Dokumentácia funkčnosti Centrálnej elektronickej podateľne

Dátum zverejnenia: 29. 9. 2017

Verzia dokumentu: 1.12

Dátum aktualizácie: 4. 6. 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
5.2.2018	1.9	Úprava elementov v 3. kapitole
27.3.2018	1.10	Formálne upresnenia v 1. kapitole – oddelenie ASiC-S od ASiC-E. Doplnenie prehľadu formátov podporovaných pri spoločnej autorizácii a viacnásobnej autorizácii a informácií o využívaní OCSP pri overovaní v 5. kapitole
17.4.2018	1.11	Doplnené informácie o predvolenom vypnutí validácie PDF súborov voči PDF/A-1a - v kapitolách 4 a 5.2..
4.6.2018	1.12	Požiadavky súladu formátu objektu s MimeType v kapitole 1, informácie o používaní Name v kapitole 1, informácie o validáciách údajov e-formulárov v kapitole 4, informácie o podporovaných formátoch podľa eIDAS v kapitole 5.1.

Popis: Tento dokument obsahuje prehľad podporovaných formátov a pravidlá vyhodnocovania autorizácie v Centrálnej elektronickej podateľni.

Vypracovalo: oddelenie administrácie aplikácií, Národná agentúra pre sieťové a elektronické 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 6
4. Validácia podpísaných dátových objektov 7
5. Formáty podpisov 9
5.1 Overovanie podpisov 9
5.1.1 Overovanie podpisov vo vnútri podpísaných dátových objektov 10
5.1.2 Používanie OCSP a CRL pri overovaní podpisov 10
5.2 Vytváranie podpisov 11
5.2.1 Formáty podpisovaných dátových objektov 11
5.2.2 Viacnásobná autorizácia rovnakého obsahu rovnakým formátom podpisu 12
5.2.3 Spoločná autorizácia viacerých elektronických dokumentov rovnakým formátom podpisu 13
5.2.4 Spájanie viacerých autorizácií rôznych formátov do jedného súboru ... 14

1. MessageContainer – vyžadované hodnoty pre podpísané objekty

Účinnosť požiadavky: od začiatku prevádzky v roku 2013

Ak je v MessageContainer v elemente Object hodnota atribútu IsSigned="true", potom hodnota atribútu MimeType musí byť niektorá z nasledovných hodnôt a v súlade s príslušným podporovaným formátom objektu, inak je výsledkom overenia autorizácie „Neoveriteľná":

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-S	application/vnd.etsi.asic-s+zip (od 19. 10. 2017) application/x-asic * (od r. 2016, vytváraný do 18. 10. 2017)	.asics, .scs
ASiC-E	application/vnd.etsi.asic-e+zip (od 19. 10. 2017) application/x-asic * (od r. 2016, vytváraný do 18. 10. 2017)	.asice, .sce

* Hodnotu „application/x-asic" centrálna elektronická podateľňa nevytvára od 19. 10. 2017, naďalej ju však podporuje pri spracúvaní podpísaných objektov. Táto hodnota nie je v súlade so špecifikáciou formátu ASiC a Výnosom o štandardoch pre IS VS č. 55/2014 Z.z., vznikla

z historických dôvodov v roku 2013 pre potreby portálu slovensko.sk a neumožňuje odlišovať ASiC-E od ASiC-S.

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

Ak hodnota atribútu MimeType nie je v súlade s príslušným formátom podpísaného objektu a hodnota atribútu IsSigned="true", elektronická správa sa v CEP spracuje a zaeviduje, avšak výsledkom overenia autorizácie je *„Neoveriteľná" - „Nie je možné overiť autorizáciu, nepodarilo sa získať potrebné údaje"*, pričom odosielateľ nie je o tejto skutočnosti automaticky informovaný. (To platí aj pre hodnoty MimeType nad rámec hodnôt uvedených v tabuľke, napr. aj pre hodnotu „application/octet-stream".) Od 17. mája 2018 to platí aj pre hodnoty MimeType „application/x-xades_zep" a „application/x-xades_zep_data_signatures", pričom do 16. mája 2018 sa v prípade nesúladu týchto hodnôt MimeType s formátom podpísaného objektu nepodarilo správu spracovať a odosielateľ bol informovaný o nemožnosti jej spracovania s chybou *„2200001"* pričom v elektronickej schránke môže byť doplnená informáciou: *„Podateľni sa nepodarilo správu spracovať"*. Nesúlad MimeType s formátom má za následok aj chybu pri ukladaní podpísaného obsahu.

Požiadavky nevalidované v CEP: 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. V atribúte Name sa uvádza názov súboru, pod ktorým sa súbor ukladá v elektronickej schránke, pričom do 16. mája 2018 nesmel obsahovať znaky, ktoré nie sú prípustné pre názov súboru vo filesystéme NTFS, a to ani vo forme tzv. „character numeric reference" alebo „character entity reference". V opačnom prípade sa elektronická správa neuložila do elektronickej schránky. Od 17. mája 2018 sa správy uložia do elektronickej schránky, avšak špeciálne znaky sa v atribúte Name dôrazne neodporúča používať, a to aj v zmysle Metodického pokynu k §18 Výnosu o štandardoch.

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 (xslReference) = 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 Centrálnej elektronickej podateľni vytvára vždy pri použití formátu ASiC-XAdES pre podpisovanie údajov vyplnených podľa elektronického formulára. Formát XMLDataContainer je povinný formát pre podpisovanie XML údajov v zmysle § 57a, § 57c a prílohy č. 11 Výnosu č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy.

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

- v elemente UsedPresentationSchemaReference 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"

- v elemente UsedXSDReference 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"

Použitie inej ako uvedenej hodnoty v XMLDataContainer nemá vplyv na vyhodnotenie platnosti autorizácie, nakoľko validácia podpísaných dátových objektov je oddelená od overenia platnosti podpisu resp. pečate. Nesúlad použitých hodnôt bude uvedený vo výsledku overenia podpisov len v informatívnej forme.

Podpora pre hodnoty URI v tvare predpísanom v §46 a prílohe č. 11 Výnosu 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 v kontajneri 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) - mimetype: application/pdf -všetky verzie (od 19. apríla 2018)
    - Portable Document Format (.pdf) len vo verzii 1.3 alebo 1.4 (od 1. júla 2017 do 18. apríla 2018)
    - Portable Document Format (.pdf) len vo verzii PDF/A-1a (od júla 2016 do 30. júna 2017)
- 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 (v prípade XML údajov e-formulára sa validuje aj voči XSD schéme z e-formulára), 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 -všetky verzie (od 1. júla 2017)
    - Portable Document Format (.pdf) len vo verzii PDF/A-1a (od júla 2016 do 30. júna 2017)
- Extensible Markup Language (.xml) - mimetype: text/xml
- Portable Network Graphics (.png) - mimetype: image/png
- XMLDataContainer (.xml) - mimetype: application/vnd.gov.sk.xmldatacontainer+xml

Formát PAdES

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

Formát ASiC

Pri overovaní platnosti podpisu v podpisovom kontajneri 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.

Nepodpísané dátové objekty

Ak ide o nepodpísaný dátový objekt v MessageContainer v class="FORM", ktorého mimetype je application/x-eform-xml, vykonáva sa jeho validácia voči XSD schéme identifikovanej na základe deklarácie menného priestoru z atribútu „xmlns".
Ak je objekt nevalidný voči XSD, podanie sa odmietne s chybou -230 („Hlavný nepodpísaný dokument nesedí voči schéme.") a doručenka sa nevystaví.
Ak nie je XSD v CEP k dispozícii, podanie sa odmietne s chybou -222 („Neznámy alebo neplatný typ objektu.") a doručenka sa nevystaví.

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.
  Pre XML údaje vyplnené podľa e-formulára sa vykonáva aj validácia voči XSD schéme.

5. Formáty podpisov

5.1 Overovanie podpisov

Pri overovaní platnosti 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 - XadesBPLevelB, XadesBPLevelT, XadesBPLevelLTA
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.

Pri overovaní platnosti podpisov je vykonávaná validácia podpísaných dátových objektov podľa kapitoly č. 4, ktorá pri niektorých formátoch podpisov priamo ovplyvňuje platnosť podpisov.

V súlade s Nariadením EP a Rady EÚ 910/2014 a Vykonávacím rozhodnutím Komisie (EÚ) č. 2015/1506 centrálna elektronická podateľňa podporuje povinné základné profily formátov:

- ASiC Baseline profile - ETSI TS 103 174 v2.2.1,
- XAdES Baseline profile - ETSI TS 103 171 v2.1.1,
- CAdES Baseline profile - ETSI TS 103 173 v2.2.1,
- PAdES Baseline profile - ETSI TS 103 172 v2.2.2.

Iné verzie uvedených formátov, ktoré obsahujú vlastnosti nad rámec týchto technických špecifikácií, nie sú v centrálnej elektronickej podateľni plne

podporované a výsledkom overenia podpisov v takýchto formátoch je chyba. Ich podpora v CEP sa v súčasnosti zvažuje.

Napríklad podpis ASiC-E XAdES vytvorený v softvéri Digital Signature Service nie je v centrálnej elektronickej podateľni podporovaný, nakoľko obsahuje element „SigningCertificateV2“, ktorý nie je súčasťou špecifikácie ETSI TS 103 171 resp. ETSI TS 103 174. Tento element je až súčasťou novej normy ETSI EN 319 132 resp. ETSI EN 319 162, ktoré však nie sú vyžadované Vykonávacím rozhodnutím Komisie.

5.1.1 Overovanie podpisov vo vnútri podpísaných dátových objektov

Centrálna elektronická podateľňa neumožňuje automatizovane overovať podpisy nachádzajúce sa vo vnútri jednotlivých externe podpísaných dátových objektov.

To znamená, že ak napríklad podpisový kontajner ASiC-E XAdES obsahuje autorizáciu elektronického dokumentu, ktorý je vo formáte PDF, pričom tento PDF dokument zároveň vo svojom vnútri obsahuje podpis PAdES, vo výsledku overenia podpisov sa v centrálnej elektronickej podateľni vyhodnotí len platnosť podpisu XAdES. Rovnako to platí pre kontajner ASiC vnorený v inom kontajneri ASiC. Podpisy nachádzajúce sa vo vnútri externe podpísaných dátových objektov sa teda automaticky neoverujú a pre ich overenie je možné samostatne zavolať službu overenia z informačného systému integrovaného s centrálnou elektronickou podateľňou. Podpora pre automatizované overovanie podpisov z vnútra externe podpísaných súborov v centrálnej elektronickej podateľni sa zatiaľ len pripravuje vzhľadom na novelu Výnosu o štandardoch pre IS VS.

5.1.2 Používanie OCSP a CRL pri overovaní podpisov

Centrálna elektronická podateľňa pri úplnom overení podpisov pri zaevidovaní podania ako aj pri informatívnom overení podpisov v overovacích komponentoch používa pre overovanie platnosti certifikátov informácie z CRL alebo OCSP nasledovne:

- XAdES_ZEP v1.0 a 1.1 sa overuje iba pomocou CRL
- XAdES_ZEP v2.0 sa overuje pomocou CRL alebo OCSP
- XAdES_ZEPbp sa overuje pomocou CRL alebo OCSP
- CAdES_ZEP sa overuje pomocou CRL alebo OCSP
- CAdES_ZEP baseline profile sa overuje pomocou CRL alebo OCSP
- PAdES sa overuje pomocou CRL alebo OCSP

V prípade ak je možné platnosť certifikátu overiť na základe CRL aj OCSP, centrálna elektronická podateľňa posiela do overovacích komponentov

zodpovedajúce CRL aj OCSP a overovacie komponenty si z nich vyberú údaje potrebné na overenie.

5.1.3 Overovanie zdokonalených a kvalifikovaných podpisov

Centrálna elektronická podateľňa vo výsledku overenia autorizácie uvádza informáciu o jej platnosti bez ohľadu na to, či ide o kvalifikovaný elektronický podpis / pečať alebo iba o zdokonalený elektronický podpis / pečať použitím kvalifikovaného certifikátu. Pokiaľ však kvalifikovaný certifikát neobsahuje položku deklarujúcu uloženie privátneho kľúča na bezpečnom zariadení - QcSSCD/QcQSCD (OID 0.4.0.1862.1.4) – výsledok autorizácie je z hľadiska legislatívy považovaný iba za zdokonalený elektronický podpis / pečať.
Do 18. 4. 2018 sa vo výsledku úplného overenia podpisov zobrazoval v položke TypPodpisu príznak „SkSysQCRules“ aj v prípade, ak certifikát použitý pri pečatení neobsahoval príznak QcSSCD/QcQSCD.
Od 19. 4. 2018 sa vo výsledku úplného overenia tento príznak nevyskytuje, čím je indikované, že nejde o kvalifikovanú elektronickú pečať.

5.2 Vytváranie podpisov

Centrálna 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) (od júla 2016)
- ASiC-E s CAdES (.asice) - iba v prípade podpisovania už podpísaného dokumentu v ASiC-E CAdES, ak nejde o XML dokument (od júla 2016)
- PAdES (.pdf)

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

Centrálna elektronická podateľňa v aktuálnej konfigurácii umožňuje vytvárať aj zdokonalené elektronické pečate použitím kvalifikovaného certifikátu, ktorý neobsahuje príznak QcSSCD/QcQSCD (OID 0.4.0.1862.1.4) (podľa T1.I,III(j) Schémy dohľadu NBÚ), okrem zdokonalených pečatí vo formáte PAdES, ktoré bolo možné vytvárať len do decembra 2017.

5.2.1 Formáty podpisovaných dátových objektov a ich validácie

Centrálna 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 1.3 alebo 1.4 - mimetype: application/pdf (možnosť podpisovania iných verzií PDF sa pripravuje)
- Extensible Markup Language (.xml) - mimetype: text/xml (nepodporovaný pri ASiC-CAdES)
- Portable Network Graphics (.png) - mimetype: image/png
- XMLDataContainer (.xml) - mimetype: application/vnd.gov.sk.xmldatacontainer+xml (nepodporovaný pri ASiC-CAdES)

Súbory vo formáte PDF sú pred podpísaním validované, konkrétne či ide o PDF súbor a či obsahuje deklaráciu, že ide o PDF 1.3 alebo 1.4. Iné validácie nie sú predvolene vykonávané. Možnosť voliteľnej validácie pri podpisovaní súborov vo formáte PDF voči PDF/A-1a je dostupná od 19. apríla 2018. Do 18. apríla 2018 bola validácia voči PDF/A-1a vždy zapnutá bez možnosti voľby.

Centrálna elektronická podateľňa ponúka integrovaným subjektom službu konverzie podpisovaného PDF súboru do formátu PDF/A-1a. Pri podpisovaní cez klientske aplikácie na slovensko.sk je táto konverzia vykonávaná automaticky. V prípade, ak súbor obsahoval podpis PAdES, môže mať takáto konverzia za následok narušenie tohto podpisu a teda jeho neplatnosť.

5.2.2 Viacnásobná autorizácia rovnakého obsahu rovnakým formátom podpisu

Viacnásobná autorizácia umožňuje opakované vykonanie autorizácie nad identickými dátovými objektami. Používa sa napríklad v prípade autorizácie rovnakého obsahu rôznymi osobami.

Formát podpisu (všetky autorizácie používajú rovnaký formát)	Možnosť viacnásobnej autorizácie kvalifikovanou elektronickou pečaťou v centrálnej elektronickej podateľni	Možnosť viacnásobnej autorizácie kvalifikovaným elektronickým podpisom v klientskej aplikácii poskytovaná na slovensko.sk
XAdES_ZEP	Áno	Áno
ZEPf	Nie	Nie
PAdES	Áno * (od 19.4.2018)	Nie
ASiC-E XAdES	Áno (od 22.2.2018)	Nie **
ASiC-E CAdES	Áno (od 22.2.2018)	Nie
ASiC-S XAdES	Áno ***	Nie **
ASIC-S CAdES	Nie	Nie

* V centrálnej elektronickej podateľni je možná autorizácia kvalifikovanou elektronickou pečaťou len PDF súborov vo verziách 1.3 alebo 1.4. Podpora vyšších verzií sa pripravuje.
V klientskych aplikáciách poskytovaných na slovensko.sk v súčasnosti nie je podporované vytváranie podpisu PAdES ani CAdES.

** Viacnásobná autorizácia v ASiC XAdES je podporovaná v klientskej aplikácii D.Signer/XAdES, resp. ASiC Factory poskytovanej na slovensko.sk, avšak zatiaľ nie je funkciami portálu slovensko.sk podporovaná. Podpora sa pripravuje v najbližších mesiacoch roka 2018.

*** Vytváranie formátu ASiC-S XAdES nie je podporované, autorizovať je však možné už existujúci obsah z ASiC-S XAdES, pričom výstupom je ASiC-E XAdES. Ak vo vstupnom ASiC-S XAdES v podpise v elemente ds:Reference absentuje atribút URI, ktorý je vyžadovaný v ASiC-E XAdES, autorizácia sa nevytvorí a výsledkom je chyba.

5.2.3 Spoločná autorizácia viacerých elektronických dokumentov rovnakým formátom podpisu

Dostupnosť funkcie: od roku 2017

Spoločná autorizácia viacerých elektronických dokumentov umožňuje jedným podpisom alebo pečaťou autorizovať niekoľko elektronických dokumentov, pričom každý z týchto dokumentov môže byť zároveň autorizovaný aj samostatne alebo spoločne s inými dokumentami. Používa sa napríklad v zmysle § 28 ods. 3 a 6 alebo § 36 zákona č. 305/2013 Z. z.

Formát podpisu (všetky autorizácie používajú rovnaký formát)	Možnosť spoločnej autorizácie kvalifikovanou elektronickou pečaťou v centrálnej elektronickej podateľni	Možnosť spoločnej autorizácie kvalifikovaným elektronickým podpisom v klientskej aplikácii poskytovaná na slovensko.sk
XAdES_ZEP	Nie *	Nie *
ZEPf	Nie	Nie
PAdES	Nie **	Nie **
ASiC-E XAdES	Áno	Nie ***
ASiC-E CAdES	Áno	Nie
ASiC-S XAdES	Áno ****	Nie ****
ASiC-S CAdES	Nie ****	Nie ****

* Spoločná autorizácia v XAdES_ZEP je technicky možná klientskou aplikáciou D.Signer/XAdES, resp. D.Sig XAdES Extender poskytovanou na slovensko.sk, avšak zatiaľ nie je funkciami portálu slovensko.sk podporovaná. Podpora sa pripravuje v najbližších mesiacoch roka 2018.

Spoločná autorizácia v XAdES_ZEP službami centrálnej elektronickej podateľne nie je podporovaná a v súčasnosti sa zvažuje.

** Spoločná autorizácia rôznych súborov jedným podpisom PAdES nie je technicky možná.
Podpora pre podpisovanie PDF súborov vo verziách 1.3 alebo 1.4, ktoré sú už autorizované podpisom PAdES, ďalším podpisom vo formáte XAdES v ASiC alebo XAdES_ZEP, je poskytovaná v službách centrálnej elektronickej podateľne od 19. apríla 2018. Podpora pre vyššie verzie PDF sa pripravuje.
Podpora pre podpisovanie PDF v iných verziách než je PDF/A-1a, konkrétne PDF 1.3 a 1.4 v klientskej aplikácii D.Signer/XAdES na slovensko.sk, vrátane súborov podpísaných PAdES, sa pripravuje v najbližších mesiacoch roka 2018. V neskoršom termíne sa pripravuje aj podpora vyšších verzií PDF.
Zatiaľ nie je podporovaná z dôvodu vykonávaných validácií validátorom PDFNet SDK.

*** Spoločná autorizácia v ASiC-E XAdES je podporovaná v klientskej aplikácii D.Signer/XAdES resp. ASiC Factory poskytovanej na slovensko.sk, avšak zatiaľ nie je funkciami portálu slovensko.sk podporovaná. Podpora sa pripravuje v najbližších mesiacoch roka 2018.

**** Existujúci ASiC-S XAdES je možné predložiť na ďalšiu autorizáciu, pričom výstupom je ASiC-E XAdES. Vo vstupnom ASiC-S XAdES v podpise v elemente ds:Reference nesmie absentovať atribút URI.
Vytváranie formátu ASiC-S XAdES ani CAdES nie je v centrálnej elektronickej podateľni a ani v klientskej aplikácii na slovensko.sk podporované. Formát ASiC-S umožňuje podpisovanie iba jedného súboru, prípadne kontajnera.

5.2.4 Spájanie viacerých autorizácií v rôznych formátoch do jedného súboru

V prípade spoločnej autorizácie už autorizovaných elektronických dokumentov je obvykle žiadúce uloženie existujúcich autorizácií a novej autorizácie do jedného súboru. To je však v súčasnosti v centrálnej elektronickej podateľni a klientskych aplikáciách poskytovaných na slovensko.sk podporované len pri niektorých kombináciách formátov podpisov a podpisových kontajnerov. V prípade vzájomne nekompatibilných formátov nie je podporované zachovanie pôvodných autorizácií zo všetkých dokumentov vo výslednom súbore.

Taktiež je len v prípade niektorých kombinácií formátov v súčasnosti podporovaná autorizácia rovnakého obsahu v odlišnom výstupnom formáte podpisu ako mal pôvodný podpis.

Poskytovaná možnosť spájať autorizácie z dvoch súborov do jedného:

Formát	XAdES_ZEP	ZEPf	PAdES	ASiC-E XAdES	ASiC-E CAdES	ASiC-S
XAdES_ZEP	Nie *	Nie	Áno **	Nie	Nie	Nie
ZEPf	Nie	Nie	Áno **	Nie	Nie	Nie
PAdES	Áno **	Áno **	Nie	Áno **	Áno **	Nie
ASiC-E XAdES	Nie	Nie	Áno **	Nie ***	Nie	Nie
ASiC-E CAdES	Nie	Nie	Áno **	Nie	Nie ***	Nie
ASiC-S	Nie	Nie	Nie	Nie	Nie	Nie

Poskytovaná možnosť pridať k autorizovanému dokumentu ďalší dokument a vytvoriť spoločnú autorizáciu:

	Výstupný formát autorizácie (napr. spoločná autorizácia s ďalším dokumentom vo formáte XML)					
Formát autorizácie na vstupe	XAdES_ZEP	ZEPf	PAdES	ASiC-E XAdES	ASiC-E CAdES	ASiC-S XAdES
XAdES_ZEP	Nie *	Nie	Nie	Nie	Nie	Nie
ZEPf	Nie	Nie	Nie	Nie	Nie	Nie
PAdES	Áno **	Áno **	Nie	Áno **	Áno **	Nie
ASiC-E XAdES	Nie	Nie	Nie	Áno	Nie	Nie
ASiC-E CAdES	Nie	Nie	Nie	Nie	Áno	Nie
ASiC-S XAdES	Nie	Nie	Nie	Áno	Nie	Nie
ASiC-S CAdES	Nie	Nie	Nie	Nie	Nie	Nie

* Spájanie samostatných autorizácií XAdES_ZEP zatiaľ nie je podporované v službách centrálnej elektronickej podateľne, je podporované v klientskej aplikácii D.Signer/XAdES, avšak zatiaľ nie je funkciami portálu slovensko.sk podporované.
Podpora pre vytváranie spoločných autorizácií XAdES_ZEP v klientskej aplikácii sa pripravuje v najbližších mesiacoch roka 2018.
Podpora pre vytváranie spoločných autorizácií XAdES_ZEP v centrálnej elektronickej podateľni sa v súčasnosti zvažuje.

** Podpisovanie PDF súborov vo verziách 1.3 a 1.4, ktoré sú autorizované podpisom PAdES, ďalším podpisom v ASiC, v ZEPf alebo v XAdES_ZEP je podporované v službách centrálnej elektronickej podateľne od 19. apríla 2018 a pripravuje sa aj v klientskych aplikáciách D.Signer/XAdES v najbližších mesiacoch roka 2018. V neskoršom termíne sa pripravuje podpora aj vyšších verzií PDF. Zatiaľ nie sú podporované z dôvodu vykonávaných validácií validátorom PDFNet SDK.

*** Možnosť spájať autorizáciu z dvoch ASiC-E súborov je technicky možná v klientskom komponente ASiC Factory avšak v súčasnosti nie je podporovaná na portáli slovensko.sk a ani v centrálnej elektronickej podateľni. Podpora sa zvažuje. Možnosť spájania autorizácie sa týka iba ASiC-E XAdES, ASiC-E CAdES. Netýka sa ASiC-S CAdES ani ASiC-S XAdES.
Podpísaný objekt v ASiC-S XAdES je možné opäť autorizovať, pričom výstupom je ASiC-E XAdES.