



Dokumentácia funkčnosti

Centrálnej elektronickej podateľne

Dátum zverejnenia: 29. 9. 2017

Verzia dokumentu: 1.8

Dátum aktualizácie: 11. 01. 2018

Zoznam zmien:

Dátum vydania	Verzia	Popis zmien
29.9.2017	1.0	Prvá verzia
9.10.2017	1.1	Doplnené pravidlá pre MessageContainer
6.11.2017	1.2	Doplnené pravidlá pre XMLDataContainer
27.11.2017	1.3	Doplnenie 4. kapitoly: Validácia podpísaných dátových objektov a 5. kapitoly: Formáty podpisov
29.11.2017	1.4	Doplnenie podporovaných formátov podpisov v CEP do 5. kapitoly
6.12.2017	1.5	Doplnenie zoznamu formátov dátových objektov do 5. kapitoly
11.12.2017	1.6	Doplnenie informácie o atribútoch Identifier a Version v 3. kapitole
22.12.2017	1.7	Doplnenie informácie o PAdES v kapitole 4
11.1.2018	1.8	Doplnenie 2. kapitoly vo formáte xml a kapitoly 4 vo formáte ZEPf

Popis: Tento dokument obsahuje pravidlá vyhodnocovania autorizácie v Centrálnej elektronickej podateľni.

Vypracovalo: oddelenie administrácie aplikácií, Národná agentúra pre sieťové a elektronicke služby



Obsah

1. MessageContainer – vyžadované hodnoty pre podpísané objekty.....	3
2. XAdES_ZEP - vyžadované hodnoty v elementoch ObjectIdentifier, Description a XMLVerificationDataReferences	4
3. XMLDataContainer - vyžadované tvary URI	5
4. Validácia podpísaných dátových objektov	6
5. Formáty podpisov	8
5.1 Vytváranie podpisov	8
5.2 Overovanie podpisov	8



1. MessageContainer – vyžadované hodnoty pre podpísané objekty

Účinnosť požiadavky: od začiatku prevádzky v roku 2013

Ak je v elemente Object hodnota atribútu IsSigned="true", potom hodnota atribútu MimeType musí byť niektorá z nasledovných hodnôt, inak je výsledkom overenia autorizácie chyba:

Formát	Prípustná hodnota v atribúte MimeType	Používaná prípona súboru v atribúte Name
XAdES_ZEP	application/x-xades_zep application/zepx	.xzep .zepx
XAdES_ZEP Formát zloženého elektronického podpisu	application/x-xades_zep_data_signatures	.xzep .zepx
ZEPf	application/x-zipzepf application/zep	.zep
PAdES	application/pdf	.pdf
ASiC	application/x-asic (od r. 2016) application/vnd.etsi.asic-s+zip (od 19. 10. 2017) application/vnd.etsi.asic-e+zip (od 19. 10. 2017)	.asics, .asice, .scs, .sce

Ak je v elemente Object hodnota atribútu IsSigned="false" alebo atribút nie je použitý, objekt je spracúvaný ako nepodpísaný a autorizácia sa nevyhodnocuje.

V elemente Object musí byť v atribúte Name použitá prípona súboru príslušná k danému formátu súboru, a to v zmysle § 18 písm. f) Výnosu o štandardoch pre ISVS č. 55/2014 Z. z.

2. XAdES_ZEP - vyžadované hodnoty v elementoch ObjectIdentifier, Description a XMLVerificationDataReferences

Účinnosť požiadavky: od začiatku prevádzky v roku 2013

Evidencia typov dátových objektov

Ak nasledovné hodnoty nie sú uvedené v XAdES_ZEP, v Centrálnej elektronickej podateľni je autorizácia vždy vyhodnotená ako neplatná:

Pri formáte PDF

v elemente Identifier v ObjectIdentifier je vyžadovaná hodnota:

"http://schemas.gov.sk/attachment/pdf"

a v elemente Description je vyžadovaná hodnota: "PDF".

Pri formáte PNG

v elemente Identifier v ObjectIdentifier je vyžadovaná hodnota:

"http://schemas.gov.sk/attachment/png"

a v elemente Description je vyžadovaná hodnota: "PNG".

Pri formáte TXT

v elemente Identifier v ObjectIdentifier je vyžadovaná hodnota:

"http://schemas.gov.sk/attachment/txt"

a v elemente Description je vyžadovaná hodnota: "TXT".

Pri formáte XML

- v elemente Identifier v ObjectIdentifier je vyžadovaná hodnota v tvare : "targetNamespace" zo súboru schema.xsd evidovaného v module elektronických formulárov doplnená o reťazec "/form.xsd", t. j. výsledná hodnota je najčastejšie nasledovná:
"http://schemas.gov.sk/form/identifikator-e-formulara/verzia/form.xsd",
- v elemente Description je vyžadovaný názov e-formulára evidovaný v module elektronických formulárov,
- v elemente VisualTransformReference v XMLVerificationDataReferences je vyžadovaná hodnota v tvare: "targetNamespace" zo súboru schema.xsd evidovaného v module elektronických formulárov doplnená o reťazec "/form.xslt", t. j. výsledná

hodnota je najčastejšie nasledovná:

"http://schemas.gov.sk/form/identifikator-e-formulara/verzia/form.xslt"

- a v elemente SchemaReference v XMLVerificationDataReferences je vyžadovaná rovnaká hodnota ako v elemente Identifier: targetNamespace" zo súboru schema.xsd evidovaného v module elektronických formulárov doplnená o reťazec "/form.xsd", t. j. výsledná hodnota je najčastejšie nasledovná:
"http://schemas.gov.sk/form/identifikator-e-formulara/verzia/form.xsd" ,
- pričom v týchto hodnotách sa ako „identifikator-e-formulara“ uvádza identifikátor evidovaný v module elektronických formulárov (resp. príslušná časť identifikátora, ak je identifikátor v tvare URI) a ako „verzia“ sa uvádza príslušná verzia e-formulára.

Pre formát XML je možné pravidlo zapísať aj nasledovne:

xsdNSUri (namespaceUri) = "targetNamespace" zo súboru schema.xsd
SchemaReference (xsdReference) = ObjectIdentifier = xsdNSUri + „/form.xsd“
VisualTransformReference (xsltReference) = xsdNSUri + „/form.xslt“
Description (objectDescription) = „dc:title“ z metaúdajov zo súboru meta.xml

V zátvorkách sú názvy parametrov metód CreateObject a CreateObject2 XML Pluginu pri volaní D.Signer, ktoré korešpondujú s položkami vo vytvorenom XAdES_ZEP.

3. XMLDataContainer - vyžadované tvary URI

Účinnosť požiadavky: od roku 2016

Formát XMLDataContainer sa v Centrálnnej elektronickej podateľni vytvára vždy pri použití formátu ASiC-XAdES pre podpisovanie údajov vyplnených podľa elektronickeho formulára.

Pre referencie použitej prezentačnej schémy a XSD schémy v XMLDataContainer sú v Centrálnnej elektronickej podateľni vyžadované nasledovné hodnoty:

- v elemente UsedPresentationSchemaReference je vyžadovaná hodnota v tvare:
"http://schemas.gov.sk/form/identifikator-e-formulara/verzia/form.xslt"
- v elemente UsedXSDReference je vyžadovaná hodnota v tvare:
"http://schemas.gov.sk/form/identifikator-e-formulara/verzia/form.xsd"

Podpora pre hodnoty v tvare predpísanom Výnosom o štandardoch pre IS VS č. [55/2014 Z. z.](#) sa pripravuje.

Ako „identifikator-e-formulara“ sa uvádza identifikátor evidovaný v module elektronických formulárov (resp. príslušná časť identifikátora, ak je identifikátor v tvare URI) a ako „verzia“ sa uvádza príslušná verzia e-formulára.

V atribúte Identifier sa používa hodnota z elementu "dc:identifier" zo súboru meta.xml z príslušného elektronického formulára.

V atribúte Version sa používa hodnota z elementu "version" zo súboru meta.xml z príslušného elektronického formulára.

4. Validácia podpísaných dátových objektov

Formát ZEPf

Pri overovaní platnosti podpisu vo formáte ZEPf je vyhodnocované, či podpísaný elektronický dokument je v jednom z nasledovných formátov súborov a používa príslušný mimetype, pričom je vykonávaná automatická validácia súboru voči príslušnej špecifikácii.

Ak podpísaný dokument nie je v jednom z nasledovných formátov, alebo je vyhodnotený ako nevalidný, alebo nie je použitý uvedený mimetype, autorizácia je vyhodnotená ako neplatná s chybou č. 110:

- Plain Text Format (.txt) - mimetype: text/plain
- Portable Document Format (.pdf) vo verzii 1.3 alebo 1.4 - mimetype: application/pdf
- Extensible Markup Language (.xml) - mimetype: text/xml
- Tagged Image File Format (.tiff, .tif) - mimetype: image/tiff
- Portable Network Graphics (.png) - mimetype: image/png
- XMLDataContainer (.xml) - mimetype: application/vnd.gov.sk.xmldatacontainer+xml
- Rich Text Format (.rtf) - mimetype: text/rtf (pridaný od 9. novembra 2017)
- OpenDocument format (.odt) - mimetype: application/vnd.oasis.opendocument.text (pridaný od 9. januára 2018)

Formát XAdES_ZEP

Pri overovaní platnosti podpisu vo formáte XAdES_ZEP je vyhodnocované, či podpísaný elektronický dokument je v jednom z nasledovných formátov súborov a používa príslušný mimetype, pričom je vykonávaná automatická validácia súboru voči príslušnej špecifikácii.

Ak podpísaný dokument nie je v jednom z nasledovných formátov, alebo je vyhodnotený ako nevalidný, alebo ak nie je použitý uvedený mimetype, autorizácia je vyhodnotená ako neplatná:

- Plain Text Format (.txt) - mimetype: text/plain
- Portable Document Format (.pdf) - mimetype: application/pdf
- Extensible Markup Language (.xml) - mimetype: text/xml
- Portable Network Graphics (.png) - mimetype: image/png
- XMLDataContainer (.xml) -
mimetype: application/vnd.gov.sk.xmldatacontainer+xml

Formát ASiC

Pri overovaní platnosti podpisu vo formáte ASiC je validácia podpísaných dátových objektov oddelená od overenia platnosti podpisu, a preto nemá vplyv na výsledok overenia autorizácie.

Pri jednotlivých formátoch podpísaných elektronických dokumentov v ASiC je automaticky vykonávaná ich validácia v informatívnej forme.

Validácie

- PDF
Pre validáciu formátu PDF je používaný nástroj PDFNet SDK od firmy PDFTron. Nahradenie tohto nástroja referenčným validátorom VeraPDF sa pripravuje.
- PNG a TIFF
Pre validáciu formátu PNG a TIFF je používaný konštruktor .NET triedy System.Drawing.Bitmap.
- TXT, XML, XMLDataContainer

Podrobná špecifikácia validácie formátov TXT, XML, XMLDataContainer je uvedená v špecifikácii komponentu [DataValidator](#).

Formát PAdES

Pri overovaní platnosti podpisu vo formáte PAdES sa validácia dátových objektov nevykonáva.

5. Formáty podpisov

5.1 Vytváranie podpisov

Centrálne elektronická podateľňa umožňuje integrovaným subjektom vytvárať cez webové služby nasledovné formáty podpisov a podpisových kontajnerov:

- XAdES_ZEP vo verziách 1.0, 1.1 a 2.0 (.xzep)
- ZEPf s CAdES_ZEP vo verziách 1.0 a 2.0 (.zep)
- ASiC-E s XAdES podľa profilu XAdES_ZEPbp (.asice)
- ASiC-E s CAdES (.asice) - iba v prípade podpisovania už podpísaného dokumentu v ASiC-E CAdES
- PAdES (.pdf)

Centrálne elektronická podateľňa umožňuje podpísať len nasledovné formáty dátových objektov, a to len v prípade, ak tieto formáty úspešne prejdú validáciou cez validačné nástroje uvedené v časti „Validácie“:

- Plain Text Format (.txt) - mimetype: text/plain
- Portable Document Format (.pdf) len vo verzii PDF/A-1a - mimetype: application/pdf (možnosť podpisovania iných verzií PDF sa pripravuje)
- Extensible Markup Language (.xml) - mimetype: text/xml
- Portable Network Graphics (.png) - mimetype: image/png
- XMLDataContainer (.xml) - mimetype: application/vnd.gov.sk.xmldatacontainer+xml

Centrálne elektronická podateľňa ponúka možnosť konverzie podpísaného PDF súboru do PDF/A-1a. V prípade ak takto konvertovaný súbor obsahoval podpis PAdES, môže mať takáto konverzia za následok narušenie tohto podpisu a teda jeho neplatnosť.

Kvalifikované elektronické pečate na elektronických doručenkách vytváraných v Centrálnej elektronickej podateľni sú vo formáte XAdES_ZEP 1.1. Prechod na formát ASiC-E XAdES sa pripravuje.

5.2 Overovanie podpisov

Pri overovaní podpisov sú v centrálnej elektronickej podateľni podporované nasledovné formáty podpisov:

1. pre XAdES_ZEP v1.0, 1.1 a 2.0 - XadesZepEpes, XadesZepT, XadesZepA, XadesZepX1
2. pre XAdES_ZEPbp - XadesBPLlevelB, XadesBPLlevelT, XadesBPLlevelLTA



3. pre CAdES_ZEP v1.0 a v2.0 - CAdES_BES, CAdES_EPES, CAdES_T, CAdES_XL, CAdES_A
4. pre CAdES baseline profile - CAdES_BpB, CAdES_BpT, CAdES_BpLTA
5. pre PAdES - PAdES-BES, PAdES-EPES, PAdES-T, PAdES-A.