Verifikačné dáta						
	Pot	dpísať OK Storno				

#### 7.4. Nastavenie dátumu a času vytvorenia podpisu

Aplikácia D.Signer/XAdES Java umožňuje používateľovi v prípade potreby nastaviť pomocou ovládacích prvkov, ktoré sú umiestnené v hornej lište okna aplikácie, dátum a čas vytvorenia podpisu. Používateľ môže takto deklarovať vytvorenie elektronického podpisu v špecifikovanom dátume a čase, pričom tento deklarovaný dátum a čas vytvorenia podpisu je zahrnutý do podpisovaných atribútov vytváraného elektronického podpisu a následne vyhodnocovaný na strane overovateľa. Je teda potrebné, aby používateľ pri vytváraní elektronického podpisu nastavil taký dátum a čas vytvorenia podpisu, ktorý neznemožní spracovanie vytvoreného elektronického podpisu na strane overovateľa.

Aplikácia umožňuje používateľovi deklarovať ako čas vytvorenia podpisu:

 buď aktuálny systémový dátum a čas, ak je zvolené v zaškrtávacom políčku použitie systémového dátumu a času,

Vytvorenie ZEP používateľom

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

 alebo manuálne nastaviť deklarovaný dátum a čas vytvorenia podpisu, ak je v zaškrtávacom políčku použitie systémového dátumu a času odznačené.

V prvom prípade nie je možné manuálne nastaviť deklarovaný dátum a čas vytvorenia podpisu, použije sa aktuálny systémový dátum a čas.

D.Signer/XAdES Java	- 🗆 🗙
🗼 Dokument nie je podpísaný 🛛 📄 🔍 🔽 25.05.2016 16:57:33	)× @
Pozor! Do ZEP sú zahrnuté všetky zobrazované dátové objekty (dokumenty) a parametre tomu, že vytvorením ZEP používateľ vyjadruje svoj súhlas s obsahom jednotlivých dokun dôkladne oboznámil s obsahom všetkých zobrazených dátových objektov.	e elektronického podpisu. Vzhľadom k nentov, je v jeho záujme, aby sa
Žiadosť o prihlásenie vozidla do evidencie	
Žiadosť o prihlásenie vozidla do evidencie Identifikačné údaje vozidlaBL869FY vin: 1234567878896987 Údaje o žiadateľovi	
priezviskoNazov: Test Udajeoziad_Priezvisko21: Testovaci datumNarodenialCO: 2013-11-06 rodneCislo: 8510094565 Udajeoziad_Obchodneme21: obchodne me	no.
Údaje o držiteľovi uvedenom pri prevode držby vozidla tvpSubiektu 01: 1	
Zalomiť text	Xml dáta Verifikačné dáta
	Podpísať OK Storno

V druhom prípade sa používateľovi sprístupní deklarovaný dátum a čas vytvorenia podpisu na editovanie.

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

D.Signer/XAdES Java		-		×
Dokument nie je podpísaný 📓 🗮 🗙 25.05.2016 16:58:30	×	0		
Pozor! Do ZEP sú zahrnuté všetky zobrazované dátové objekty (dokumenty) a parametre elektronicky tomu, že vytvorením ZEP používateľ vyjadruje svoj súhlas s obsahom jednotlivých dokumentov, je v j dôkladne oboznámil s obsahom všetkých zobrazených dátových objektov.	ého podr eho záuj	oisu. V: me, ab	zhľado y sa	ım k
Žiadosť o prihlásenie vozidla do evidencie				
Žiadosť o prihlásenie vozidla do evidencie Identifikačné údaje vozidlaBL869FY vin: 1234567878896987 Údaje o žiadateľovi priezviskoNazov: Test Udajeoziad_Priezvisko21: Testovaci datumNarodeniaICO: 2013-11-06 rodneCislo: 8510094565 Udajeoziad_Obchodneme21: obchodne meno Údaje o držiteľovi uvedenom pri prevode držby vozidla				
Zalomiť text Xml dát	a Ve	erifikač	iné dá	ita
Pod	dpísať	OK	St	orno

### Pozor! Pri vytváraní elektronického podpisu odporúčame použiť správne nastavený aktuálny systémový dátum a čas.

V prípade, že v rámci danej klientskej aplikácie nie je potrebné do parametrov podpisu zahrnúť aj používateľom deklarovaný dátum a čas vytvorenia podpisu, nemusia byť príslušné ovládacie prvky pre jeho nastavenie k dispozícii. Ich zobrazenie závisí na zavolaní príslušných funkcií aplikačného rozhrania aplikácie D.Signer/XAdES Java z klientskej aplikácie.

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

D.Signer/XAdES Java	- 🗆 ×
🔃 Dokument nie je podpísaný 🛛 📄 🗙 🧏 🎯	
Pozor! Do ZEP sú zahrnuté všetky zobrazované dátové objekty (dokumenty) a parametr tomu, že vytvorením ZEP používateľ vyjadruje svoj súhlas s obsahom jednotlivých dokur dôkladne oboznámil s obsahom všetkých zobrazených dátových objektov.	e elektronického podpisu. Vzhľadom k nentov, je v jeho záujme, aby sa
Žiadosť o prihlásenie vozidla do evidencie	
Žiadosť o prihlásenie vozidla do evidencie Identifikačné údaje vozidlaBL869FY vin: 1234567878896987 Údaje o žiadateľovi priezviskoNazov: Test Udajeoziad_Priezvisko21: Testovaci datumNarodeniaICO: 2013-11-06 rodneCislo: 8510094565 Udajeoziad_Obchodneme21: obchodne me Údaje o držiteľovi uvedenom pri prevode držby vozidla typSubjektu 01: 1	eno V
Zalomiť text	Xml dáta Verifikačné dáta
	Podpísať OK Storno

### 7.5. Podpísanie dokumentu

V prípade úspešného načítania všetkých častí podpisovaného dokumentu je prístupné tlačidlo Podpísať, ktoré aktivuje proces vytvorenia elektronického podpisu dokumentu. Prvým krokom procesu vytvorenia podpisu je výber certifikátu, ktorým bude daný dokument podpísaný. V prípade, že nastavený spôsob prístupu k SSCD a podpisovým certifikátom je prostredníctvom PKCS#11 knižnice, tak pred výberom podpisového certifikátu je ešte potrebné zvoliť poskytovateľa kryptografických služieb zo zoznamu povolených poskytovateľov a slot (úložisko certifikátov na SSCD zariadení).

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

e	Nastavenia ×
<sub>E</sub> Jazyk apliká	icie
	Slovenský 💌
<sub>[</sub> Spôsob prí:	stupu k certifikátom
	CryptoAPI  • PKCS#11/PKCS#12
<sub>E</sub> Výber posky	/tovateľa kryptografických služieb
Knižnica Pł	<cs#11 pkcs#12<="" súbor="" td=""></cs#11>
I.CA - Secu	ireStore
Súbor: C	:Windows\System32\SecureStorePkcs11.dll
Slot-	
#1 92030	)30000013131 (9203030000013131)
#2 92030	) <del>36600012248 (020303666601</del> 2248)
	Ďalej Zrušiť

Na nasledujúcom obrázku je znázornený dialóg prevýber certifikátu podpisovateľa.

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

Výber certifikátu 🗙					
Vyberte certifikát, ktorý chcete použiť. Pre vytvorenie zaručeného elektronického podpisu musí byť použitý kvalifikovaný certifikát, vydaný akreditovanou certifikačnou autoritou.					
Ak príslušný právny úkon vyžaduje autorizáciu mandátnym kvalifikovaným certifikátom, vyberte mandátny kvalifikovaný certifikát s príslušným oprávnením pre daný úkon podľa osobitného predpisu. Zoznam zobrazených certifikátov, ktoré sú k dispozícii pre vytvorenie elektronického podpisu, je možné riadiť nastavením filtra certifikátov.					
Overte platnosť vybraného podpisového certifikátu na základe relevantných verejne dostupných informácii o revokácii (aktuálne platný zoznam zrušených certifikátov). Použitie neplatného certifikátu má za následok vytvorenie neplatného elektronického podpisu!					
Potvrdením výberu certifikátu podpíšete	e dokument!				
Filtrovať zoznam certifikátov: SK QC	•				
Vydaný pre	Vydavateľ	Platný do			
	LCA - Qualified Certification Auth 12. 01. 2017 16:24:37				
C Zobraziť certifikát OK Storno					

V rámci zoznamu osobných certifikátov na danom PC sú zobrazené položky:

- meno subjektu, pre ktorý bol certifikát vydaný,
- meno vydavateľa certifikátu,
- dátum konca platnosti certifikátu.

Detaily zvoleného certifikátu je možné prezrieť kliknutím na tlačidlo "Zobraziť

certifikát". V prípade potreby je možné kliknutím na tlačidlo s ikonou sktualizovať zoznam zobrazených certifikátov.

Integrátor aplikácie D.Signer/XAdES Java môže spolu s aplikáciou distribuovať tiež nastavenia filtra pre zobrazenie len určitých certifikátov, ktoré spĺňajú definované pravidlá. V uvedenom dialógu pre výber certifikátu podpisovateľa sú napríklad zobrazené len kvalifikované certifikáty vydané v súlade so slovenskou legislatívou.

Pre vytvorenie zaručeného elektronického podpisu musí podpisovateľ zvoliť zo svojho personálneho úložiska certifikátov kvalifikovaný certifikát, ktorý bol vydaný akreditovanou certifikačnou autoritou. Ak príslušný právny úkon vyžaduje autorizáciu mandátnym kvalifikovaným certifikátom, používateľ musí zvoliť mandátny kvalifikovaný certifikát s príslušným oprávnením pre daný úkon podľa osobitného predpisu. Pre vytvorenie obyčajného elektronického podpisu nie je potrebné použiť kvalifikovaný certifikát vydaný akreditovanou certifikačnou autoritou.

Vytvorenie ZEP používateľom

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

Zoznam zobrazených certifikátov, ktoré sú k dispozícii pre vytvorenie elektronického podpisu, je možné riadiť nastavením filtra certifikátov v okne pre výber certifikátu v aplikácii D.Signer/XADES Java.

Výber certifikátu ×					
Vyberte certifikát, ktorý chcete použiť. Pre vytvorenie zaručeného elektronického podpisu musí byť použitý kvalifikovaný certifikát, vydaný akreditovanou certifikačnou autoritou.					
Ak príslušný právny úkon vyžaduje autorizáciu mandátnym kvalifikovaným certifikátom, vyberte mandátny kvalifikovaný certifikát s príslušným oprávnením pre daný úkon podľa osobitného predpisu. Zoznam zobrazených certifikátov, ktoré sú k dispozícii pre vytvorenie elektronického podpisu, je možné riadiť nastavením filtra certifikátov.					
Overte platnosť vybraného podpisovéh (aktuálne platný zoznam zrušených ce elektronického podpisu!	Overte platnosť vybraného podpisového certifikátu na základe relevantných verejne dostupných informácii o revokácii (aktuálne platný zoznam zrušených certifikátov). Použitie neplatného certifikátu má za následok vytvorenie neplatného elektronického podpisu!				
Potvrdením výberu certifikátu podpíšete	e dokument!				
Filtrovať zoznam certifikátovi (SK QC					
Vydaný pre	Vydavateľ	Platný do			
	I.CA - Qualified Certification Auth	12. 01. 2017 16:24:37			
C Zobraziť certifikát OK Storno					

Po zvolení certifikátu a potvrdení výberu tlačidlom OK sa vykoná proces vytvorenia elektronického podpisu. Aplikácia D.Signer/XAdES Java vytvorí reprezentáciu podpisovaných dát a parametrov podpisu – digitálny odtlačok. Pomocou rozhrania MS CryptoAPI, resp. PKCS#11 knižnice a príslušného SSCD zariadenia, na ktorom je uložený privátny kľúč patriaci k zvolenému podpisovému certifikátu, vytvorí hodnotu elektronického podpisu. Sprístupnenie privátneho kľúča na SSCD zariadení môže vyžadovať autentifikáciu používateľa – zadanie PINu.<sup>5</sup>

<sup>&</sup>lt;sup>5</sup> Nastavenia SSCD (napr. timeout pre PIN, dĺžka PIN apod.) sú v správe používateľa SSCD zariadenia. Aplikácia D.Signer/XAdES Java neumožňuje meniť tieto nastavenia.

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

SecureStoreCSP - zadať PIN ×				
K uskutočneniu operácie je potrebné zadať PIN. Operácia : Podpis dát kľúčom umiestneným na karte				
PIN: ****				
☐ Zapamätať PIN				
OK Storno				

Aplikácia D.Signer/XAdES Java následne vytvorí a sformátuje výstupný podpísaný dokument v súlade s profilom XAdES\_ZEP, resp. XAdES\_ZEPbp. V prípade chyby v rámci procesu vytvorenia podpisu sa zobrazí príslušné chybové hlásenie. Ak sa dokument podarilo podpísať, v hlavnom okne sa zmení stav dokumentu a niektorých tlačidiel (sprístupnia sa tlačidlá tých funkcií, ktoré je možné vykonať len nad podpísaným dokumentom).

1	D.Signer/XAdES Java -					
🔱 Dokument bol podpísaný 🍶 🗎 🗙	× 0					
Pozor! Do ZEP sú zahrnuté všetky zobrazované dátové objekty (dokumenty) a parametre elektronického podpisu. Vzhľadom k tomu, že vytvorením ZEP používateľ vyjadruje svoj súhlas s obsahom jednotlivých dokumentov, je v jeho záujme, aby sa dôkladne oboznámil s obsahom všetkých zobrazených dátových objektov.						
Žiadosť o prihlásenie vozidla do evidenci	ie					
Žiadosť o prihlásenie vozidla do evidencie	3					
Identifikačné údaje vozidla	aBL869FY					
vin: 12345	567878896987					
Údaje o žiadateľovi						
priezviskoNazov: Test						
Udajeoziad_Priezvisko21: Testovaci						
datumNar	rodenialCO: 2013-11-06					
rodneCisl	lo: 8510094565					
Udajeozia	ad_Obchodneme21: obchodne meno					
Udaje o držiteľovi uvedeno	om pri prevode držby vozidla					
typSubjek	du 01:1					
Zalomiť text	Xml dáta Verifika	ačné dáta				
	Podpísať O	< Storno				

Po úspešnom vytvorení elektronického podpisu je podpísaný dokument odovzdaný klientskej aplikácii až po kliknutí na tlačidlo OK.

Vytvorenie ZEP používateľom

-33/35-

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

### 7.6. Zobrazenie parametrov podpisu

Používateľ, resp. podpisovateľ si môže pred alebo po podpísaní dokumentu zobraziť parametre podpisu (ikona s ozubeným kolieskom v hornej časti). V prípade ich zobrazenia pred vytvorením podpisu, resp. po vymazaní podpisu (tlačidlo Zmazať podpis – s ikonou s červeným krížikom v hornej časti okna), zobrazené informácie nebudú úplné, pretože niektoré z nich sú závislé na výbere podpisového certifikátu.

Na nasledujúcom obrázku je zobrazené dialógové okno s parametrami podpisu po podpísaní dokumentu. K dispozícii sú všetky tlačidlá, ako aj informácie o formáte vytvoreného podpisu, použitých kryptografických algoritmoch a vypočítaných hodnôt odtlačkov, podpisovej politike, podpisovom certifikáte, ako aj samotná hodnota vytvoreného podpisu.

ø	Parametre podpisu	×
Š	pecifikácia formátu podpisu: http://www.ditec.sk/ep/signature_formats/xades_zep/v1.1 Identifikátor algoritmu kanonizácie podpisovaných informácií: http://www.w3.org/TR/2001/REC-xml-c14n-20010315 Identifikátor algoritmu digitálneho podpisu: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256	
P s p h	odpisová politika: Identifikátor podpisovej politiky: urn:oid:1.3.158.36061701.1.2.1 Identifikátor algoritmu digitálneho odtlačku: http://www.w3.org/2001/04/xmlenc#sha256 Hodnota digitálneho odtlačku: +Ce4bXF5DGPGR63De6v7IrF0uFqsaBjrQTV5h7gs1jc= Platnosť od: 03.12.2013 01:00:00 Platnosť do: 03.12.2017 01:00:00 Povinnosť uvádzať dátum a čas vytvorenia podpisu: Áno Pre vytvorenie ZEP musí byť aplikácia použítá len v súlade s platnou podpisovou politikou pre ZEP, ktorá bola chválená NBÚ SR. Používateľ je pred vytvorením podpisu povinný presvedčiť sa, že podpisová politika, ktorú aplikácia oužíva, je stále platná a nebola zo strany vydavateľa predčasne zrušená. URL pre overenie platnosti podpisovej politiky: ttp://www.nbusr.sk/sk/elektronicky-podpis/podpisove-politiky/index.html	
	lodnota digitálneho podpisu: tbMDN4yWnl8SGXSoAWqJL3cJup3T1U0fCjEta8nOojyGdnrt0u3riyo+fHeLCLOyAJl8KApiNwW0EmrFQis1rhMoQbC4wQe IDntzy3glwr2c2QTWApI2VecS9uWluqitdEbiEGKiudB7nPSDRW3jhk5vG62KK0Miz4hZKo9ffaUDpPNM82174wOfxKRmkR yUDrP+eJNzv0dCn0vcJCVY1SHXtsCpabyk1bUmEGe3rpn2FDPRkfW7SJJUZevq0oy0lqQXNwLcH0cN4uh+OI6XVnt6BnX7 qxd82L9DolLAL24TyvGgyni54rBVIcKt9dZhYf9tpYeVV9V4DQCliRoWw==	
lo	dentifikácia certifikátu podpisovateľa: Vydavateľ: I.CA - Qualified Certification Authority, 09/2009 Sériové číslo <del>: Engeneration</del> Názov subjektu: Engeneration	
D	látum a čas vytvorenia podpisu: 25.05.2016 17:09:31	•
	Uložiť Zavi	riet'

V prípade, že podpis je z nejakého dôvodu potrebné zrušiť, tak je toto umožnené kliknutím na ikonu s červeným krížikom v hornej časti – Zrušiť vytvorený podpis a uviesť tak aplikáciu do východzieho stavu.

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.212	Verzia	6

## 8. Trademarks

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

