Dokumentácia funkčnosti Centrálnej elektronickej podateľne

Zoznam zmien:

Dátum vydania	Verzia	Popis zmien
1.7.2019	1.13	Odporúčanie používať Encoding Base64 v MessageContainer uvedené v kapitole 1, informácia o vyžadovaných hodnotách „Identifier“ pri opakovanej alebo spoločnej autorizácii v kapitole 2, upozornenie na pripravovaný začiatok používania jednotných referencovateľných identifikátorov e-formulárov počas r. 2019 uvedené v kapitole 2 a 3, informácia o dopĺňaní nových hodnôt do evidencie akceptovaných typov dátových objektov v kapitole 2, úprava zoznamu validovaných formátov pre XAdES_ZEP a ASiC v kapitole 4, oprava informácie o podpore podpisov z DSS v kapitole 5.1, doplnenie informácie o neposkytovaní kvalifikovanej služby validácie v kapitole 5.1 a informácie o overovaní podpisov/pečatí a časových pečiatok v kapitole 5.1.4, aktualizácia informácií o predvolenom formáte-ASiC, o podpore spoločnej autorizácie na portáli slovensko.sk, o podpore PDF 1.3 a 1.4 a o doplnení funkcie spájania ASiC v kapitole 5.2, doplnený bod 6 s pravidlami replikácie formulárov z MEF do CEP
25.7.2019	1.14	Informácie o podporovaných možnostiach overovania a vytvárania časových pečiatok v bode 5.1.4.3 a 5.2.5. Informácia o podpore PDF 1.5 a vyšších verzií v ASiC-CAdES a PAdES v bode 5.2.1.
27.8.2019	1.15	Informácia o overovaní podpisov/pečatí pri nesprávnej hodnote z evidencie typov objektov v bode 2.1, informácia o ukončení vyžadovania hodnoty v elementoch ObjectIdentifier a Description v ASiC-XAdES uvedená v bode 2.2, Informácie o podpore pečatenia XML a XMLDataContainer v ASiC-CAdES v bode 5.2.1

Obsah

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.

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

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 s class="FORM" nepodarilo správu spracovať a odosielateľ bol informovaný o nemožnosti jej spracovania s chybou *„2200001"* pričom v elektronickej schránke bola doplnená informáciou: *„Podateľni sa nepodarilo správu spracovať"*. Nesúlad MimeType s formátom môže mať za následok aj chybu pri ukladaní podpísaného obsahu (služba CEP pre vrátenie podpísaných dát).

Ako hodnotu atribútu Encoding sa dôrazne odporúča používať hodnotu „Base64" aj v prípade, ak je objekt s podpisom vo formáte XML (napr. XAdES_ZEP), nakoľko sa v praxi vyskytujú chybné systémy tretích strán, ktoré do súborov zasahujú a tým spôsobujú narušenie integrity, čo má za následok neplatnosť podpisov.

Požiadavky nevalidované v CEP:

V elemente Object je potrebné v atribúte Name používať príponu súboru príslušnú 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 na portáli slovensko.sk. 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 pre IS VS.

2 Formáty XAdES_ZEP, XAdES_ZEPbp a XAdESbp - evidencia typov dátových objektov a URI referencií

Účinnosť požiadavky: od začiatku prevádzky v roku 2013

2.1 Evidencia typov dátových objektov pre formát XAdES_ZEP

Nasledovné hodnoty sú uvádzané vo formáte XAdES_ZEP vytváranom v centrálnej elektronickej podateľni alebo klientskymi aplikáciami na portáli slovensko.sk v elementoch ObjectIdentifier, Description a XMLVerificationDataReferences.

Pri overovaní autorizácie v centrálnej elektronickej podateľni je autorizácia vyhodnotená ako neplatná alebo neoveriteľná, ak nasledovné hodnoty nie sú uvedené vo formáte XAdES_ZEP v elementoch ObjectIdentifier (neoveriteľná), Description (neplatná) a XMLVerificationDataReferences (SchemaReference - neplatná, VisualTransformReference - neoveriteľná).

> Pozn.: Kontrola týchto hodnôt sa pri overovaní v centrálnej elektronickej podateľni vykonáva prednostne, pred kontrolou digitálneho odtlačku podpísaného súboru. V prípade iných hodnôt elementov, než sú uvedené v tejto kapitole, nie je možné z výsledku overenia zistiť, či je chyba iba v nesprávnej hodnote ObjectIdentifier alebo Description, ktoré sa zobrazujú prednostne, alebo je zároveň narušená aj integrita podpísaných údajov. Riešenie je možné požiadaním NASES o pridanie špecifickej hodnoty medzi akceptované hodnoty v CEP (viď Poznámka č. 4).

V prípade viacnásobnej alebo spoločnej autorizácie vo formáte XAdES_ZEP v centrálnej elektronickej podateľni je podmienkou jej vykonania súlad hodnoty Identifier v existujúcom podpise vo vstupnom súbore XAdES_ZEP s nasledovnými hodnotami.

Formát dátového objektu	**Hodnota v elemente Identifier**	**Hodnota v elemente Description**
PDF	http://schemas.gov.sk/attachment/pdf	PDF
PNG	http://schemas.gov.sk/attachment/png	PNG
TXT	http://schemas.gov.sk/attachment/txt	TXT
XML údaje vyplnené podľa elektronického formulára	Hodnota z atribútu "targetNamespace" zo súboru schema.xsd e-formulára evidovaného v module elektronických formulárov (MEF) doplnená o reťazec "/form.xsd". Príklad: http://schemas.gov.sk/form/ED.DeliveryReport/1.9/form.xsd	Hodnota z elementu „dc:title“ (názov e-formulára) zo súboru meta.xml z e-formulára v MEF
XML údaje vyplnené	https://data.gov.sk/doc/egov/eform/identifikator-e-formulara/verzia/cesta-k-suboru	Hodnota z elementu

podľa elektronického formulára	- Bude sa používať až od dátumu v r. 2020, ktorý bude určený v 3./ 4.Q 2019	„dc:title“ (názov e-formulára) zo súboru meta.xml z e-formulára v MEF

Formát dátového objektu	**Hodnota v elemente VisualTransformReference**	**Hodnota v elemente SchemaReference**
XML údaje vyplnené podľa elektronického formulára	Hodnota z atribútu "targetNamespace" zo súboru schema.xsd e-formulára evidovaného v MEF doplnená o reťazec "/form.xslt", t.j. výsledná hodnota je najčastejšie v nasledovnom tvare: "http://schemas.gov.sk/form/identifikator-e-formulara/verzia/form.xslt" *	Hodnota z atribútu "targetNamespace" zo súboru schema.xsd e-formulára evidovaného v MEF doplnená o reťazec "/form.xsd", ", t. j. výsledná hodnota je najčastejšie v nasledovnom tvare: "http://schemas.gov.sk/form/identifikator-e-formulara/verzia/form.xsd" *
XML údaje vyplnené podľa elektronického formulára	https://data.gov.sk/doc/egov/eform/identifikator-e-formulara/verzia/cesta-k-suboru - Bude sa používať až od dátumu v r. 2020, ktorý bude určený v 3./ 4.Q 2019	https://data.gov.sk/doc/egov/eform/identifikator-e-formulara/verzia/cesta-k-suboru - Bude sa používať až od dátumu v r. 2020, ktorý bude určený v 3./ 4.Q 2019

- Poznámka č. 1:
  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/XAdES, ktoré korešpondujú s položkami vo vytvorenom XAdES_ZEP.

- Poznámka č. 2:
  Ako „identifikator-e-formulara“ sa uvádza príslušná časť URI identifikátora-referencia a ako „verzia“ sa uvádza príslušná verzia e-formulára.

- Poznámka č. 3:
  Od dátumu, ktorý bude zverejnený na portáli slovensko.sk v časti „O portáli“/“Technické informácie“ sa môžu pre referenciu schém

v XAdES_ZEP používať jednotné referencovateľné identifikátory v nasledujúcom tvare:„https://data.gov.sk/doc/egov/eform/identifikator-e-formulara/verzia/cesta-k-suboru“, a to na základe Výnosu č. 55/2014 Z. z. o štandardoch pre IS VS, ustanovení § 46 písm. a) bod 3b a prílohy č. 3 bodu 2.2.1 písm. b) a bodu 7.3.6. Tieto budú funkčné aj ako živá linka pre stiahnutie schémy.

- Poznámka č. 4:
  V Centrálnej elektronickej podateľni je evidencia typov dátových objektov postupne **dopĺňaná o ďalšie prípustné hodnoty** elementov Identifier a Description. Návrh na doplnenie chýbajúcej hodnoty je možné zaslať na adresu prevadzka@nases.gov.sk, pričom NASES predložené návrhy zváži.

Zoznam doplnených akceptovaných hodnôt pre element Identifier v centrálnej elektronickej podateľni, len pre účel overenia historických podpisov, je nasledovný, pričom tieto hodnoty by sa už nemali používať:

Pre formát PDF

- http://www.ditec.sk/ep/signature_formats/xades_zep_pdf/v1.0
- http://www.ditec.sk/ep/signature_formats/xades_zep_pdf/v1.1
- http://www.ditec.sk/ep/signature_formats/xades_zep_pdf/v2.0
- http://www.ditec.sk/ep/signature_formats/xades_zep_pdf/v1
- http://www.adobe.com
- uri_rozhodnutia

(pozn.: ide o string s hodnotou „uri_rozhodnutia“, nie o URI rozhodnutia)

2.2 Evidencia typov dátových objektov pre formát XAdES_ZEPbp a XAdESbp v ASiC-XAdES

Pozn.:
Evidencia typov dátových objektov sa nevzťahuje na hodnoty uvádzané v XMLDataContainer

Hodnoty uvedené v nasledujúcej tabuľke sú uvádzané v štruktúre formátu XAdES_ZEPbp (v ASiC-XAdES) vytváranom v centrálnej elektronickej podateľni (ak ide o prvú autorizáciu) alebo klientskymi aplikáciami na portáli slovensko.sk.

V prípade opakovanej alebo spoločnej autorizácie vytváranej v centrálnej elektronickej podateľni v XAdES_ZEPbp sa od 26.7.2019 používa (kopíruje) hodnota z predchádzajúcej autorizácie. Ak predchádzajúca autorizácia neobsahovala elementy Identifier a Description, nebudú tieto elementy použité ani v novej autorizácii.

Pozn.:
V prípade viacnásobnej alebo spoločnej autorizácie vo formáte XAdES_ZEPbp a XAdESbp v centrálnej elektronickej podateľni bol do 25.7.2019 podmienkou jej vykonania súlad hodnoty Identifier v podpise vo vstupnom súbore (ASiC XAdES) s hodnotami z evidencie typov dátových objektov. Toto obmedzenie neplatilo pre podpisovanie klientskou aplikáciou.

Formát dátového objektu	**Hodnota v elemente Identifier**	**Hodnota v elemente Description**
PDF	http://schemas.gov.sk/attachment/pdf	PDF
PNG	http://schemas.gov.sk/attachment/png	PNG
TXT	http://schemas.gov.sk/attachment/txt	TXT
XML údaje vyplnené podľa elektronického formulára	hodnota z elementu "dc:identifier" zo súboru meta.xml z príslušného elektronického formulára v module elektronických formulárov. Príklad: http://data.gov.sk/doc/eform/ED.DeliveryReport/1.9	Hodnota z elementu dc:title (názov e-formulára) zo súboru meta.xml z príslušného e-formulára

V Centrálnej elektronickej podateľni je evidencia typov dátových objektov postupne dopĺňaná o ďalšie prípustné hodnoty elementov Identifier a Description. Návrh na doplnenie chýbajúcej hodnoty je možné zaslať na adresu prevadzka@nases.gov.sk , pričom NASES predložený návrh zváži.

3 XMLDataContainer - vyžadované tvary URI

Účinnosť požiadavky: od roku 2016

Formát XMLDataContainer sa v Centrálnej elektronickej podateľni a v klientskych aplikáciách D.Signer/XAdES vytvára ako podpisovaný dátový objekt vždy pri použití formátu ASiC-XAdES pre podpisovanie údajov vyplnených podľa elektronického formulára na základe údajov o použitom elektronickom formulári. V prípade opakovanej autorizácie sa XMLDataContainer nanovo nevytvára a pokiaľ je validný voči XSD schéme pre XMLDataContainer, autorizuje sa bez jeho zmeny (platné od 22.9.2018).
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.

3.1 Používanie referencovateľných identifikátorov

Pre referencie použitej prezentačnej schémy elektronického formulára 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 e-formulára 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 e-formulára 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.

- Ako „identifikator-e-formulara“ sa uvádza identifikátor evidovaný v module elektronických formulárov (resp. príslušná časť URI identifikátora-referencia) 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.

3.2 Používanie jednotných referencovateľných identifikátorov podľa štandardov pre IS VS

Vytváranie hodnoty URI v XMLDataContainer v nasledujúcom tvare sa začne **približne začiatkom roka 2020, od dátumu, ktorý bude do konca roka 2019 zverejnený** na portáli slovensko.sk v časti „O portáli“/“Technické informácie“ , a to na základe prílohy č. 3 bodu 7.3.6 Výnosu č. 55/2014 Z. z. o štandardoch

pre IS VS, v tvare predpísanom v §46 písm. a) bod 3a a 3b a prílohe č. 11 bodov D.4.2.1 a D.4.3.1 tohto Výnosu.

Do tohto dátumu sa jednotné referencovateľné identifikátory v XMLDataContainer nepoužívajú, a preto môžu byť odmietnuté v systémoch.

Hodnota pre referencie schém (typ „doc“)

Hodnota pre referencie schém bude podľa § 46 písm. a) bod 3b nasledovná (funkčná aj ako živá linka na úložisko):
„https://data.gov.sk/**doc**/egov/eform/identifikator-e-formulara/verzia/cesta-k-suboru“

- V elemente UsedXSDReference bude používaná hodnota v tvare:

„https://data.gov.sk/doc/egov/eform/identifikator-e-formulara/verzia/schema.xsd“

- V elemente UsedPresentationSchemaReference bude používaná hodnota v tvare:

„https://data.gov.sk/doc/egov/eform/identifikator-e-formulara/verzia/cesta-k-suboru“
Príklad:
„https://data.gov.sk/doc/egov/eform/Doc.GeneralAgenda/1.9/Content/form.1.sb.xslt“

Hodnota pre Identifikátor elektronického formulára (typ „id“)

- Hodnota používaná v atribúte Identifier v XMLDataContainer, na základe elementu dc:identifier elektronického formulára z modulu elektronických formulárov, môže nadobúdať hodnotu jednotného referencovateľného identifikátora podľa §46 písm. a) bod 3a: „https://data.gov.sk/**id**/egov/eform/identifikator-e-formulara/verzia“, a to od dátumu zverejneného v zmysle prílohy č. 3 bodu 7.3.6 Výnosu o štandardoch pre IS VS na portáli slovensko.sk v časti „O portáli“/“Technické informácie“.

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)

(Konfiguračný súbor: SMimeObjects.config)

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: application/xml
- Portable Network Graphics (.png) - mimetype: image/png

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.
Validácia sa automaticky vykonáva len pre nasledovné vybrané formáty podpísaných dátových objektov v ASiC, pre ostatné formáty sa nevykonáva. Je vecou nastavenia príslušného agendového systému, či bude výsledok validácie dátového objektu vyhodnocovať a zohľadňovať pri ďalšom konaní.

- 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

(Konfiguračný súbor: DataValidator.config)

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". Pre iné hodnoty mimetype sa nevykonáva.
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 (application/pdf)
  Pre validáciu formátu PDF je používaný nástroj PDFNet SDK od firmy PDFTron. Nahradenie tohto nástroja referenčným validátorom VeraPDF sa pripravuje počas roka 2020.
- PNG (image/png) a TIFF (image/tiff)
  Pre validáciu formátu PNG a TIFF je používaný konštruktor .NET triedy System.Drawing.BitMap.
- TXT (text/plain), XML (text/xml), XMLDataContainer (application/vnd.gov.sk.xmldatacontainer+xml)
  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 e-formulára.
- RTF (text/rtf), ODT (application/vnd.oasis.opendocument.text)
  Pre formáty RTF, ODT sa vykonáva len kontrola voči zoznamu akceptovaných mimetype.

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 (baseline profile) - XadesBPLevelB, XadesBPLevelT, XadesBPLevelLTA (používaný v ASiC)
3. pre CAdES_ZEP v1.0 a v2.0 - CAdES_BES, CAdES_EPES, CAdES_T, CAdES_XL, CAdES_A (používaný v ZEPf a v2.0 aj v ASiC)
4. pre CAdES baseline profile - CAdES_BpB, CAdES_BpT, CAdES_BpLTA (používaný v ASiC)
5. pre PAdES – PAdES baseline -B-level, PAdES baseline T-level, PAdES baseline LT-level (vyhodnocovaný ako T-level), PAdES baseline LTA-level.

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 pri predvolenej konfigurácii softvéru 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. Po zmene predvoleného nastavenia tohto softvéru je možné vytvárať podpisy podľa Vykonávacieho rozhodnutia Komisie podporované v CEP.

Služba overenia v centrálnej elektronickej podateľni nie je kvalifikovanou službou validácie kvalifikovaného elektronického podpisu / pečate v zmysle článku 33 a 40 Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014. Využívanie kvalifikovanej služby validácie sa v centrálnej elektronickej podateľni plánuje. Pre overovanie podpisov/pečatí sa v centrálnej elektronickej podateľni používajú certifikované aplikácie. Taktiež sa uchovávajú CRL, OCSP a certifikáty v ceste potrebné pre overenie podpisov a prípadné dodatočné dokazovanie overenia použitého v asynchrónnej službe úplného/čiastočného overenia.

5.1.1 Overovanie vnorených podpisov vo vnútri podpísaných dátových objektov

Centrálna elektronická podateľňa v súčasnosti neumožňuje automatizovane overovať podpisy nachádzajúce sa vo vnútri jednotlivých externe podpísaných dátových objektov (napr. podpisy v ASiC, ktorý je vnorený v inom ASiC). Podpora pre automatizované overovanie podpisov z vnútra externe podpísaných súborov v centrálnej elektronickej podateľni sa zatiaľ len pripravuje vzhľadom na novelu Výnosu č. 55/2014 Z.z. o štandardoch pre IS VS.

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 (t.j. PDF s PAdES vo vnútri ASiC-E XAdES), vo výsledku overenia podpisov sa v centrálnej elektronickej podateľni vyhodnotí len platnosť podpisu XAdES. Rovnako to platí pre podpisové kontajnery ako ASiC, ZEPf alebo XAdES_ZEP vnorené v ďalšom podpisovom kontajneri. 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.

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 Odlišovanie 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. Zákon č. 305/2013 Z.z. však pre niektoré úkony vyžaduje autorizáciu kvalifikovaným elektronickým podpisom a zdokonalený elektronický podpis preto v niektorých prípadoch nemusí byť akceptovaný. Vyhodnotenie, či je autorizácia dostatočná pre konkrétne konanie, nevykonáva centrálna elektronická podateľňa, musí si ho vyhodnotiť adresát správy prostredníctvom svojho informačného systému alebo manuálne.

Centrálna elektronická podateľňa uvádza vo výsledku služby „informatívne overenie podpisov 3“ od septembra 2018 informáciu, či je podpis kvalifikovaný alebo zdokonalený. (Netýka sa to výsledku informatívneho overenia dostupného vo verejne prístupnej službe na stránke slovensko.sk.) Vo výsledku overenia podpisov zasielaného do schránok orgánov verejnej moci sa táto informácia v súčasnosti neuvádza ako samostatný údaj a jej doplnenie sa pripravuje.

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. (Príznak bol zároveň v septembri 2019 nahradený novým SkQESealRules).

5.1.4 Výsledok overenia podpisov, pečatí a časových pečiatok

5.1.4.1 Podpisy/pečate bez časovej pečiatky

Synchrónna služba informatívneho overenia

V prípade informatívneho overenia podpisov prostredníctvom synchrónnej služby dostupnej na verejne dostupnej stránke portálu slovensko.sk alebo prostredníctvom ponuky v elektronickej schránke „Overiť podpisy“ sa vykonáva overenie podpisov bez časovej pečiatky k aktuálnemu času (voči poslednému dostupnému CRL alebo výsledku OCSP), nakoľko centrálna elektronická podateľňa nemá k dispozícii spoľahlivý údaj o čase vytvorenia podpisu/pečate. Výsledkom overenia môže byť údaj o podpise/pečati „predbežne platná“, ktorý však nie je konečným výsledkom overenia a v prípade úplného overenia môže byť takýto podpis vyhodnotený napríklad ako „platný“, „neplatný“ alebo „nie je možné rozhodnúť“.

Asynchrónna služba predbežného/úplného overenia

Orgány verejnej moci, ktoré používajú centrálnu elektronickú podateľňu ako svoju elektronickú podateľňu, dostávajú do svojej elektronickej schránky v rámci služby zaevidovania prijatej správy podania (EGOV_APPLICATION) alebo elektronického úradného dokumentu (EGOV_DOCUMENT) aj výsledok overenia podpisov v doručovanej správe, t.j. technickú správu Sk-Talk s Class "SIGN_VERIFY_RESULT".
Centrálna elektronická podateľňa v rámci zaevidovania prijatej správy pre tie podpisy, ktoré časovú pečiatku neobsahujú, dopĺňa vo svojej internej evidencii kvalifikovanú časovú pečiatku.
Kvalifikovaná časová pečiatka je následne použitá pri overení podpisu, ako dôveryhodná informácia o čase existencie podpisu. Vo výsledku overenia podpisu zasielaného do schránky OVM je preto uvedená informácia o kvalifikovanej časovej pečiatke rovnako ako keby bola časová pečiatka súčasťou podpisu (rozdiel je obvykle len vo väčšom časovom odstupe času podpisu a času časovej pečiatky). Keďže sa kvalifikovaná časová pečiatka pri zaevidovaní správy nedopĺňa priamo do správy, podpis v správe zostáva v pôvodnom stave, v akom bol zaslaný. Orgán verejnej moci môže volaním služby „informatívne overenie“ z centrálnej elektronickej podateľne preveriť, či podpis obsahuje časovú pečiatku, ak potrebuje túto informáciu.

5.1.4.2 Podpisy/pečate s neplatnou časovou pečiatkou

V prípade, ak podpis obsahuje:
- iba neplatnú časovú pečiatku / časové pečiatky,
- časové pečiatky pripojené k podpisu až po konci platnosti certifikátu podpisu/pečate (a prípadnej pripojenej časovej pečiatky),

centrálna elektronická podateľňa vyhodnocuje podpisy nasledovne:

Synchrónna služba informatívneho overenia

- v prípade XAdES_ZEP s neplatnou časovou pečiatkou sa podpis vyhodnotí ako neplatný.

- v prípade XAdESbp s neplatnou časovou pečiatkou sa podpis overuje ku aktuálnemu času („now“) a vo výsledku overenia sa uvádza časová informácia z neplatnej časovej pečiatky.
- v prípade CAdES_ZEP a CAdESbp s neplatnou časovou pečiatkou sa podpis/pečať vyhodnotí ako neplatný.
- v prípade PAdES s neplatnou časovou pečiatkou sa podpis overuje ku aktuálnemu času a vo výsledku overenia sa uvádza čas z neplatnej časovej pečiatky.

Asynchrónna služba predbežného/úplného overenia

- V prípade XAdES_ZEP s neplatnou časovou pečiatkou sa v internej evidencii CEP táto časová pečiatka pre účely overenia podpisov odstráni a doplní sa nová, ktorá sa použije pre overenie a informácia z doplnenej časovej pečiatky sa uvádza vo výsledku overenia.
- V prípade XAdESbp s neplatnou časovou pečiatkou sa podpis overuje ku aktuálnemu času („now“) a vo výsledku overenia sa uvádza časová informácia z neplatnej časovej pečiatky.
- V prípade CAdES_ZEP a CAdESbp s neplatnou časovou pečiatkou sa podpis/pečať vyhodnotí ako neplatný.
- V prípade PAdES s neplatnou časovou pečiatkou sa podpis overuje ku aktuálnemu času a vo výsledku overenia sa uvádza čas z neplatnej časovej pečiatky.

5.1.4.3 Overovanie časových pečiatok

Certifikát časovej pečiatky sa pre všetky typy podpisov (XAdES_ZEP, XAdESbp, XAdES_ZEPbp, CAdESbp, CAdES_ZEP, PAdES) overuje nasledovne:

- Skontroluje sa, či je uvedený so stavom „granted“ v niektorom z Trusted list EÚ.
- Ak je uvedený v trusted list so stavom „granted“, nekontroluje sa už voči CRL resp. OCSP uvedeným v certifikáte časovej pečiatky.
- Ak nie je certifikát uvedený v trusted list so stavom „granted“, časová pečiatka sa považuje za neplatnú.

Služby centrálnej elektronickej podateľne v súčasnosti neposkytujú informácie o časovej pečiatke zahrnutej do autorizácie (t.j. contentTimestamp v CAdES podpise, AllDataObjectsTimeStamp alebo IndividualDataObjectsTimeStamp v XAdES podpise) a ani informácie o časovej pečiatke obsahu (t.j. samostatnej časovej pečiatke viazanej na

dokument a nie na podpis, napr. súbor .tst). Funkčnosť pre overovanie takýchto časových pečiatok sa pripravuje.

5.1.4.4 Overovanie na základe podpisovej politiky a TSA politiky

Formát XAdESbp (baseline profile)

Overovanie časových pečiatok:

- TSA politika časovej pečiatky sa ignoruje a pri overovaní sa časová pečiatka validuje voči „default“ politike platnej v čase, voči ktorému sa časová pečiatka overuje (v prípade poslednej časovej pečiatky to je „now“). Obsah „default“ politiky sa nastavuje v súlade s informáciami z aktuálne platných dokumentov ETSI TS 119 312, SOGIS Agreed Cryptographic Mechanisms 1.1 a TSL.
- Ak kvalifikovaná časová pečiatka nie je v súlade s „default“ politikou, napríklad ak je použitá stará hašovacia funkcia SHA-1, vyhodnotí sa ako neplatná.

Overovanie podpisov/pečatí:

- Pri validácii podpisu/pečate sa vychádza z podpisovej politiky v podpise/pečati. Ak v podpise/pečati absentuje podpisová politika, validuje sa voči “default“ podpisovej politike, ktorej obsah sa nastavuje v súlade s informáciami z aktuálne platných dokumentov ETSI TS 119 312, SOGIS Agreed Cryptographic Mechanisms 1.1 a TSL. V prípade uvedenej podpisovej politiky v podpise/pečati sa validuje voči podpisovej politike platnej v čase vytvorenia podpisu (podľa času v časovej pečiatke).

Formáty XAdES_ZEP, CAdES_ZEP, CAdESbp

Overovanie časových pečiatok:

- V konfigurácii overovačov v CEP sa aktualizáciami dodávateľa vkladajú a uchovávajú informácie o TSA politikách, voči ktorým sa validujú časové pečiatky. (Informácie: TSAPolicyID, NotBefore, NotAfter, MessageImprintAlgorithmConstraints, TimeStampTrustConditions, CertAlgorithmConstraints).

- Ak kvalifikovaná časová pečiatka obsahuje referenciu na TSA politiku, kontroluje sa, či ide o platnú politiku voči internej databáze politík uchovávaných v CEP a v prípade neplatnosti politiky alebo neznámej politiky sa časová pečiatka vyhodnotí ako neplatná.

- Ak kvalifikovaná časová pečiatka bez referencie na TSA/podpisovú politiku nie je v súlade s platnou podpisovou politikou vydanou NBÚ v

SR, napríklad ak je použitá stará hašovacia funkcia SHA-1 nepovolená v aktuálnej podpisovej politike, nemá to vplyv na platnosť časovej pečiatky vo výsledku overenia z CEP a môže sa vyhodnotiť ako platná. Vo výsledku overenia sa nezobrazuje upozornenie o nesúlade s podpisovou politikou.

Overovanie podpisov/pečatí:

- Pri validácii podpisu/pečate sa vychádza z podpisovej politiky v podpise/pečati. Ak v podpise/pečati absentuje podpisová politika (len formát CAdES+ASiC), validuje sa voči "default" podpisovej politike, ktorej obsah sa nastavuje v súlade s informáciami z aktuálne platných dokumentov ETSI TS 119 312, SOGIS Agreed Cryptographic Mechanisms 1.1 a TSL. V prípade uvedenej podpisovej politiky v podpise/pečati sa validuje voči podpisovej politike platnej v čase vytvorenia podpisu (podľa času v časovej pečiatke).

Formát PAdES

Overovanie časových pečiatok:

- V prípade PAdES sa TSA/podpisová politika časovej pečiatky ignoruje a pri overovaní sa časová pečiatka validuje voči podpisovej politike nastavenej v overovači (aktuálna podpisová politika vydaná NBÚ SR).

- Ak kvalifikovaná časová pečiatka v PAdES nie je v súlade s nastavenou podpisovou politikou, napríklad ak je použitá stará hašovacia funkcia SHA-1 nepovolená v aktuálnej podpisovej politike, časová pečiatka sa v CEP vyhodnocuje ako neplatná (čiže sa vyhodnocuje akoby tam nebola).

Overovanie podpisov/pečatí:

- Pri validácii podpisu/pečate sa využíva podpisová politika nastavená v overovači. (Od 26. júla 2019 aktuálna podpisová politika vydaná NBÚ SR.) Podpisová politika uvedená v podpise/pečati sa ignoruje. Nezohľadňuje sa teda, aká podpisová politika bola platná v čase vytvorenia podpisu.

- Ak podpis/pečať nie je v súlade s aktuálnou nastavenou podpisovou politikou, podpis/pečať sa vyhodnocuje ako neplatný/á.

5.1.5 Spôsob identifikácie a overovanie použitej podpisovej prezentačnej schémy v podpísanom súbore

V prípade doručenia podania alebo úradného dokumentu podpísaného XAdES_ZEP 1.x alebo 2.0 alebo v XMLDataContainer postupuje overovač v CEP nasledovne pri identifikácii podpisovej prezentačnej schémy, voči ktorej overuje digitálny odtlačok uvedený v podpise.

1. V prípade XAdES_ZEP 1.x a aj 2.0

CEP pre danú verziu dátového objektu typu xml overí, či sa v ňom nachádza identifikácia typu vizualizácie v elemente VisualTransformType. Pokiaľ je uvedený, použije sa pri hľadaní konkrétnej vizualizácie – xsltUri + typ vizualizácie („TXT“ alebo „HTML“). Ak typ vizualizácie nie je uvedený, je default predpokladaná „TXT“ hodnota.

Rozlišovacím znakom je aj verzia formátu pre xml plugin. Existujú 2 verzie:

- https://www.ditec.sk/ep/signature_formats/xades_zep_xml/v1.0/index.html - tento formát umožňoval podpisovať iba TXT vizualizáciu. Vznikol dávno pred možnosťou podpisovať HTML, resp. pred vznikom MEF (pred rokom 2013).

- https://www.ditec.sk/ep/signature_formats/xades_zep_xml/v2.0/index.html - tento formát vznikol cca v roku 2014 kedy bola legislatívne zachytená možnosť podpisovať aj HTML a zaviedol identifikáciu typu vizualizácie.

2. V prípade ASiC s XMLDataContainer

Najprv sa identifikuje, ci sú použité referencie, potom na základe xsltUri + hodnoty MediaDestinationTypeDescription sa vyhľadá evidovaná vizualizácia. Hľadanie je rovnaké ako v bode 1.

3. V prípade ASiC bez XMLDataContainer

Ak sú údaje vyplnené podľa elektronického formulára podpísané priamo, bez ich vloženia do XMLDataContainer, podpisová vizualizácia sa nevyhľadáva, resp. CEP nevyhodnocuje dáta ako údaje vyplnené podľa elektronického formulára.

Overovanie:

CEP pre identifikovanú podpisovú schému použitú v podpise príp. v XMLDataContainer vypočíta digitálny odtlačok a porovná ho s odtlačkom uvedeným v podpise, resp. v XMLDataContainer.

Ak v podpise nie je jednoznačne identifikovaná podpisová schéma a vo formulári je viacero schém rovnakého typu (napr. HTML), použije sa prvá schéma daného typu podľa poradia elementu file-entry v manifest.xml

Ak nie je digitálny odtlačok podpisovej prezentačnej schémy zhodný, podpis sa vyhodnocuje:

- V prípade XAdES_ZEP vždy ako neplatný
- V prípade XAdESbp alebo XAdES_ZEPbp sa vyhodnocuje platnosť podpisu nezávisle od digitálneho odtlačku schémy. Informácia o chybnom odtlačku sa uvádza v informáciách o validácii dátového objektu.

Ak identifikovaná podpisová schéma použitá v podpise je v databáze CEP (podľa bodu 6) evidovaná s media-destination="view", vo výsledku overenia podpisov sa neposkytuje informácia o skutočnosti, že v podpise bola použitá iná schéma než podpisová. Doplnenie tejto informácie sa pripravuje.

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, potvrdeniach o odoslaní a potvrdeniach o úhrade vytváraných Ústredným portálom verejnej správy sú od 22. septembra 2018 vo formáte ASiC-E XAdES.
Do 21. septembra 2018 boli vytvárané vo formáte XAdES_ZEP 1.1 (s verifikačnými údajmi pre XML dokumenty verzia 1.0 CreateObject do 6/2018 a vo verzii 2.0 CreateObject2 od 19.7.2018 s identifikáciou formátu použitej podpisovej prezentačnej schémy), pričom ako predvolená sa používala podpisová prezentačná transformácia do formátu TXT.

Predvolený formát pri podpisovaní v konštruktore správy na ÚPVS je od 22.9.2018 formát ASiC-E XAdES. Do 21.9.2018 bol predvolene vytváraný formát XAdES_ZEP 1.0 (s verifikačnými údajmi pre XML dokumenty 1.0).

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) - mimetype: application/pdf
    - pri ASiC-CAdES a PAdES - všetky verzie PDF
    - pri ASiC-XAdES a XAdES_ZEP - PDF len vo verzii 1.3 alebo 1.4 možnosť podpisovania iných verzií PDF s XAdES sa pripravuje)
- Extensible Markup Language (.xml) - mimetype: text/xml, mimetype: application/xml
    - pri ASiC-CAdES je podporovaný application/xml od 26.7.2019, text/xml (oba pre opakovanú alebo spoločnú autorizáciu)
    - pri ASiC-XAdES nie je podporovaný text/xml a pri opakovanej a spoločnej autorizácii nie je podporovaný ani application/xml
- Portable Network Graphics (.png) - mimetype: image/png
- Tagged Image File Format (.tiff, .tif) - mimetype: image/tiff
    - pri ASiC-XAdES a XAdES_ZEP nie je podporovaný
- XMLDataContainer (.xml) - mimetype: application/vnd.gov.sk.xmldatacontainer+xml
    - pri ASiC-CAdES je podporovaný od 26.7.2019
- ľubovoľný formát - mimetype: ľubovoľná hodnota (nevykonáva sa žiadna validácia)
    - podporovaný len pri opakovanej autorizácii už podpísaného objektu v ASiC-CAdES

Súbory vo formáte PDF sú pred podpísaním vo formáte ASiC-XAdES alebo XAdES_ZEP 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 voči PDF/A-1a pri podpisovaní súborov vo formáte PDF 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. V prípade, ak súbor obsahoval podpis PAdES, môže mať takáto konverzia za následok narušenie tohto podpisu a teda jeho neplatnosť. Pri podpisovaní cez klientske aplikácie na slovensko.sk je konverzia do PDF/A-1a vykonávaná automaticky, pokiaľ nejde o už podpísaný dokument.

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.

V prípade viacnásobnej autorizácie vo formátoch XAdES_ZEPbp (ASiC XAdES) alebo XAdES_ZEP v centrálnej elektronickej podateľni je podmienkou jej vykonania súlad hodnoty Identifier s hodnotami z evidencie typov dátových objektov podľa kapitoly 2.

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)	Áno (od 22.09.2018)
ASiC-E CAdES	Áno (od 22.2.2018)	Nie
ASiC-S XAdES	Áno ***	Áno (od 22.09.2018)
ASIC-S CAdES	Nie	Nie

* V klientskych aplikáciách poskytovaných na slovensko.sk v súčasnosti nie je podporované vytváranie podpisu PAdES ani CAdES.

*** 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.

V prípade spoločnej autorizácie vo formátoch XAdES_ZEPbp (ASiC XAdES) alebo XAdES_ZEP v centrálnej elektronickej podateľni je podmienkou jej vykonania súlad hodnoty Identifier s hodnotami z evidencie typov dátových objektov podľa kapitoly 2.

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 *	Áno (od 22.9.2018)
ZEPf	Nie	Nie
PAdES	Nie **	Nie **
ASiC-E XAdES	Áno	Áno (od 22.9.2018)
ASiC-E CAdES	Áno	Nie
ASiC-S XAdES	Áno ***	Áno***(od 22.9.2018)
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 len ak je vstupný formát XAdES_ZEP..

Spoločná autorizácia v XAdES_ZEP službami centrálnej elektronickej podateľne nie je podporovaná a v súčasnosti sa zvažuje. Vzhľadom na požiadavky legislatívy sa však v prípade potreby ďalšej autorizácie XAdES_ZEP odporúča vykonať zaručenú konverziu do ASiC.

** 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. Do tohto dátumu bol podporovaný len formát PDF/A-1a. Podpora pre podpisovanie vyšších verzií PDF XAdES podpisom 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, bola pridaná od 22.9. 2018. V neskoršom termíne sa pripravuje aj podpora vyšších verzií PDF.
Zatiaľ nie je podporovaná z dôvodu vykonávaných validácií validátorom PDFNet SDK.

*** 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 **	Áno ***	Nie	Nie
ASiC-E CAdES	Nie	Nie	Áno **	Nie	Áno ***	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	Áno *	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 bola pridaná od 22. 9. 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 (nevalidných podľa PDF/A-1a), ktoré sú autorizované podpisom PAdES, ďalším podpisom v ASiC-XAdES, v ZEPf alebo v XAdES_ZEP je podporované v službách centrálnej elektronickej podateľne od 19. apríla 2018 a v klientskych aplikáciách D.Signer/XAdES bola podpora pridaná od 22. 9. 2018. V neskoršom termíne sa pripravuje podpora aj vyšších verzií PDF. Zatiaľ nie sú v prípade XAdES podpisu podporované z dôvodu vykonávaných validácií validátorom PDFNet SDK. V prípade ASiC-CAdES sú podporované ľubovoľné verzie PDF.

*** Možnosť spájať autorizáciu z dvoch ASiC-E súborov je technicky možná v klientskom komponente ASiC Factory a je podporovaná na portáli slovensko.sk aj v centrálnej elektronickej podateľni od 22.9.2018.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.

5.2.5 Časové pečiatky

Podporované možnosti vytvárania kvalifikovaných časových pečiatok:

	Služba v centrálnej elektronickej podateľne	Funkčnosť v klientskej aplikácii na slovensko.sk
Pripojenie časovej pečiatky k podpisu (časová pečiatka nie je zahrnutá do podpísaných údajov, napr. v XAdES sa nachádza v „UnsignedProperties“)	Áno	Nie *
Zahrnutie časovej pečiatky do podpisovaných údajov	Nie	Nie

(contentTimestamp,v CAdES, AllDataObjectsTimeStamp alebo IndividualDataObjectsTimeStamp v XAdES)		
Vytvorenie časovej pečiatky dokumentu (napr. súbor .tst v ASiC alebo samostatná časová pečiatka v PAdES)	Nie	Nie

* Kvalifikovaná časová pečiatka sa automaticky pripája ku každému podpisu vytvorenému na portáli slovensko.sk (v konštruktore správy) po úspešnom podpísaní, a to volaním služby modulu CEP z modulu eDesk. Časová pečiatka sa teda nevytvára v samotnej klientskej aplikácii.

6 Pravidlá replikácie formulárov z MEF do CEP

CEP z MEF každý deň kopíruje elektronické formuláre pre účely vytvárania pečatí a pre účely overovania podpisov.

Postup replikácie:

1. Z modulu elektronických formulárov sa kopírujú len ZIP balíky e-formulárov.

2. V ZIP balíku sa postupne vyhľadajú súbory **schema.xsd, meta.xml** a **manifest.xml**.
   Ak sa tieto súbory nenájdu, proces pre daný formulár skončí s chybou a daný formulár sa neuloží a teda nebude pre podateľňu k dispozícii pre účely overovania podpisov.

3. S pomocou XPath sa prehľadá súbor manifest.xml za účelom vyhľadania podpisových prezentačných schém, a to v nasledovných krokoch, pričom pri prvom úspešnom kroku skončí:

Pre každý záznam file-entry z manifest.xml sa overí, či spĺňa nasledovné podmienky:

a) atribút **media-destination** musí obsahovať hodnotu **sign** alebo **view**, či už samotnú alebo oddelenú čiarkou od iných hodnôt. (view je prípustné z historických dôvodov, pretože sa často používalo pre podpisovanie ak bola k dispozícii len textová prezentačná schéma)
   a. hodnota atribútu **media-type** je **application/xslt+xml** alebo **text/xsl**, alebo

   b. hodnota atribútu **media-type** je **text/xml** alebo **application/xml** a zároveň je prípona súboru (uvedená v atribúte **full-path**) .**xsl** alebo .**xslt),**

b) názov súboru v atribúte **full-path** je v tvare ***.sb.xslt** alebo ***.html.xslt** (používané pre historické formuláre)

c) v nájdenej množine podpisových prezentačných schém z predchádzajúcich krokov sa identifikuje typ (formát prezentácie) nasledovným postupom:
   a. Do databázy sa pre každú schému zapisuje, či v atribúte **media-destination** bolo “sign” alebo “view”,
   b. Ak je uvedený atribút **media-destination-type-description**, tak sa rozlišujú hodnoty **TXT**, **HTML**, **XHTML** a akékoľvek iné**,** pričom pre každú prezentačnú schému sa v databáze ukladá hodnota, aká bola nájdená
   c. Ak je uvedený atribút **media-destination-type** tak sa rozlišujú hodnoty **text/plain** pre TXT, **text/html** pre HTML, **application/xhtml+xml** pre XHTML a rôzne iné, pričom sa všetky zistené hodnoty ukladajú v databáze (pri prezentačnej schéme sa v databáze evidujú hodnoty media-destination-type a aj media-destination-type-description – podľa toho, ktorú sa podarilo nájsť)
   d. Ak nie je uvedený **media-destination-type-description** a ani **media-destination-type**, tak sa v XSLT alebo XSL súbore vyhľadá <xsl:output method="html|xml|text pričom html=typ HTML, text=typ TXT, xml=typ XHTML, iné=typ INÉ.
   Pre XHTML sa pred identifikovaním ešte validuje, či v XSLT/XSL súbore je v „doctype-system“ substring "http://www.w3.org/TR/xhtml1"
   e. Ak je názov súboru v atribúte full-path v tvare ***.sb.xslt** identifikuje sa TXT, ak je v tvare ***.html.xslt** identifikuje sa HTML prezentácia.

   f. Ak sa **nepodarilo** určiť typ podpisovej transformácie podľa b,c,d ,e, systém to vyhodnotí ako **iné,** ktoré budú v množine schém pre overovanie podpisu.

   g. Ak formulár neobsahuje ani jeden z typov TXT, HTML, XHTML, formulár sa neuloží do databázy CEP.

Pre každú prezentačnú schému sa zapisuje do evidencie jej poradie v manifest.xml. Pri overovaní podpisov sa v prípade prezentačných schém rovnakého typu bude ako prioritná brať tá s najnižším poradovým číslom.

Pri replikácii sa zároveň do databázy ako referencia schém ukladá:

a) hodnota vyskladaná v tvare

http://schemas.gov.sk/form/identifikator-e-formulara/verzia/form.xsd (pre XSD schému)
http://schemas.gov.sk/form/identifikator-e-formulara/verzia/form.xslt (pre podpisovú prezentačnú schému)

b) hodnota z atribútu full-path-url pre súbor schema.xsd a podpisovú prezentačnú schému, a to od dátumu určeného v konfigurácii CEP a na základe verzie kontajnera elektronického formulára.
c) od dátumu určeného podľa bodu 7.3.6 prílohy č. 3 Výnosu č. 55/2014 Z.z. o štandardoch pre IS VS hodnota vyskladaná v tvare:
https://data.gov.sk/doc/egov/eform/identifikator-e-formulara/verzia/schema.xsd (pre XSD schému)
https://data.gov.sk/doc/egov/eform/identifikator-e-formulara/verzia/cesta-k-suboru (pre podpisovú prezentačnú schému)

7 Pravidlá pre určovanie poradia súborov z jedného podpisového kontajnera

Vo výstupe služby centrálnej elektronickej podateľne „vrátenie podpísaných dát“ sa poradie dokumentov uložených v podpisovom kontajneri určuje nasledovne:

V podpisovom kontajneri vo formáte ASiC-E je poradie dokumentov určené tým, v akom poradí sú podpísané súbory referencované v popisných súboroch "ASiCManifest*.xml" alebo "XAdES signatures*.xml" v adresári META-INF v štruktúre tohto podpisového kontajnera. V prípade viacerých popisných súborov „ASiCManifest*.xml“ alebo „XAdES signatures*.xml“ v ASiC sa najskôr vychádza z poradia, v akom sú uvedené v "ZIP central directory" súboru ASiC a následne pre každý z týchto súborov, je poradie určené tým, v akom poradí sú podpísané súbory referencované z "ASiCManifest*.xml" alebo "XAdES signatures*.xml". V prípade podpisu XAdES sa vychádza z poradia referencií v elemente XAdES DataObjectFormat v ds:Object. (T.j. nevychádza sa z poradia referencií v ds:Reference). V podpisovom kontajneri vo formáte ASiC-S obsahujúcom vnorený súbor vo formáte ZIP (tzv. „degradovaný ASiC“) je poradie spracovania elektronických dokumentov určené poradím, v akom sú uvedené v "ZIP central directory" tohto vnoreného súboru.