DITEC
Data Information Technology & Expert Consulting

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

# Copyright



**Popisné charakteristiky dokumentu**

| | | | |
|---|---|---|---|
| Projekt | GOV_ZEP | | A3019_002 |
| Dokument | Integračná príručka | | |
| Podnázov | D.Signer/XAdES Java - PNG Plugin, v2.0 | | |
| Ref. číslo | GOV_ZEP.211 | Verzia | 4 |

| | | | |
|---|---|---|---|
| Vypracoval | Vittek Robert | Podpis | Dátum 27. 12. 2022 |
| 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.211 | Verzia | 4 |

## 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 – PNG Plugin 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.

# 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

PNG – Portable Network Graphics

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, v1.2 (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 PNG obrázok v rámci profilu XAdES_ZEP, v1.0, DITEC, a.s., 2013

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

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

[32] 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

[33] 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

[34] 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

[35] 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

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

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

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

[39] 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

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

# 4. Formát PNG

Formát PNG (Portable Network Graphics) je bitmapový bezstratový obrazový formát, ktorý vznikol s cieľom zlepšiť a nahradiť formát GIF, ktorý bol patentovo chránený (resp. v ňom použitá dátová kompresia LZW). V súčasnosti je stále platná verzia 1.2, ktorá bola v roku 2004 publikovaná ako ISO/IEC štandard [31].

PNG ponúka podporu 24-bitovej farebnej hĺbky, nemá teda ako GIF obmedzenie na maximálny počet 256 farieb súčasne. PNG teda do istej miery nahradzuje GIF, ponúka viac farieb a lepšiu kompresiu. Navyše obsahuje osembitovú priehľadnosť (tzv. alfa kanál), to znamená, že obrázok môže byť v rôznych častiach rôzne priehľadný (tzv. RGBA farebný model). PNG však neumožňuje jednoduché animácie, ktoré naopak umožňuje formát GIF.

Obrázky vo formáte PNG sa používajú aj na dlhodobú archiváciu. Medzi ich základné výhody patrí široká podpora na úrovni operačných systémov a grafických programov, nakoľko pre jeho použitie nie je potrebná licencia. Primárne je tento formát určený na prenos obrázkov na internete. Patrí k najmladším grafickým formátom.

Formát PNG má oporu v legislatíve ako jeden z dátových formátov, nad ktorými je možné vytvárať zaručený/kvalifikovaný elektronický podpis (ZEP/KEP). Vyhláška NBÚ SR [15] umožňovala používať pre administratívny styk PNG obrázky, ktoré sú v súlade so špecifikáciou [31]. Výnos MFSR č. 55/2014 o štandardoch [40] definuje ako jeden zo štandardov pre prijímanie a čítanie podpísaných elektronických dokumentov aj formát grafických súborov Portable Network Graphics (.png).

# 5. Architektúra PNG Pluginu

V rámci tejto kapitoly je popísaná architektúra PNG 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].

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

PNG 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 PNG Plugin činnosti potrebné pre spracovanie a vizualizáciu dát typu PNG obrázok pred spustením procedúry vytvorenia ZEP/KEP a vytvorenie príslušných XML štruktúr pre formát podpisu v súlade s profilmi XAdES_ZEP/XAdES_ZEPbp.

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

- integračné Java API – umožňuje volanie služieb komponentu PNG 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 PNG Plugin GUI rozhranie, v rámci ktorého je realizované:

- zobrazenie obsahu podpisovaných PNG obrázkov,
- zobrazenie obsahu verifikačných údajov pre podpisované PNG obrázky,
- zobrazenie ostatných relevantných parametrov ZEP/KEP (napr. použité algoritmy pre digitálne odtlačky a ich hodnoty)

pred spustením procedúry vytvorenia ZEP/KEP.

Komponent PNG 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 [30].

Komponent PNG 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 PNG 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 PNG Plugin pre D.Signer/XAdES Java implementované nasledujúce dôveryhodné komponenty:

- SDP – Signer's Document Presentation Component – zabezpečuje zobrazenie podpisovaných PNG obrázkov podpisovateľovi,
- SAV – Signature Attributes Viewer – zabezpečuje zobrazenie príslušných verifikačných údajov pre podpisované PNG obrázky a ďalších atribútov vytváraného ZEP/KEP podpisovateľovi,
- DTBSF – Data To Be Signed Formatter – zabezpečuje kontrolu vstupných dát, či naozaj predstavujú PNG obrázok, sformátovanie a tranformáciu verifikačných údajov vstupného PNG obrázku do kanonickej formy a vytvorenie štruktúry DTBSF,
- SIC – Signer Interaction Component – GUI rozhranie pre vizualizáciu PNG obrázkov a ďalších atribútov ZEP/KEP a pre interakciu medzi podpisovateľom a aplikáciou D.Signer/XAdES Java.

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

- SDOC – Signed Data Object Composer – modul pre spracovanie a transformáciu PNG obrázku do base64 a vytvorenie príslušných XML fragmentov výsledného ZEP/KEP vo formáte XAdES_ZEP, resp. XAdES_ZEPbp zo vstupného PNG obrázku 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 [30].

# 6. Špecifikácia funkčnosti

## 6.1. Popis činnosti

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

- vytvorenie dátového objektu pre PNG obrázok pre aplikáciu D.Signer/XAdES Java,
- spracovanie vstupných dátových objektov typu PNG obrázok, kontrola, či vstupné dáta naozaj predstavujú PNG obrázok, spracovanie verifikačných parametrov a aplikovanie príslušných transformácií pre vytyvorenie DTBSF,
- vizualizácia PNG obrázku a ďalších atribútov vytváraného ZEP/KEP podpisovateľovi,
- spracovanie a transformácia PNG obrázku do base64 a vytvorenie príslušných fragmentov výslednej štruktúry ZEP/KEP podľa profilu XAdES_ZEP a prílohy Formát dátových objektov pre PNG obrázok, 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 [30].

# 7. Špecifikácia API

Komponent PNG Plugin pre D.Signer/XAdES Java tvorí JAR knižnica, ktorá pre klientské aplikácie poskytuje 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 špecifikácie SCA aplikácie D.Signer/XAdES Java [30], kapitoly 8.1.1 a 8.1.2.

PNG Plugin definuje v rámci integračného API triedy pre typ dátového objektu PNG obrázok, ktoré reprezentujú:

- podpisovaný PNG obrázok,
- verifikačné údaje pre daný PNG obrázok.

PNG Plugin pre D.Signer/XAdES Java implementuje abstraktné API IPlugin pre komunikáciu s hlavnou aplikáciou D.Signer/XAdES Java.

V nasledujúcich kapitolách je popísané integračné rozhranie PNG Pluginu.

## 7.1. Integračné API pluginu

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

**Package:**

```
sk.ditec.zep.dsigner.xades.plugins.pngplugin
```

**Triedu:**

```
PngPlugin
```

**Metódy a premenné:**

```
public DataObject createObject
(     String objectId
,     String objectDescription
,     String sourcePngBase64
,     String objectFormatIdentifier
);

public String getErrorMessage();
```

**Package:**

```
sk.ditec.zep.dsigner.xades.bp.plugins.pngplugin
```

**Triedu:**

```
PngBpPlugin
```

### Metódy a premenné:

```
public DataBpObject createObject
(     String objectId
,     String objectDescription
,     String sourcePngBase64
,     String objectFormatIdentifier
);

public String getErrorMessage();
```

### Package:

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

### Triedu:

```
PngPluginApplet
```

### Metódy a premenné:

```
public boolean createObject
(     final Object objectId
,     final Object objectDescription
,     final Object imageB64
,     final Object objectFormatIdentifier
,     final JSObject callback
);

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

### Package:

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

### Triedu:

```
PngBpPluginApplet
```

### Metódy a premenné:

```
public boolean createObject
(     final Object objectId
,     final Object objectDescription
,     final Object sourcePngBase64
,     final Object objectFormatIdentifier
,     final JSObject callback
);

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

### 7.1.1. Popis funkcií a premenných API pluginu

#### 7.1.1.1. createObject (trieda PngPlugin, PngPluginApplet)

Umožňuje vytvoriť dátový objekt typu PNG obrázok 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 PNG obrázku, napr: "Fotografia na pas",

sourcePngBase64 – samotný vstupný PNG obrázok, kódovaný v base64,

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

callback – viď dokument [30], 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 (trieda PngBpPlugin, PngBpPluginApplet)

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

**Parametre:**

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

objectDescription – popis obsahu daného PNG obrázoku, napr: "Fotografia na pas", môže byť null

sourcePngBase64 – samotný vstupný PNG obrázok, kódovaný v base64,

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

callback – viď dokument [30], 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. getErrorMessage

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

**Parametre:**

callback – viď dokument [30], kapitola 8.1.2