

**Formát datových objektov pre
PDF dokument v1.0
v rámci profilu XAdES_ZEP**

Projekt	GOV_ZEP	A3019_002
Dokument	Formát dátových objektov pre PDF dokument v1.0	
Referencia	GOV_ZEP.53	Verzia 1

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	Formát dátových objektov pre PDF dokument v1.0	
Podnázov	v rámci profilu XAdES_ZEP	
Ref. číslo	GOV_ZEP.53	Verzia 1

Vypracoval	Víttek Róbert	Podpis	Dátum 25. 5. 2009
Preveril	Major Marián	Podpis	Dátum
Schválil	Dobias Ján	Podpis	Dátum

Formulár	Dokument		
Ref. číslo	Fo 11	Dátum poslednej aktualizácie	Dátum 13. 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 PDF dokument v1.0	
Referencia	GOV_ZEP.53	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		

Projekt	GOV_ZEP	A3019_002
Dokument	Formát dátových objektov pre PDF dokument v1.0	
Referencia	GOV_ZEP.53	Verzia 1

Obsah

1.	Zoznam použitých skratiek	5
2.	Referencie	6
3.	Úvod	8
4.	Dátový objekt pre PDF dokument.....	9
4.1.	Uloženie PDF dokumentu v rámci štruktúry podpisu	9
4.2.	Štruktúra a obsah PDF dokumentov.....	10
4.3.	Typ dátového objektu.....	10
4.4.	Referencia dátového objektu v rámci profilu XAdES_ZEP	10
5.	Verifikačné údaje pre PDF dokument.....	12
5.1.	Štruktúra verifikačných údajov pre PDF dokumenty	13
5.2.	Typ dátového objektu s verifikačnými údajmi	14
5.3.	Referencia dátového objektu s verifikačnými údajmi ...	14
6.	Požiadavky pre vytvorenie archívneho podpisu ...	15

Projekt	GOV_ZEP	A3019_002
Dokument	Formát dátových objektov pre PDF dokument v1.0	
Referencia	GOV_ZEP.53	Verzia 1

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

Projekt	GOV_ZEP	A3019_002
Dokument	Formát dátových objektov pre PDF dokument v1.0	
Referencia	GOV_ZEP.53	Verzia 1

2. Referencie

- [1] W3C/IETF Recommendation: "XML-Signature Syntax and Processing" v2002-02-12 (XMLDSIG)
- [2] ETSI TS 101 733 – CMS Advanced Electronic Signatures (CAAdES) v1.6.3
- [3] ETSI TS 101 903 – XML Advanced Electronic Signatures (XAdES) v1.3.2
- [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

Projekt	GOV_ZEP	A3019_002
Dokument	Formát dátových objektov pre PDF dokument v1.0	
Referencia	GOV_ZEP.53	Verzia 1

- [25] PDF Reference, Second Edition, version 1.3, Adobe Incorporated/Addison Wesley, ISBN 0-201-61588-6
- [26] PDF Reference, Third edition, version 1.4, Adobe Incorporated/Addison Wesley, ISBN 0-201-75839-3
- [27] PDF Reference, Sixth Edition, version 1.7, Adobe Incorporated
- [28] Document management – Electronic document file format for long-term preservation – Use of PDF 1.4 (PDF/A-1), ISO 19005-1:2005(E)
- [29] 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)

Projekt	GOV_ZEP	A3019_002
Dokument	Formát dátových objektov pre PDF dokument v1.0	
Referencia	GOV_ZEP.53	Verzia 1

3. Úvod

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

Tento dokument stanovuje požiadavky:

- na štruktúru elementu ds:Object a obalujúceho koreňového elementu pre dátový objekt pre PDF dokument,
- na štruktúru a obsah dátového objektu pre verifikačné údaje pre PDF dokument,
- na obsah príslušných xades:DataObjectFormat elementov v rámci xades:SignedDataObjectProperties elementu profilu XAdES_ZEP,
- na obsah príslušných ds:Reference elementov v rámci ds:Manifest elementov profilu XAdES_ZEP,
- na spracovanie dátových objektov pre PDF dokumenty pred vytvorením archívneho podpisu.

Projekt	GOV_ZEP	A3019_002
Dokument	Formát dátových objektov pre PDF dokument v1.0	
Referencia	GOV_ZEP.53	Verzia 1

4. Dátový objekt pre PDF dokument

Formát PDF bol vytvorený v roku 1993 firmou Adobe Systems pre účely *desktop publishing* a v súčasnosti predstavuje rozšírený a podporovaný štandard pre publikovanie a distribúciu tlačiteľných *device independent a display resolution independent* dokumentov. V súčasnosti je aktuálna verzia 1.7 špecifikácie formátu PDF [27].

Formát PDF 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 PDF dokumenty, ktoré sú v súlade so špecifikáciami PDF, verzie 1.3 a 1.4 [25][26].

Dokumenty vo formáte PDF je možné podľa [21] (kapitola 8.2) zaradiť do skupiny *Presentation Sensitive SDs*, pretože ich sémantika je závislá na presnosti prezentácie dokumentu podpisovateľovi, resp. overovateľovi. Špecifikácia bezpečnostných požiadaviek na SCA [21] stanovuje ďalšie požiadavky na podpisované dokumenty, ktorých cieľom je zabezpečiť jednoznačnosť interpretácie sémantiky podpisovaných dokumentov.

Naplnenie týchto požiadaviek pre PDF dokumenty realizuje špecifikácia PDF/A-1 [28][29], ktorá poskytuje mechanizmus pre takú reprezentáciu elektronických dokumentov vo formáte PDF, ktorá umožňuje zabezpečenie ich vizualizácie a čitateľnosti (teda reprodukovateľnosti) v rámci dlhého časového obdobia a bez ohľadu na použitú technológiu ich reprodukcie.

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

4.1. Uloženie PDF dokumentu v rámci štruktúry podpisu

PDF dokument 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 PDF dokument vložený priamo do elementu ds:Object, ktorý musí obsahovať nasledujúce atribúty:

- Id – identifikátor elementu ds:Object,
- Encoding – definuje kódovanie vložených dát, Encoding = "base64".

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

Projekt	GOV_ZEP	A3019_002
Dokument	Formát dátových objektov pre PDF dokument v1.0	
Referencia	GOV_ZEP.53	Verzia 1

Príklad:

```
<ds:Object Encoding="base64"
Id="objectId">JVBERi0xLjIN.....lRU9GDQ==</ds:Object>
```

4.2. Štruktúra a obsah PDF dokumentov

Podpisované PDF dokumenty musia byť v súlade so špecifikáciou PDF, verzie 1.3 alebo 1.4 [25][26].

Pri vytváraní (zaručeného) elektronického podpisu nad PDF dokumentami je dôležité zabezpečenie jednoznačnosti interpretácie sémantiky podpísaných PDF dokumentov, teda ich presnej a výstižnej vizualizácie a čitateľnosti (reprodukateľnosti) v rámci dlhého časového obdobia (bezpečnostné požiadavky kapitoly 8.2 špecifikácie SCA [21] pre SDP komponent). Tieto bezpečnostné požiadavky je možné naplniť napríklad obmedzením, aby podpísané PDF dokumenty spĺňali požiadavky špecifikácie PDF/A-1 pre požadovanú úroveň súladu – Level A Conformance, resp. Level B Conformance [28][29].

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 PDF dokumenty.

4.3. Typ dátového objektu

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

Pre podpísaný dátový objekt pre PDF dokument musia mať nasledujúce elementy xades:DataObjectFormat elementu nasledovné hodnoty:

- Description – string, obsahuje popis, ktorý bližšie definuje typ podpísaného dátového objektu (napr. "Všeobecné zmluvné podmienky"),
- ObjectIdentifier – URI, obsahuje identifikátor, ktorý bližšie definuje typ podpísaného dátového objektu (napr. URI pre daný typ PDF dokumentov; definuje správca daného typu dokumentov),
- MimeType – string, hodnota "application/pdf",
- Encoding – definuje kódovanie vložených dát, Encoding = "base64".

4.4. Referencia dátového objektu v rámci profilu XAdES_ZEP

Dátový objekt pre PDF dokument musí byť v rámci profilu XAdES_ZEP referencovaný z príslušného ds:Manifest elementu. V rámci tohto dokumentu sa požaduje, aby referencia dátového objektu pre PDF dokument obsahovala:

Projekt	GOV_ZEP	A3019_002
Dokument	Formát dátových objektov pre PDF dokument v1.0	
Referencia	GOV_ZEP.53	Verzia 1

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

Projekt	GOV_ZEP	A3019_002
Dokument	Formát dátových objektov pre PDF dokument v1.0	
Referencia	GOV_ZEP.53	Verzia 1

5. Verifikačné údaje pre PDF dokument

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 podpisované PDF dokumenty môže byť z pohľadu aplikačnej úrovne potrebné zabezpečiť:

- dlhodobú správnu vizualizáciu podpisovaných PDF dokumentov,
- zachovanie logickej štruktúry a čitateľnosti podpisovaných PDF dokumentov v rámci dlhého časového obdobia,
- prístupnosť a zrozumiteľnosť obsahu PDF dokumentov pre fyzicky postihnutých čitateľov.

Technické požiadavky a obmedzenia formátu PDF, ktoré umožňujú, aby príslušný PDF dokument spĺňal vyššie uvedené požiadavky, definuje špecifikácia PDF/A-1 [28][29], kde sú definované dve základné úrovne súladu PDF dokumentov s požiadavkami tejto špecifikácie:

- Level A Conformance – úplný súlad so špecifikáciou PDF/A-1,
- Level B Conformance – súlad so špecifikáciou PDF/A-1 zabezpečujúci dlhodobú reprodukovateľnosť správnej vizualizácie daného PDF dokumentu.

Vyhláška NBÚ SR [16] a dokument NBÚ SR [20] umožňuje používať pre administratívny styk aj také PDF dokumenty, ktoré sú v súlade so špecifikáciami PDF, verzie 1.3 a 1.4 [25][26], ktoré ale nemusia nutne spĺňať požiadavky špecifikácie PDF/A-1 [28][29]. Pre takýto prípad teda verifikačné údaje pre PDF dokument v rámci profilu XAdES_ZEP umožňujú deklarovat' nepožadovanie súladu so špecifikáciou PDF/A-1 [28][29]:

Projekt	GOV_ZEP	A3019_002
Dokument	Formát dátových objektov pre PDF dokument v1.0	
Referencia	GOV_ZEP.53	Verzia 1

- No PDF/A-1 Conformance – nepožadovanie súladu so špecifikáciou PDF/A-1 a zabezpečenie jednoznačnosti interpretácie sémantiky podpísaného PDF dokumentu a reprodukovateľnosti jeho správnej vizualizácie v rámci dlhého časového obdobia inými prostriedkami.

V tomto prípade je potrebné zabezpečiť splnenie požiadaviek kapitoly 8.2 špecifikácie SCA [21] pre SDP komponent na jednoznačnosť interpretácie sémantiky podpísaných PDF dokumentov, a teda ich presnej a výstižnej vizualizácie a čitateľnosti (reprodukovateľnosti) v rámci dlhého časového obdobia inými prostriedkami. Táto špecifikácia nedefinuje nástroje na deklaráciu splnenia týchto požiadaviek inými prostriedkami ako je súlad so špecifikáciou PDF/A-1.

Stanovenie požadovanej úrovne súladu podpísaného PDF dokumentu so špecifikáciou PDF/A-1 je na správcovi komunikačného scenára, v rámci ktorého sa požaduje spracovanie PDF dokumentov podpísaných zaručeným elektronickým podpisom. Zodpovednosť za vytvorenie PDF dokumentu, ktorý spĺňa požadovanú úroveň súladu so špecifikáciou PDF/A-1 je na podpisovateľovi príslušného PDF dokumentu.

5.1. Štruktúra verifikačných údajov pre PDF dokumenty

Dátový objekt s verifikačnými údajmi pre PDF dokument je podpísaný dátový objekt, čiže v rámci štruktúry elektronického podpisu musí pre neho existovať ds:Manifest element, ktorý je referencovaný z ds:SignedInfo podľa požiadaviek profilu XAdES_ZEP.

Dátový objekt s verifikačnými údajmi pre PDF dokument musí obsahovať:

- element s informáciou o požadovanej úrovni súladu so špecifikáciou PDF/A-1.

Štruktúra objektu s verifikačnými údajmi pre PDF dokument 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_pdf/v1.0"
targetNamespace="http://www.ditec.sk/ep/signature_formats/xades_zep_pdf/
v1.0">

<xsd:element name="PDFVerificationData">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element ref = "PDFAConformanceLevel"/>
    </xsd:sequence>
    <xsd:attribute name="DataTarget" type="xsd:anyURI"
      use="required"/>
  </xsd:complexType>
</xsd:element>

<xsd:element name = "PDFAConformanceLevel">
```

Verifikačné údaje pre PDF dokument

-13/15-

Projekt	GOV_ZEP	A3019_002
Dokument	Formát dátových objektov pre PDF dokument v1.0	
Referencia	GOV_ZEP.53	Verzia 1

```

<xsd:simpleType>
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="No_PDF/A-1_Conformance" />
    <xsd:enumeration value="PDF/A-1_LevelAConformance" />
    <xsd:enumeration value="PDF/A-1_LevelBConformance" />
  </xsd:restriction>
</xsd:simpleType>
</xsd:element>

</xsd:schema>

```

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

Atribút DataTarget slúži na previazanie dátového objektu s verifikačnými údajmi s príslušným dátovým objektom pre PDF dokument 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 PDF dokument musia mať nasledujúce elementy xades:DataObjectFormat elementu nasledovné hodnoty:

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

5.3. Referencia dátového objektu s verifikačnými údajmi

Dátový objekt s verifikačnými údajmi pre PDF dokument musí byť v rámci profilu XAdES_ZEP referencovaný z príslušného ds:Manifest elementu. V rámci tohto dokumentu sa požaduje, aby referencia takého dátového objektu obsahovala:

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

Projekt	GOV_ZEP	A3019_002
Dokument	Formát dátových objektov pre PDF dokument v1.0	
Referencia	GOV_ZEP.53	Verzia 1

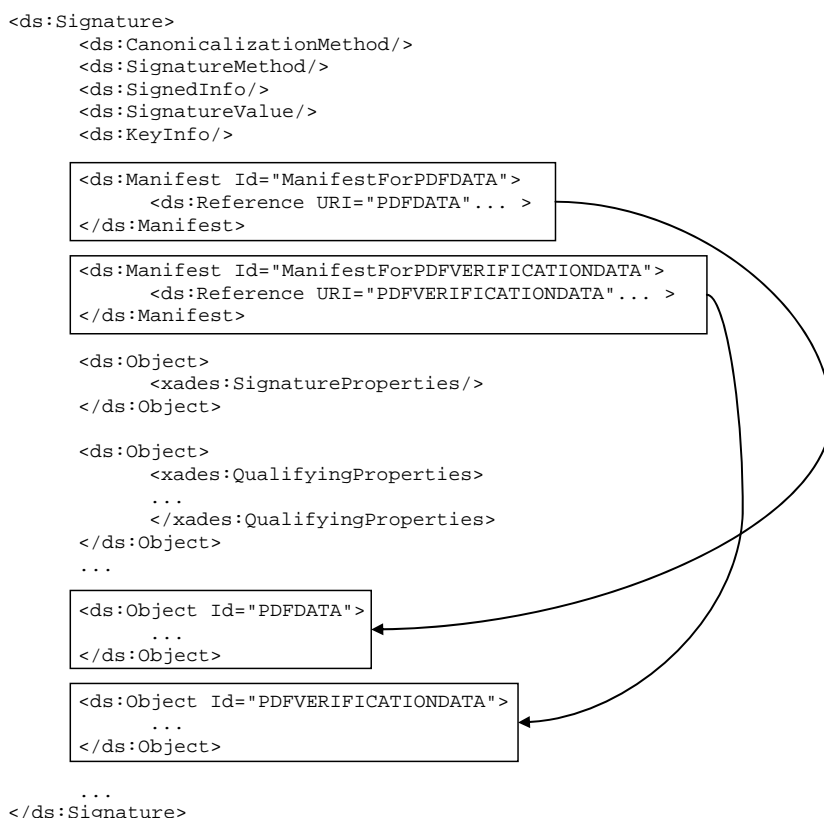
6. Požiadavky pre vytvorenie archívneho podpisu

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:Manifest elementov v rámci ds:Signature,
- 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 PDF dokument 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 PDF dokumentu a verifikačných údajov pre PDF dokument do štruktúry ds:Signature.