DITEC
Data Information Technology & Expert Consulting

Formát dátových objektov pre PNG obrázok v1.0

v rámci profilu XAdES_ZEP

Copyright

Popisné charakteristiky dokumentu

Projekt	GOV_ZEP		A3019_002
Dokument	Formát dátových objektov pre PNG obrázok v1.0		
Podnázov	v rámci profilu XAdES_ZEP		
Ref. číslo	GOV_ZEP.117	Verzia	1

Vypracoval	Galuščák Rastislav, Vittek Róbert	Podpis	Dátum 4.7.2013
Preveril	Major Marián	Podpis	Dátum
Schválil	Dobias Ján	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	Formát dátových objektov pre PNG obrázok v1.0		
Referencia	GOV_ZEP.117	Verzia	1

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. Zoznam použitých skratiek

CA – certifikačná autorita
CMS – Cryptographic Message Syntax
CRL – Certificate Revocation List
HTML – HyperText Markup Language
NBÚ – Národný bezpečnostný úrad
PDF – Portable Document Format
PKI – Public Key Infrastructure
PNG – Portable Network Graphics
RTF – Rich Text Format
SCA – Signature Creation Application
SCVA – Signature Creation and Validation Application
SVA – Signature Validation Application
TIFF – Tagged Image File Format, formát obrazových súborov
TSA – Autorita vydávajúca časové pečiatky
XAdES – XML Advanced Electronic Signatures
XML – eXtended Markup Language
XSD – XML Schema Definition
XSL – eXtensible Stylesheet Language
XSLT– XSL Transformation
ZEP – Zaručený elektronický podpis

2. Referencie

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

[2] ETSI TS 101 733 – CMS Advanced Electronic Signatures (CAdES) v1.6.3

[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 3852 – Cryptographic Message Syntax (CMS)

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

[11] Smernica Európskej únie č. 1999/93/EC z 13. decembra 1999 o rámci spoločenstva pre elektronické podpisy

[12] Zákon č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

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

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

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

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

[17] NBÚ Formáty certifikátov a kvalifikovaných certifikátov, v3.0 (2009-06-30)

[18] NBÚ Formáty zoznamu zrušených kvalifikovaných certifikátov, v1.2 (2005-11-06)

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

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

[21] CWA 14170:2001 E – Security Requirements for Signature Creation Applications

[22] CWA 14171:2001 E – Procedures for Electronic Signature Verification

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

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

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

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

[27] 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

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

3. Úvod

Tento dokument tvorí prílohu dokumentov profilu XAdES_ZEP – formát ZEP na báze XAdES [23][24][26] (ďalej len XAdES_ZEP) a stanovuje požiadavky na štruktúru a obsah dátových objektov pre obrázky v grafickom formáte PNG (ďalej len PNG obrázky). V rámci tohto dokumentu sú zároveň bližšie profilované niektoré elementy špecifikácie formátu elektronického podpisu XAdES_ZEP, týkajúce sa podpisovaných dátových objektov pre PNG obrázky.

Tento dokument stanovuje požiadavky:

- na štruktúru elementu ds:Object a obaľujúceho koreňového elementu pre dátový objekt pre PNG obrázok,
- na štruktúru a obsah dátového objektu pre verifikačné údaje pre PNG obrázok,
- na obsah príslušných xades:DataObjectFormat elementov v rámci xades:SignedDataObjectProperties elementu profilu XAdES_ZEP,
- na obsah príslušných ds:Reference elementov v rámci ds:Manifest, resp. ds:SignedInfo elementov v súlade s príslušným profilom XAdES_ZEP,
- na spracovanie dátových objektov pre PNG obrázky pred vytvorením archívneho podpisu.

V rámci tohto dokumentu sú kvôli prehľadnosti a jednoznačnosti elementy z nasledujúcich namespacov prefixované nasledovne:

- XML Signature:
  xmlns:ds = "http://www.w3.org/2000/09/xmldsig#",
- XAdES, v1.3.2:
  xmlns:xades = "http://uri.etsi.org/01903/v1.3.2#".

4. Dátový objekt pre PNG obrázok

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 [25].

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 elektronický podpis (ZEP). Vyhláška NBÚ SR [16] umožňuje používať pre administratívny styk PNG obrázky, ktoré sú v súlade so špecifikáciou [25].

4.1. Uloženie PNG obrázku v rámci štruktúry podpisu

PNG obrázok predstavuje binárne kódované dáta, preto musí byť pred zahrnutím do XML štruktúry elektronického podpisu vytvorenej podľa profilu XAdES_ZEP zakódovaný do base64.

V rámci profilu XAdES_ZEP musí byť base64 kódovaný PNG obrázok vložený priamo do elementu ds:Object, ktorý musí obsahovať nasledujúce atribúty:

- Id – identifikátor elementu ds:Object,
- Encoding – definuje kódovanie vložených dát, Encoding = "http://www.w3.org/2000/09/xmldsig#base64".

Atribút xmlns nie je potrebný vzhľadom k tomu, že element ds:Object neobsahuje žiadne ďalšie XML elementy.

Príklad:

```
<ds:Object Encoding="http://www.w3.org/2000/09/xmldsig#base64"
Id="objectId">JVBERi0xLjIN.....lRU9GDQ==</ds:Object>
```

4.2. Štruktúra a obsah PNG obrázkov

Podpisované PNG obrázky musia byť v súlade so špecifikáciou PNG [25]. Na štruktúru a obsah samotných dátových objektov pre PNG obrázky inak nie sú v rámci tohto dokumentu stanovené žiadne ďalšie požiadavky okrem tých, ktoré sú uvedené v dokumentoch [23][24] a [26], v kapitole Dátové objekty.

V nasledujúcich kapitolách sú uvedené požiadavky bližšie profilujúce obsah niektorých z požadovaných elementov a atribútov elementov špecifikácie formátu elektronického podpisu XAdES_ZEP pre účely podpisovania dátových objektov pre PNG obrázky.

4.3. Typ dátového objektu

V rámci štruktúry elektronického podpisu podľa profilu XAdES_ZEP je potrebné identifikovať typ podpisovaného dátového objektu pomocou podpísaného elementu xades:DataObjectFormat.

Pre podpisovaný dátový objekt pre PNG obrázok musia mať nasledujúce elementy xades:DataObjectFormat elementu nasledovné hodnoty:

- Description – string, obsahuje popis, ktorý bližšie definuje typ podpísaného dátového objektu (napr. "Fotografia na pas"),
- ObjectIdentifier – URI, obsahuje identifikátor, ktorý bližšie definuje typ podpísaného dátového objektu (napr. URI pre daný typ PNG obrázkov; definuje správca daného typu dokumentov),
- MimeType – string, hodnota "image/png",
- Encoding – definuje kódovanie vložených dát, Encoding = "http://www.w3.org/2000/09/xmldsig#base64".

4.4. Referencia dátového objektu v rámci profilu XAdES_ZEP

Dátový objekt pre PNG obrázok musí byť podľa profilov XAdES_ZEP referencovaný z príslušného ds:Reference elementu v rámci ds:Manifest, resp. ds:SignedInfo elementu. V rámci tohto dokumentu sa požaduje, aby táto referencia dátového objektu pre PNG obrázok obsahovala:

- element ds:Transforms – hodnota musí byť Base64 http://www.w3.org/2000/09/xmldsig#base64.

5. Verifikačné údaje pre PNG obrázok

Verifikačné údaje pre dátové objekty obsahujú špecifické údaje, resp. referencie na špecifické údaje pre daný typ dátových objektov, ktoré:

- nie sú zahrnuté v rámci štandardných podpisovaných atribútov profilu XAdES_ZEP,
- dokumentujú také atribúty dátového objektu, ktoré by mohli ovplyvniť výsledok overenia ZEP na strane overovateľa, napr.:
  - ⇒ spôsob a požadované atribúty vizualizácie podpisovaného dátového objektu,
  - ⇒ dodatočné obmedzenia alebo požiadavky na formát alebo štruktúru podpisovaných dátových objektov,
  - ⇒ aplikačne závislé parametre vytvárania podpisu nad podpisovaným dátovým objektom a pod.

Pre samotný PNG obrázok nie sú v rámci tohto profilu definované žiadne doplňujúce verifikačné údaje. Dátový objekt s verifikačnými údajmi je pre PNG obrázok vytváraný len za účelom identifikácie verzie formátu uloženia PNG obrázku v rámci štruktúry podpisu XAdES_ZEP, a to pomocou elementu ObjectIdentifier, ktorý sa nachádza v rámci elementu xades:DataObjectFormat popisujúceho dátový objekt s verifikačnými údajmi pre príslušný PNG obrázok.

5.1. Štruktúra verifikačných údajov pre PNG obrázky

Dátový objekt s verifikačnými údajmi pre PNG obrázok je podpisovaný dátový objekt, čiže v rámci štruktúry elektronického podpisu musí pre neho existovať ds:Object element, ktorý je referencovaný z ds:Manifest, resp. ds:SignedInfo elementu v súlade s požiadavkami príslušného profilu XAdES_ZEP.

Dátový objekt s verifikačnými údajmi pre PNG obrázok musí obsahovať len prázdny element PNGVerificationData. Štruktúra objektu s verifikačnými údajmi pre PNG obrázok je popísaná v rámci nasledujúcej XML schémy:

```
<?xml version="1.0"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns="http://www.ditec.sk/ep/signature_formats/xades_zep_png/v1.0"
targetNamespace="http://www.ditec.sk/ep/signature_formats/xades_zep_png/
v1.0">

<xsd:element name="PNGVerificationData">
      <xsd:complexType>
            <xsd:attribute name="DataTarget" type="xsd:anyURI"
                  use="required"/>
      </xsd:complexType>
</xsd:element>

</xsd:schema>
```

Prostriedky pre vizualizáciu dátového objektu typu verifikačné údaje pre PNG obrázok musia byť súčasťou príslušného komponentu SCVA aplikácie.

Atribút DataTarget slúži na previazanie dátového objektu s verifikačnými údajmi s príslušným dátovým objektom pre PNG obrázok a obsahuje URI dátového objektu, ku ktorému sa vzťahujú dané verifikačné údaje.

5.2. Typ dátového objektu s verifikačnými údajmi

V rámci štruktúry elektronického podpisu podľa profilu XAdES_ZEP je potrebné identifikovať typ podpisovaného dátového objektu pomocou podpísaného elementu xades:DataObjectFormat.

Pre podpisovaný dátový objekt s verifikačnými údajmi pre PNG obrázok musia mať nasledujúce elementy xades:DataObjectFormat elementu nasledovné hodnoty:

- Description – string, obsahuje popis, ktorý bližšie definuje typ dátového objektu s verifikačnými údajmi pre PNG obrázok (napr. "Verifikačné údaje pre PNG obrázky"),
- ObjectIdentifier – URI identifikátor, ktorý definuje typ dátového objektu s verifikačnými údajmi pre PNG obrázok, hodnota: "http://www.ditec.sk/ep/signature_formats/xades_zep_png/v1.0"
- MimeType – string, hodnota "application/xml".

5.3. Referencia dátového objektu s verifikačnými údajmi

Dátový objekt s verifikačnými údajmi pre PNG obrázok musí byť v súlade s príslušným profilom XAdES_ZEP referencovaný z ds:Reference elementu uloženého v rámci ds:Manifest, resp. ds:SignedInfo elementu. V rámci tohto dokumentu sa požaduje, aby referencia tohto dátového objektu obsahovala:

- element ds:Transforms – hodnota musí byť Canonical XML (omits comments) http://www.w3.org/TR/2001/REC-xml-c14n-20010315.

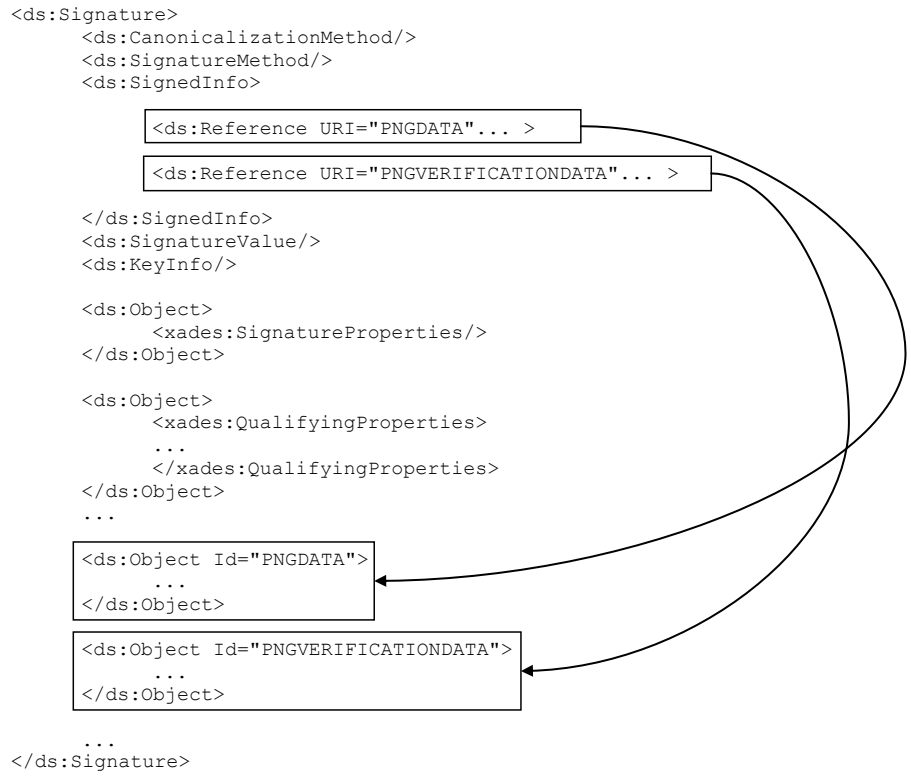
6. Požiadavky pre vytvorenie archívneho podpisu

Podľa požiadaviek profilu XAdES_ZEP musia byť pred vytvorením archívneho podpisu zahrnuté pod ds:Signature element:

- všetky dátové objekty ds:Object, ktoré sú referencované z niektorého z ds:Reference elementu v rámci príslušného ds:Manifest, resp. ds:SignedInfo elementu,
- všetky externé objekty, referencované pomocou ds:Reference elementu z niektorého z podpísaných dátových objektov, teda aj z objektu obsahujúceho verifikačné údaje pre podpísaný dátový objekt.

Pred vytvorením archívneho podpisu musí teda SCVA aplikácia pre každý dátový objekt pre PNG obrázok a pre každý príslušný dátový objekt s verifikačnými údajmi vložiť daný ds:Object ako *child* element do štruktúry ds:Signature.

Takýmto spôsobom budú tieto dáta zahrnuté do výpočtu hodnoty odtlačku pre archívnu časovú pečiatku.



Obr. 1 Zaradenie podpísaného PNG obrázku a verifikačných údajov pre PNG obrázok do štruktúry ds:Signature.