Workshop k prechodu na formát ASiC

Národná agentúra pre sieťové a elektronické služby

22. a 24. augusta, 5., 6., 7., 11., 13. septembra 2018

Workshop k prechodu na formát ASiC

Obsah workshopu:

1. Predstavenie eIDAS a povinných formátov (NASES) – s. 5
2. Princípy spoločnej a opakovanej autorizácie – s. 69
3. Ukážka bezplatnej aplikácie QES od NBÚ pre dokumenty, PDF, ASiC (NBÚ) – s. 86
4. Otázky a odpovede (NASES, NBÚ), Prestávka 10 minút
5. Predstavenie XMLDataContainer (NASES) – s. 90
6. Zmena predvoleného formátu vytváraného na ÚPVS z XAdES_ZEP na ASiC-E XAdES (NASES) – s. 96
7. Služby Centrálnej elektronickej podateľne pre vytváranie ASIC a iných formátov podľa eIDAS, vytváranie opakovanej autorizácie a spoločnej autorizácie (NASES) – s. 104
8. Predstavenie novej služby informatívneho overenia podpisov 3 a služby vrátenie podpísaných dát 2 (NASES)
9. Nové pravidlá replikácie elektronických formulárov v CEP, spôsob určovania predvolenej podpisovej transformácie pri vytváraní a overovaní autorizácie (NASES) – s. 111
10. Validácia podpisov a pečatí (NASES) – s. 122
11. Otázky a odpovede

Workshop k prechodu na formát ASiC

Témy za NASES

Štefan Szilva

stefan.szilva@nases.gov.sk

Témy za NBÚ

plk. Ing. Peter Rybár

Predstavenie eIDAS a formátu ASiC

Legislatíva

Elektronické podpisovanie – pôvodná legislatíva

Pôvodná legislatíva

- **1999 -** Smernica EP a Rady 1999/93/ES o rámci spoločenstva pre elektronické podpisy
  „elektronický podpis “,
  „zdokonalený elektronický podpis (AdES)“, „kvalifikovaný certifikát (QC)“

- **2002 -** Zákon č. 215/2002 Z. z. o elektronickom podpise
  „**elektronický podpis / pečať (EP)“,**
  „zaručený elektronický podpis / pečať (ZEP, ZEPe)“
  - Vykonávacie predpisy: Vyhlášky NBÚ č. 131/2009 Z. z. - 136/2009 Z. z.
- ... - osobitné predpisy
- **2013 -** Zákon č. 305/2013 Z. z. o e-Governmente (o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci)
  - § 23 - Autorizácia a preukazovanie oprávnenia konať v mene inej osoby **– účinný od 1. 11. 2013**

Elektronické podpisovanie – nová legislatíva (KEP)

Nová legislatíva

- **2015** - Výnos č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy
  - § 57a až § 57d **účinné od 15. októbra 2015** (pri formátoch ASiC / PAdES vychádzal z eIDAS)

- **2016 -** eIDAS - Nariadenie EP a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES – **uplatňuje sa od 1. 7. 2016**
  - Vykonávacie rozhodnutie Komisie (EÚ) 2015/1506 ktorým sa ustanovujú špecifikácie týkajúce sa formátov zdokonalených elektronických podpisov a zdokonalených elektronických pečatí, ktoré môžu subjekty verejného sektora uznávať, podľa článkov 27 ods. 5 a 37 ods. 5 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu
  - **„zdokonalený elektronický podpis / pečať (AdES)“**
    „kvalifikovaný elektronický podpis / pečať (QES - KEP / KEPe)“

- **2016 -** Zákon č. 272/2016 Z. z. o dôveryhodných službách (o dôveryhodných službách pre elektronické transakcie na vnútornom trhu) **účinný od 20. 9. 2016**

Elektronické podpisovanie – nová legislatíva (KEP)

Nová legislatíva

- Zákon č. 305/2013 Z. z. o e-Governmente (o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci)
    - § 23 - Autorizácia a preukazovanie oprávnenia konať v mene inej osoby – **zosúladenie s eIDAS,**
    - **rozšírenie možností autorizácie od 1. novembra 2017**

- Osobitné predpisy ...

- **2018** - Výnos č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy
    - novela – Opatrenie 11/2018

eIDAS – čo to je?

eIDAS *(neformálne):*

eID ***-*** *electronic identification,*

A ***-*** *authentication,*

S *- signatures, trust services*

- *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*
- *Nariadenie EP a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES*

- Pozn: eIDAS autentifikácia bude pre prihlasovanie cez WebSSO ÚPVS spustená koncom septembra 2018, NASES o tom bude samostatne informovať integrované subjekty.

eIDAS - Podpis

„elektronický podpis“ sú údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme a ktoré podpisovateľ používa na podpisovanie;

„zdokonalený elektronický podpis“ je elektronický podpis, ktorý spĺňa požiadavky stanovené v článku 26;

***„kvalifikovaný elektronický podpis“ je zdokonalený elektronický podpis** vyhotovený s použitím zariadenia na vyhotovenie elektronického podpisu a založený na kvalifikovanom certifikáte pre elektronické podpisy;*

*„certifikát pre elektronický podpis“ je elektronické osvedčenie, ktoré spája údaje na validáciu elektronického podpisu **s fyzickou osobou a potvrdzuje aspoň jej meno alebo pseudonym**;*

*„kvalifikovaný certifikát pre elektronický podpis“ je certifikát pre elektronický podpis, **ktorý vydáva kvalifikovaný poskytovateľ dôveryhodných služieb** a ktorý spĺňa požiadavky stanovené v prílohe I;*

(článok 3 eIDAS)

eIDAS - Pečať

„elektronická pečať“ sú údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme s cieľom zabezpečiť pôvod a integritu týchto pridružených údajov;

„zdokonalená elektronická pečať“ je elektronická pečať, ktorá spĺňa požiadavky stanovené v článku 36;

***„kvalifikovaná elektronická pečať“ je zdokonalená elektronická pečať** vyhotovená pomocou zariadenia na vyhotovenie elektronickej pečate a založená na kvalifikovanom certifikáte pre elektronickú pečať;*

*„certifikát pre elektronickú pečať“ je elektronické osvedčenie, ktoré spája údaje na validáciu elektronickej pečate **s právnickou osobou a potvrdzuje jej názov**;*

*„kvalifikovaný certifikát pre elektronickú pečať“ je certifikát pre elektronickú pečať, ktorý vydáva **kvalifikovaný poskytovateľ dôveryhodných služieb** a ktorý spĺňa požiadavky stanovené v prílohe III;*

(článok 3 eIDAS)

eIDAS – povinnosť akceptovať AdES-QC/QES

Článok 27

Elektronické podpisy vo verejných službách

1. Ak členský štát na využívanie služby online, ktorú ponúka subjekt verejného sektora alebo ktorá sa ponúka v jeho mene, ***vyžaduje zdokonalený elektronický podpis, uznáva tento členský štát zdokonalené elektronické podpisy, zdokonalené elektronické podpisy založené na kvalifikovanom certifikáte pre elektronické podpisy a kvalifikované elektronické podpisy****, a to aspoň tie, ktoré sú vo formátoch alebo ktoré používajú metódy vymedzené vo vykonávacích aktoch uvedených v odseku 5.*

2. Ak členský štát na využívanie služby online, ktorú ponúka subjekt verejného sektora alebo ktorá sa ponúka v jeho mene, ***vyžaduje zdokonalený elektronický podpis založený na kvalifikovanom certifikáte****, uznáva tento členský štát zdokonalené elektronické podpisy založené na kvalifikovanom certifikáte a kvalifikované elektronické podpisy, a to aspoň tie, ktoré sú vo formátoch alebo ktoré používajú metódy vymedzené vo vykonávacích aktoch uvedených v odseku 5. (Slovenská republika)*

3. Členské štáty ***nesmú vyžadovať*** *na cezhraničné využívanie služby online, ktorú ponúka subjekt verejného sektora, elektronický podpis* ***vyššej úrovne bezpečnosti ako kvalifikovaný elektronický podpis****. (t.j. nesmú vyžadovať ani XAdES_ZEP)*

4. Komisia môže prostredníctvom vykonávacích aktov určiť referenčné čísla noriem ***pre zdokonalené elektronické podpisy****. Ak zdokonalený elektronický podpis spĺňa uvedené normy, má sa za to, že je v súlade s požiadavkami na zdokonalené elektronické podpisy uvedenými v odsekoch 1 a 2 tohto článku a v článku 26. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.*

5. Komisia do 18. septembra 2015 prostredníctvom vykonávacích aktov vymedzí referenčné formáty zdokonalených elektronických podpisov alebo referenčné metódy pre prípady, keď sa používajú alternatívne formáty, pričom zohľadní existujúcu prax, normy a právne akty Únie. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

eIDAS – povinnosť akceptovať AdES-QC/QES

Článok 37

Elektronické pečate vo verejných službách

1. Ak členský štát na využívanie služby online, ktorú ponúka subjekt verejného sektora alebo ktorá sa ponúka v mene tohto subjektu, ***vyžaduje zdokonalenú elektronickú pečať, uznáva tento členský štát zdokonalené elektronické pečate, zdokonalené elektronické pečate založené na kvalifikovanom certifikáte pre elektronické pečate a kvalifikované elektronické pečate****, a to aspoň tie, ktoré sú vo formátoch alebo ktoré používajú metódy vymedzené vo vykonávacích aktoch uvedených v odseku 5.*

2. Ak členský štát na využívanie služby online, ktorú ponúka subjekt verejného sektora alebo ktorá sa ponúka v mene tohto subjektu, ***vyžaduje zdokonalenú elektronickú pečať založenú na kvalifikovanom certifikáte****, uznáva tento členský štát zdokonalené elektronické pečate založené na kvalifikovanom certifikáte a kvalifikované elektronické pečate, a to aspoň tie, ktoré sú vo formátoch alebo ktoré používajú metódy vymedzené vo vykonávacích aktoch uvedených v odseku 5.*

3. Členské štáty ***nesmú vyžadovať*** *na cezhraničné využívanie služby online, ktorú ponúka subjekt verejného sektora, elektronickú pečať* ***vyššej úrovne bezpečnosti ako kvalifikovaná elektronická pečať****.*

4. ...

eIDAS – alternatívne formáty

Vykonávacie rozhodnutie Komisie (EÚ) 2015/1506

Článok 2

1. *Členské štáty vyžadujúce zdokonalený elektronický podpis alebo zdokonalený elektronický podpis založený na kvalifikovanom certifikáte, ako sa ustanovuje v článku 27 ods. 1 a 2 nariadenia (EÚ) č. 910/2014, uznajú iné formáty elektronických podpisov než tie, ktoré sú uvedené v článku 1 tohto rozhodnutia, za predpokladu, že členský štát, v ktorom má sídlo poskytovateľ dôveryhodných služieb používaný podpisovateľom, ponúkne iným členským štátom možnosti validácie podpisu, ktoré budú podľa možnosti vhodné na automatizované spracovanie.*
2. *Možnosti validácie podpisu musia:*

a) *umožňovať ostatným členským štátom validovať prijaté elektronické podpisy online, bezplatne a spôsobom, ktorý je zrozumiteľný pre cudzincov;*

b) *...*

Autorizácia – zákon 305/2013 Z.z.

§ 23 ods. 1

Autorizácia a preukazovanie oprávnenia konať v mene inej osoby

*(1) Orgán verejnej moci vykoná pri výkone verejnej moci autorizáciu elektronického podania alebo elektronického úradného dokumentu **kvalifikovaným elektronickým podpisom**17) vyhotoveným s použitím mandátneho certifikátu20) alebo **kvalifikovanou elektronickou pečaťou**,18) ku ktorým pripojí kvalifikovanú elektronickú časovú pečiatku,19) a to spôsobom podľa odseku 3. Osoba, ktorá nie je orgánom verejnej moci, vykoná autorizáciu elektronického podania,*

a) ak sa podľa zákona podáva v elektronickej podobe a zákon neustanovuje iný spôsob autorizácie alebo ak je podľa osobitného predpisu náležitosťou podania vlastnoručný podpis

*1. **kvalifikovaným elektronickým podpisom**17) alebo kvalifikovanou elektronickou pečaťou,18)*

2. použitím na to určenej funkcie informačného systému prístupového miesta a po úspešnej autentifikácii osoby ktorá autorizáciu vykonáva, zodpovedajúcej najmenej úrovni zabezpečenia „pokročilá“ podľa osobitného predpisu,20a) ak sa zabezpečí uvedenie tejto osoby ako odosielateľa elektronickej správy, nemennosť obsahu autorizovaného dokumentu do momentu uloženia v elektronickej schránke adresáta, spojenie autorizovaného dokumentu s identifikátorom osoby odosielateľa a zachovanie väzby medzi nimi, ak to osobitný predpis nezakazuje alebo *(tzv. „autorizácia klikom“)*

3. uznaným spôsobom autorizácie, ak to osobitný predpis nezakazuje, *(vydáva sa osobitným predpisom ÚPPVII, nebol zatiaľ vydaný)*

b) ak podľa osobitného predpisu je náležitosťou vlastnoručný podpis, ktorý musí byť úradne osvedčený

*1. **kvalifikovaným elektronickým podpisom**17) alebo **kvalifikovanou elektronickou pečaťou**,18) ku ktorým pripojí kvalifikovanú elektronickú časovú pečiatku,19) alebo*

2. uznaným spôsobom autorizácie pre taký právny úkon, ak to osobitný predpis nezakazuje.

---

17) Čl. 3 ods. 12 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Ú. v. EÚ L 257, 28. 8. 2014).

18) Čl. 3 ods. 27 nariadenia (EÚ) č. 910/2014

Autorizácia – zákon 305/2013 Z.z.

§ 3

o) autorizáciou úkonu vyjadrenie súhlasu s obsahom právneho úkonu a s vykonaním tohto právneho úkonu,

§ 23 ods. 3

(3) Ak tento zákon alebo osobitný predpis20b) vyžaduje autorizáciu ***konkrétnou osobou alebo osobou v konkrétnom postavení****, na autorizáciu sa použije kvalifikovaný elektronický podpis17) vyhotovený s použitím mandátneho certifikátu,20) ku ktorému sa pripojí kvalifikovaná elektronická časová pečiatka.19) Ak tento zákon alebo osobitný predpis20c) ustanovuje len povinnosť autorizácie* ***bez označenia konkrétnej osoby alebo osoby v konkrétnom postavení, alebo autorizujúcu osobu označuje len všeobecne ako oprávnenú osobu****, na autorizáciu sa použije kvalifikovaný elektronický podpis17) vyhotovený s použitím mandátneho certifikátu20) alebo kvalifikovaná elektronická pečať,18) ku ktorým sa pripojí kvalifikovaná elektronická časová pečiatka.19)*

eIDAS – povinné formáty podpisov / pečatí - baseline profile

- Vykonávacie rozhodnutie Komisie (EÚ) č. 2015/1506 predpisuje povinné základné profily formátov zdokonalených elektronických podpisov / pečatí / čas. pečiatok:
  - ETSI TS 103 171 v2.1.1 - XAdES Baseline profile (2012-03)
  - ETSI TS 103 173 v2.2.1 - CAdES Baseline profile (2013-04)
  - ETSI TS 103 172 v2.2.2 - PAdES Baseline profile (2013-04)
  - ETSI TS 103 174 v2.2.1 - ASiC Baseline profile (2013-06)

- **Povinnosť prijímať všetky tieto formáty a vytvárať najmenej jeden z nich**
- V Centrálnej elektronickej podateľni podporované od júla 2016

ETSI EN – nové verzie, zatiaľ nepovinné

- V roku 2016 boli vydané nové verzie (ETSI EN) špecifikácií ASiC, XAdES, CAdES, PAdES, ktoré však **nie sú povinne predpísané** Vykonávacím rozhodnutím Komisie 2015/1506
  - ETSI EN 319 132 - XAdES digital signatures (2016)
  - ETSI EN 319 122 - CAdES digital signatures (2016)
  - ETSI EN 319 142 - PAdES digital signatures (2016)
  - ETSI EN 319 162 - Associated Signature Containers (ASiC) (2016)

  - Ak je rozpor v požiadavkách v ETSI EN a ETSI TS, musia byť splnené požiadavky vyžadované z legislatívy účinnej v čase vyhotovenia podpisu, alebo pečate. (Vyjadrenie NBÚ)
  - Používané predvolene v aplikácii Digital Signature Service (financované EÚ)

- Centrálna elektronická podateľňa tieto nové verzie podporuje len čiastočne. Plánuje sa podpora v budúcnosti. (napr. nepodporuje ASiC-XAdES vytvorený podľa novej normy)

PAdES, XAdES, CAdES

- **QES – Qualified Electronic Signature / Seal** - kvalifikovaný elektronický podpis / pečať
- **AdES – Advanced Electronic Signature / Seal** - zdokonalený elektronický podpis / pečať

- **CAdES** – **CMS** Advanced Electronic Signatures

založené na RFC 5652 - Cryptographic Message Syntax (CMS) (vydané 1999), vychádza z PKCS#7 (1993)

- **XAdES** – **XML** Advanced Electronic Signatures

založené na W3C XML Signature Syntax and Processing (vydané 2002)

- **PAdES** – **PDF** Advanced Electronic Signatures

založené na: CAdES a PDF, ktoré definuje spôsob ukladania podpisov (prvýkrát v r. 2000)

+ doplnková možnosť využitia XAdES pre embedované XML objekty (nesúvisí s kvalifikovaným elektronickým podpisom a pečaťou)

ASiC

- **ASiC – Associated Signature Container**

Definuje povinné rozširujúce pravidlá pre CMS AdES, XML AdES a časovú pečiatku dokumentu, pričom využíva niektoré princípy existujúcich formátov (ZIP, OpenDocument format, ePUB, atď)

Sankcie za používanie formátov v rozpore s eIDAS – do 3000 EUR

§ 14 zákona č. 272/2016 Z.z. o dôveryhodných službách dáva Národnému bezpečnostnému úradu právomoc udeľovať sankcie:

(3) Úrad uloží pokutu do 3 000 eur orgánu verejnej moci, ktorý sa dopustí správneho deliktu tým, že odmietne prijať kvalifikovaný elektronický podpis alebo kvalifikovanú elektronickú pečať ***vo formáte, ktorý je v súlade*** *s prílohou vykonávacieho aktu Komisie vydaného podľa čl. 27 ods. 5 a čl. 37 ods. 5 nariadenia (EÚ) č. 910/2014.*

(4) Úrad uloží pokutu do 3 000 eur orgánu verejnej moci, ktorý sa dopustí správneho deliktu tým, že ***vytvorí kvalifikovaný elektronický podpis alebo kvalifikovanú elektronickú pečať vo formáte, ktorý nie je v súlade*** *s prílohou vykonávacieho aktu Komisie vydaného podľa čl. 27 ods. 5 a čl. 37 ods. 5 nariadenia (EÚ) č. 910/2014.*

Výnos o štandardoch pre IS VS č. 55/2014 Z.z.

Výnos o štandardoch pre IS VS č. 55/2014 Z.z. (už **od 15. októbra 2015** povinnosť prijímať a vytvárať ASiC)

§ 57b

Prijímanie a čítanie podpisových kontajnerov

Štandardom pre prijímanie a čítanie podpisových kontajnerov je prijímanie a čítanie

a) podpisového kontajneru vo formáte Associated Signature Containers (.asics, .scs, .asice, .sce) podľa osobitného predpisu11b) a podľa technických špecifikácií11ea) a to aj viacnásobne vnoreného, pričom vnorený kontajner môže byť aj formát ZIP podľa technickej špecifikácie11eb) alebo formát podľa § 25 ods. 1 písm. a) prvého bodu,

b) iných formátov podpisových kontajnerov ako uvedených v písmene a), ak sa na tom zasielateľ a prijímateľ dohodnú,

c) modulom centrálnej elektronickej podateľne externe podpísaných elektronických dokumentov alebo v ZEPf transportnom kontajneri obsahujúcom podpísaný dokument a jeho podpis CMS AdES alebo XML AdES podľa zverejnenej technickej špecifikácie11ec), pričom modul centrálnej elektronickej podateľne zabezpečuje aj overenie elektronického podpisu vyhotoveného podľa pravidiel platných do 30. júna 2016, ak takýto podpis strana spoliehajúca sa na podpis akceptuje; na overenie podpisov sa obsah transportného kontajnera ZEPf alebo samostatné podpisy a nimi podpísané dokumenty môžu uložiť do formátu ASiC, podľa písmena a),

d) priamo podpísaných elektronických dokumentov podľa § 57a písm. a), ktoré sú zároveň externe podpísanými elektronickými dokumentami v podpisových kontajneroch podľa písmena a).“

(pozn.: písm. c) a d) sa uplatňuje najneskôr od 1. júna 2019)

Výnos o štandardoch pre IS VS č. 55/2014 Z.z.

Výnos o štandardoch pre IS VS č. 55/2014 Z.z. (už **od 15. októbra 2015** povinnosť prijímať a vytvárať ASiC)

§ 57c

Vytváranie podpisových kontajnerov a podpísaných elektronických dokumentov

Štandardom pre vytváranie podpisových kontajnerov a podpísaných elektronických dokumentov podpísaných elektronickým podpisom alebo elektronickou pečaťou je

a) pri úkonoch súvisiacich s poskytovaním elektronických služieb verejnej správy, povinným poskytovaním informácií podľa osobitných predpisov, 3) alebo ak je podpísaním vykonaná autorizácia podľa osobitného predpisu, 11f) používanie formátov podľa § 57a písm. a) bodu 1, písm. b) bodov 1, 3 a 4, písm. c) a písm. e) a § 57b písm. a),

b) používanie iných formátov ako uvedených v písmene a), napríklad ostatných formátov podľa § 19 až 24, ak sa na tom všetky strany príslušnej komunikácie dohodnú, s vedomím možných škôd a nezrovnalostí v ďalšom konaní vyplývajúcich z takého postupu,

c) spravidla nevytváranie viacnásobne vnorených podpisových kontajnerov,

d) vytváranie formátov podľa písmena a) v súlade s validáciami podľa § 57e, ak je to preukázateľne a objektívne možné.
(pozn.: písm. d) sa uplatňuje najneskôr od 1. júna 2019)

Výnos o štandardoch pre IS VS č. 55/2014 Z.z.

§ 57a

Prijímanie a čítanie podpísaných elektronických dokumentov

Štandardom pre prijímanie a čítanie podpísaných elektronických dokumentov je prijímanie a čítanie

a) priamo podpísaných elektronických dokumentov vo formáte

1. textových súborov Portable Document Format podľa rozhodnutia Komisie EÚ11b) vo verzii A-1 (PDF/A-1) a A-2 (PDF/A-2) najmä podľa technickej normy11c)
2. textových súborov podľa § 19 písm. a) druhý bod , ak nejde o použitie na zaručenú konverziu podľa osobitného predpisu11ca),

b) externe podpísaných elektronických dokumentov vo formáte

1. textových súborov Portable Document Format vo verzii A-1 (PDF/A-1) a A-2 (PDF/A-2) najmä podľa technickej normy11c)
2. textových súborov podľa § 19 písm. a) druhý bod, ak nejde o použitie na zaručenú konverziu podľa osobitného predpisu11ca),
3. textových súborov podľa § 19 písm. a) tretieho bodu,
4. grafických súborov podľa § 20 písm. a) druhého bodu,

c) elektronických dokumentov vo formáte jazyka pre prenos dátových prvkov podľa § 12 v štruktúre podľa prílohy č. 11 (ďalej len „kontajner XML údajov“), pričom ak nejde o vyplnené údaje elektronického formulára, zároveň

1. sa v tomto elektronickom dokumente používa znaková sada podľa § 13 písm. c),
2. schéma tohto elektronického dokumentu je vytvorená v súlade s § 13 písm. a),
3. transformácia tohto elektronického dokumentu je vytváraná v súlade s § 13 písm. d) a zabezpečuje vytvorenie podpisovej prezentácie vo formáte podľa prílohy č. 3 bodu 2.6.7,

d) iných formátov elektronických dokumentov ako uvedených v písmenách a) až c), ak sa na tom zasielateľ a prijímateľ dohodnú,

e) formátov elektronických dokumentov podľa písmen a) až d) podľa § 57e, *(pozn.: písm. e) sa uplatňuje najneskôr od 1. júna 2019)*

f) ...

Výnos o štandardoch pre IS VS č. 55/2014 Z.z.

Výnos o štandardoch pre IS VS č. 55/2014 Z.z. (posledná novela opatrením 11/2018, aktuálne ďalšia po MPK)

Úpravy v oblasti podpisovania:

- 15. marca 2018
  - vypustenie povinného používania certifikovaných prostriedkov - v §57e
  - povolenie vytvárania PDF/A-1 a PDF/A-2 - v §57a
  - povinné prijímanie aj PDF 1.3 až 1.7 bez aktívnych prvkov
  - upresnenie povinnosti prijímať ZIP v ASiC (pôvodne „degradovaný ASiC“) – v §57b
- 1. júla 2018
  - identifikátor podpísaného elektronického dokumentu (MessageImprint) - v §57d
  - nové jednotné referencovateľné identifikátory (https://data.gov.sk/...) pre identifikáciu podpisových schém v podpisoch – s uplatňovaním od dátumu zverejneného na ÚPVS po dohode s ÚPPVII - v prílohe č. 11
- 1. júna 2019
  - povinnosť prijímať PAdES v ASiC – v §57b
  - povinnosť CEP prijímať a overovať ZEPf a XAdES_ZEP – v §57b
  - povinnosť prijímať a vytvárať formáty v súlade s validáciami predpísanými ÚPPVII - §57a a §57c

Sankcie za nedodržiavanie štandardov – od 2000 do 25000 EUR

Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy

„§ 10 Správne delikty

*(1) Ministerstvo **uloží pokutu***

*b) **od 2 000 eur do 25 000 eur** povinnej osobe, ktorá je správcom, ak poruší povinnosti ustanovené v § 3 ods. 4 písm. d), e) a i) .....“*

Povinnosť správcov:

*„i) zabezpečovať, aby bol informačný systém verejnej správy **v súlade so štandardmi** informačných systémov verejnej správy (ďalej len „štandardy“),“*

eIDAS vs Výnos o štandardoch pre IS VS

Nariadenie eIDAS

- nepredpisuje formáty podpisovaných dokumentov
- je nadradené národnej legislatíve
- problémy s interoperabilitou formátov dokumentov, snaha riešiť v budúcnosti, napr. eDelivery, identifikované štandardy ...

Výnos o štandardoch pre IS VS

- oblasti nepokryté v eIDAS alebo nejasne špecifikované
- zabezpečovanie interoperability a integrovateľnosti systémov

Zariadenie na vyhotovenie podpisu / pečate

eIDAS

- *„zariadenie na vyhotovenie kvalifikovaného elektronického podpisu“ je zariadenie na vyhotovenie elektronického podpisu, ktoré spĺňa požiadavky stanovené v prílohe II;*
- *„zariadenie na vyhotovenie kvalifikovanej elektronickej pečate“ je zariadenie na vyhotovenie elektronickej pečate, ktoré primerane spĺňa požiadavky stanovené v prílohe II;*

Zverejňovaný zoznam certifikovaných zariadení:

- *Qualified Signature Creation Device (QSCD)*
- *Qualified Seal Creation Device (QSCD)*

- *Secure Signature Creation Device (SSCD) (podľa pôvodnej legislatívy)*

https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

Zariadenie na vyhotovenie podpisu / pečate

PRÍLOHA II - POŽIADAVKY NA KVALIFIKOVANÉ ZARIADENIA NA VYHOTOVENIE ELEKTRONICKÝCH PODPISOV

1. Kvalifikované zariadenia na vyhotovenie elektronických podpisov musia vhodnými technickými a procedurálnymi prostriedkami zabezpečovať prinajmenšom, aby:

a) v primeranej miere bola zaručená dôvernosť údajov na vyhotovenie elektronického podpisu použitých na vyhotovenie elektronického podpisu;

b) ***sa údaje na vyhotovenie elektronického podpisu*** *použité na vyhotovenie elektronického podpisu mohli v praxi* ***objaviť iba raz****;*

c) údaje na vyhotovenie elektronického podpisu použité na vyhotovenie elektronického ***podpisu nebolo možné s primeranou úrovňou zabezpečenia odvodiť*** *a elektronický podpis bol spoľahlivo chránený proti falšovaniu pomocou aktuálne dostupných technológií;*

d) oprávnený podpisovateľ mohol údaje na vyhotovenie elektronického podpisu použité na vyhotovenie elektronického ***podpisu spoľahlivo chrániť pred použitím inými osobami****.*

2. Kvalifikované zariadenia na vyhotovenie elektronických podpisov ***nesmú meniť údaje, ktoré sa majú podpísať, ani brániť, aby sa takéto údaje podpisovateľovi pred podpísaním zobrazili****.*

3. Generovať alebo ***spravovať údaje na vyhotovenie elektronického podpisu v mene podpisovateľa môže výhradne kvalifikovaný poskytovateľ dôveryhodných služieb****.*

4. Bez toho, aby bol dotknutý bod 1 písm. d), kvalifikovaní poskytovatelia dôveryhodných služieb spravujúci údaje na vyhotovenie elektronického podpisu v mene podpisovateľa môžu údaje na vyhotovenie elektronického podpisu duplikovať len na účely zálohovania za predpokladu, že sú splnené tieto požiadavky:

a) bezpečnosť duplikovaných súborov údajov musí byť na rovnakej úrovni ako v prípade pôvodných súborov údajov;

b) počet duplikovaných súborov údajov nesmie prekročiť minimálne množstvo nevyhnutné na zabezpečenie kontinuity služby.

Certifikáty - vydávanie

- Generovanie kľúčového páru priamo na bezpečnom zariadení (napr. v čipe na smart karte), v HSM module (hardware security module), prípadne len softvérom (napr. OpenSSL)

- **Kľúčový pár je bez údajov o vlastníkovi – preto je potrebné overiť vlastníka a vydať certifikát**
  - Vytvorenie Certificate Signing Request (CSR) **s verejným kľúčom** a údajmi pre certifikát
  - Poskytovateľ dôveryhodnej služby / Certifikačná autorita (CA) overí identitu
  - Podpísanie certifikátu privátnym kľúčom poskytovateľa dôveryhodnej služby / CA
  - Uloženie vydaného certifikátu s kľúčovým párom (napr. na smart karte)

- Povinnosť chrániť privátny kľúč - ZEP PIN a pod.

Pečatenie na ÚPVS

- eIDAS - spravovanie údajov na vyhotovenie elektronického podpisu / pečate v mene podpisovateľa (autentifikácia pre prístup k HSM)
- NASES ako poskytovateľ dôveryhodných služieb od 14. januára 2018

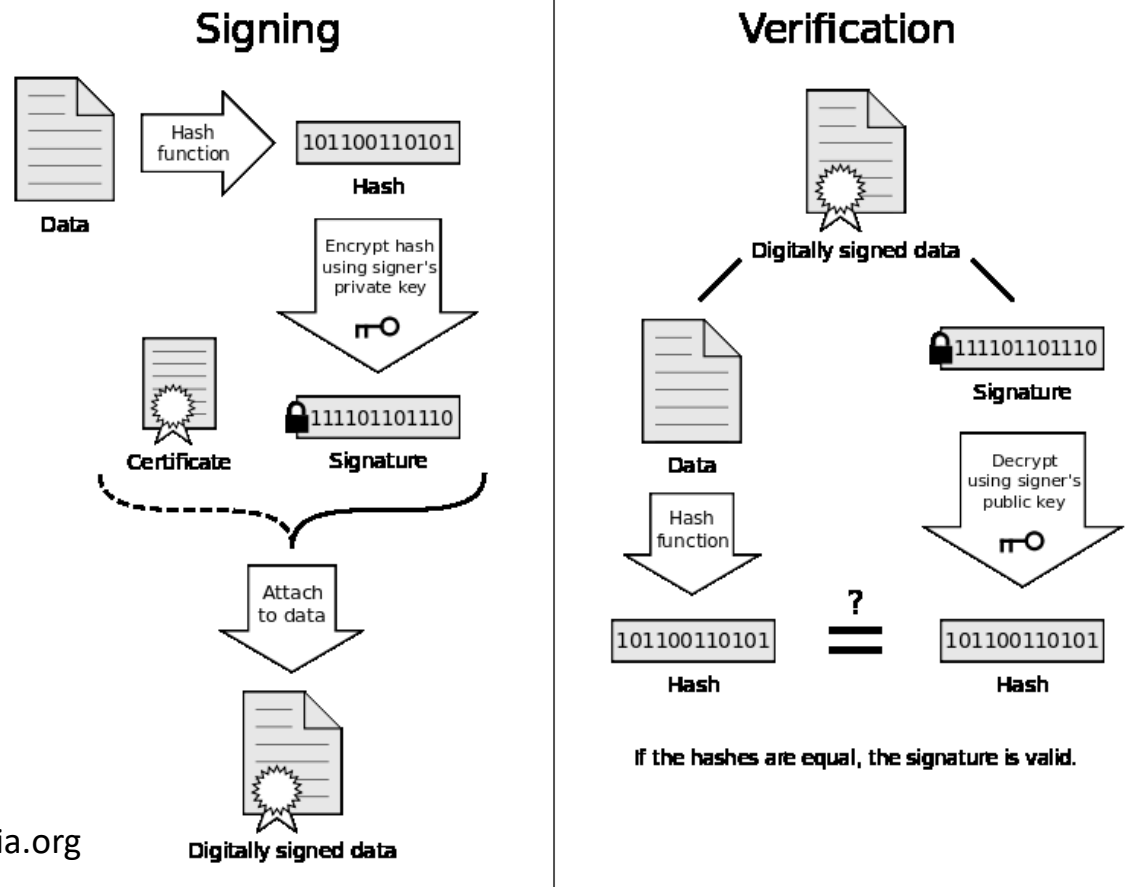
- HSM (Hardware Security Module)
  - musí spĺňať požadavky eIDAS
  - bezpečné generovanie kľúčových párov
    -> certificate signing request -> CA
    -> vydanie certifikátu podpísaného certifikačnou autoritou
  - bezpečné uchovávanie certifikátov a kľúčových párov

Pečate a podpisy s certifikátom bez príznaku QcSSCD/QcQSCD

- Pečate / podpisy vyhotovené s kvalifikovaným certifikátom, ktorý nemá príznak „QcSSCD“/ „QcQSCD“ sú len **zdokonalené elektronické pečate / podpisy**.
- Nejde teda o platnú autorizáciu podľa § 23 zákona č. 305/2013 Z.z.
- Odporúčame si kontrolovať, či kvalifikovaný certifikát vydaný v minulosti certifikačnou autoritou / poskytovateľom dôveryhodných služieb má tento príznak.
- NASES príznak nekontroluje.
- Vytváranie XAdES alebo CAdES pečatí v CEP umožní vytvorenie zdokonalenej elektronickej pečate.
- PAdES komponent na UPVS neumožňuje vytvorenie zdokonalenej pečate.

Asymetrické šifrovanie – verejným kľúčom - podpisovanie

Šifrovanie privátnym kľúčom a dešifrovanie verejným kľúčom
(napr. **podpisovanie**)



Zdroj obrázka: commons.wikimedia.org

Certifikát s príznakom QcSSCD/QcQSCD

Rozdiel v certifikátoch, ktoré majú alebo nemajú potrebný príznak QcSSCD vyžadovaný v kvalifikovanom podpise/pečati je možné zistiť zo súboru certifikátu (.cer) napríklad nasledovne:

1. spôsob:

Napríklad cez aplikáciu LockIt od NBÚ (cez menu "Info" / "Ukáž DER alebo BER dump"), kde je v zozname rôznych vlastností certifikátu vidieť aj toto:

SEQUENCE {
OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.3 qcStatements
OCTET STRING, encapsulates {
SEQUENCE {
SEQUENCE {
OBJECT IDENTIFIER 0.4.0.1862.1.1 etsiQcsCompliance
}
SEQUENCE {
OBJECT IDENTIFIER 0.4.0.1862.1.4 etsiQcsQcSSCD

Certifikát s príznakom QcSSCD/QcQSCD

2. spôsob:

V podrobnostiach certifikátu pečate je po otvorení certifikátu v MS Windows v záložke "Podrobnosti" v položke "Výpisy platných certifikátov" (uvedené v tzv. hexadecimálnej forme):

- Príznak QcCompliance - OID 0.4.0.1862.1.1 je uvedený v podobe: 06 06 04 00 8E 46 01 01

- Príznak QcSSCD/QcQSCD - OID 0.4.0.1862.1.4 je uvedený v podobe: 06 06 04 00 8E 46 01 04

V certifikáte s QcCompliance avšak bez QcSSCD/QcQSCD je uvedené : 30 14 30 08 06 06 04 00 8E 46 01 01

V certifikáte, ktorý má uvedené QcCompliance a aj QcSSCD/QcQSCD je uvedené: 30 14 30 08 06 06 04 00 8E 46 01 01 30 08 06 06 04 00 8E 46 01 04

Ide o hodnoty predpísané podľa:

Kapitola 5.2.3 v Schéme dohľadu NBÚ:

http://ep.nbu.gov.sk/kca/tsl/SchemaDohladu.pdf

Tabuľka T1 riadok T1.I,III,IV (a). , Tabuľka T1 riadok T1.I,III(j).

Formáty podpisov a spôsob ich prenosu

Formáty podpisov a podpisových kontajnerov

Formáty podpisov / podpisových kontajnerov používané v SR podľa legislatívy do 30. 6. 2016:

XAdES_ZEP - .xzep, .zepx

ZEPf (CAdES) - .zep

PAdES - .pdf (povinná podpisová politika, vyžaduje CMS AdES, neuzná sa PKCS1 a PKCS7)

Formáty podpisov a podpisových kontajnerov podľa eIDAS od 1. júla 2016:

Kontajnery:

ASiC-E - .asice, .sce, .zip

ASiC-S - .asics, .scs, .zip

Podpisy:

XAdES - .xml

CAdES - .p7s, .p7m

PAdES - .pdf (nie je povinná podpisová politika)

Formáty podpisov a podpisových kontajnerov

Formáty podpisov :

XAdES_ZEP	- .xzep, .zepx	- v rozpore s eIDAS
XAdES	- .xml	
CAdES	- .p7s, .p7m	
PAdES	- .pdf	

Formáty podpisových kontajnerov:

ZEPf	- .zep	- v rozpore s eIDAS je len ZIP adresárová štruktúra a prípona
ASiC-E	- .asice, .sce, .zip	
ASiC-S	- .asics, .scs, .zip	

Formáty časových pečiatok

Časová pečiatka dokumentu:

Time stamp - .tst

- obsahuje CAdES podpis údaja o čase (súbor TSInfo) a digitálneho odtlačku dokumentu

Používa sa napríklad na samostatný dokument:

- *subor.pdf*
- *subor.pdf.tst* *(časové pečiatka)*

Časová pečiatka podpisu, integrity podpisu (aj obsahu a dokumentu) - sa ukladá do štruktúry podpisu

XAdES - .xml

CAdES - .p7s, .p7m

PAdES - .pdf

Spôsob prenosu podpisov

CAdES, XAdES, PAdES - formáty a varianty

Spôsob prenosu podpisov:

- Detached – XAdES, CAdES
- Enveloping – XAdES, CAdES
- Enveloped – XAdES, PAdES

- CAdES sa označuje aj ako interný/externý
- PAdES ako sériový či sekvenčný

Podpis - **detached (externý)**

Podpis je samostatný súbor, oddelený od podpisovaného dokumentu.

CAdES

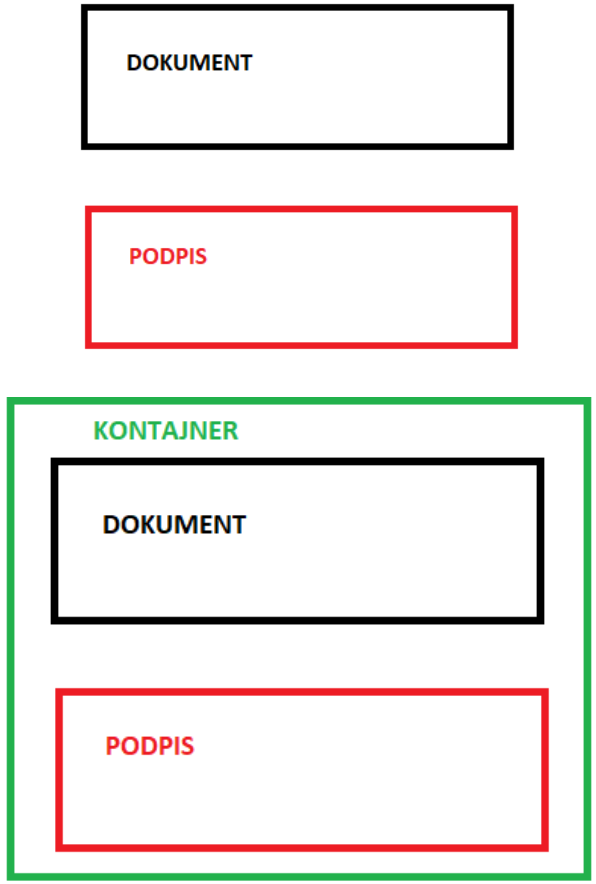
- Dokument.pdf (príklad)
- Dokument.pdf.p7s (príklad)

XAdES

- Dokument.pdf (príklad)
- podpis.xml (príklad)

<u>Vhodné prenášať v podpisovom kontajneri</u>

- **ASiC**
- **ZEPf** - nesúladná s eIDAS je ZIP adresárová štruktúra aj prípona
- XAdES_ZEP - v rozpore s eIDAS



Podpis - **enveloped (obalený)**

Podpis je v podpisovanom dokumente ako jeho súčasť (obalený dokumentom).

XAdES

- Dokument.xml (príklad)

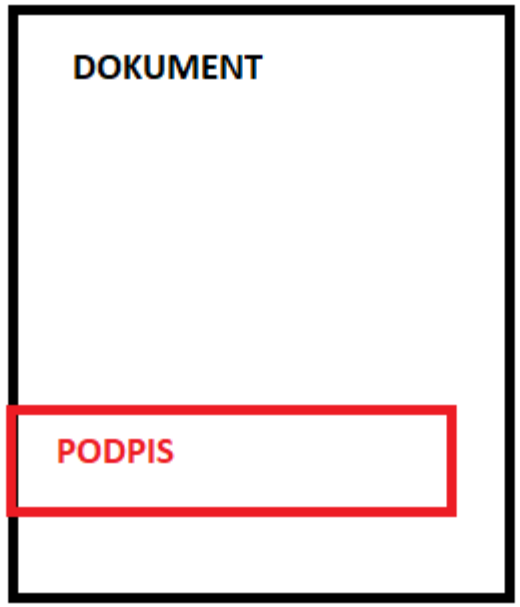
Ide o menej rozšírený spôsob prenosu podpisu XAdES.

Použiteľný len pre XML dokument. (napr. dôveryhodný zoznam)

PAdES (obvykle neoznačovaný ako „enveloped“)

- Dokument.pdf (príklad)

V praxi rozšírený spôsob podpisovania.



Podpis - **enveloping (obaľujúci)**

Podpis obaľuje podpisovaný dokument.

XAdES

- Dokument.xml (príklad)

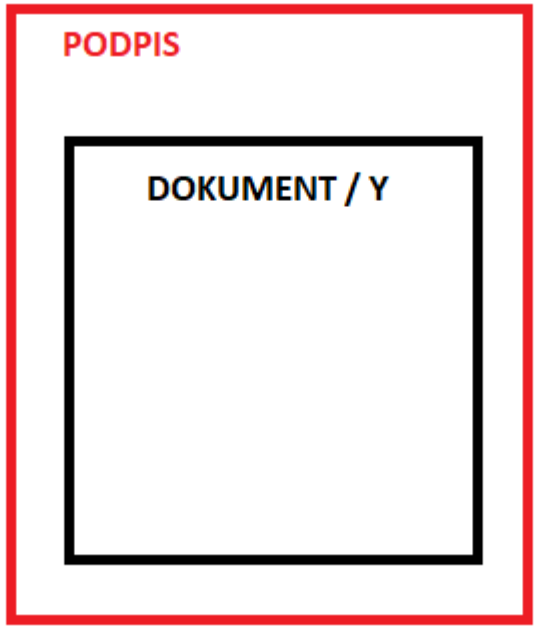
Ide o menej rozšírený spôsob prenosu podpisu XAdES.

CAdES

- Dokument.p7m (príklad)

Ide o rozšírený spôsob prenosu podpisu CAdES.

Použitý napr. v podpísanej elektronickej pošte (S/MIME)



CAdES, XAdES, PAdES - formáty

	XAdES	**CAdES**	**PAdES**
Enveloped: Podpis je vo vnútri podpisovaného dokumentu	Áno .xml, ... (iba v XML)	Áno * (používa sa v S/MIME – elektronická pošta)	Áno .pdf
Enveloping: Podpis obaľujúci dokument	Áno .xml, ...	Áno .p7m, ...	Nie
Detached: Podpis ako samostatný súbor	Áno .xml, ...	Áno .p7s, ...	Nie

CAdES, XAdES, PAdES - formáty v CEP

Centrálna elektronická podateľňa svojimi službami v súčasnosti **nepodporuje prijímanie a vytváranie**:

- XAdES a CAdES enveloping
- XAdES enveloped
- XAdES a CAdES detached, ak nie sú v podpisovom kontajneri

Podpora sa zvažuje do budúcna.

Podporované formáty v CEP

Dokumentácia CEP:

1. Integračný manuál na Partner framework portáli

2. Zverejnená dokumentácia, ktorá dopĺňa integračný manuál
https://www.slovensko.sk/_img/CMS4/Dokumentacia_funkcnosti_CEP.pdf

ASiC

application/vnd.etsi.asic-e+zip - .asice, .sce, .zip
application/vnd.etsi.asic-s+zip - .asics, .scs, .zip

Podpisové kontajnery – ASiC

Čo je ASiC?

- **ZIP** súbor - môžete ho rozbaliť cez aplikácie na prácu so ZIP a získať tak podpísaný súbor
- obsahuje dokumenty, podpisy/pečate (XAdES alebo CAdES) a / alebo časové pečiatky + môže obsahovať metaúdaje
- štruktúrou zhodný s existujúcimi formátmi .ODT, .EPUB, ...
- **predpísaný eIDAS od roku 2016** (v štandardoch pre IS VS od októbra 2015)
- zatiaľ málo rozšírený

- paralelné podpisy (obvykle) - pri opakovanom podpise sa podpisuje samotný dokument, nezávisle od predošlého podpisu
- spoločná autorizácia viacerých dokumentov, aj rôzne podmnožiny

Podpisové kontajnery – ASiC

Varianty ASiC:

- ASIC-S (.asics, .scs, .zip) – podpísaný (a časovo opečiatkovaný) **jeden objekt**
- ASiC-E (.asice, .sce, .zip) – podpísaný (a časovo opečiatkovaný) **jeden alebo viacero objektov**

Podľa použitého formátu podpisu / pečate:

XAdES

- ASiC-S XAdES
- ASiC-E XAdES

CAdES

- ASiC-S CAdES
- ASiC-E CAdES

Podpisové kontajnery – ASiC - Time stamp

Varianty ASiC:

- ASIC-S (.asics, .scs, .zip) – časová pečiatka **pre jeden objekt**
- ASiC-E (.asice, .sce, .zip) – časová pečiatka **pre jeden alebo viacero objektov**

Ak obsahuje len časovú pečiatku dokumentu bez podpisu:

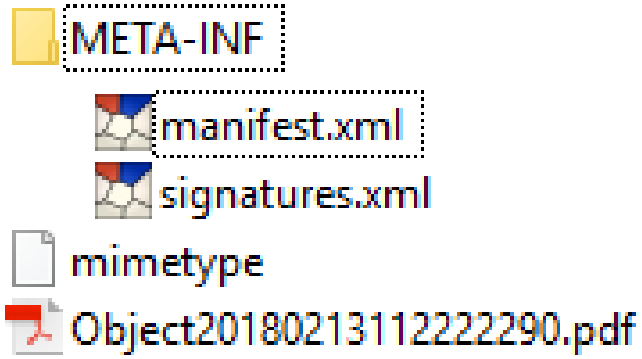
- ASiC-S Time stamp token
- ASiC-E Time stamp token

    - RFC 3161 Time stamp protocol

Podpisové kontajnery – ASiC-E XAdES

Príklad štruktúry obsahu ASiC-E XAdES - podpísaný jeden PDF súbor

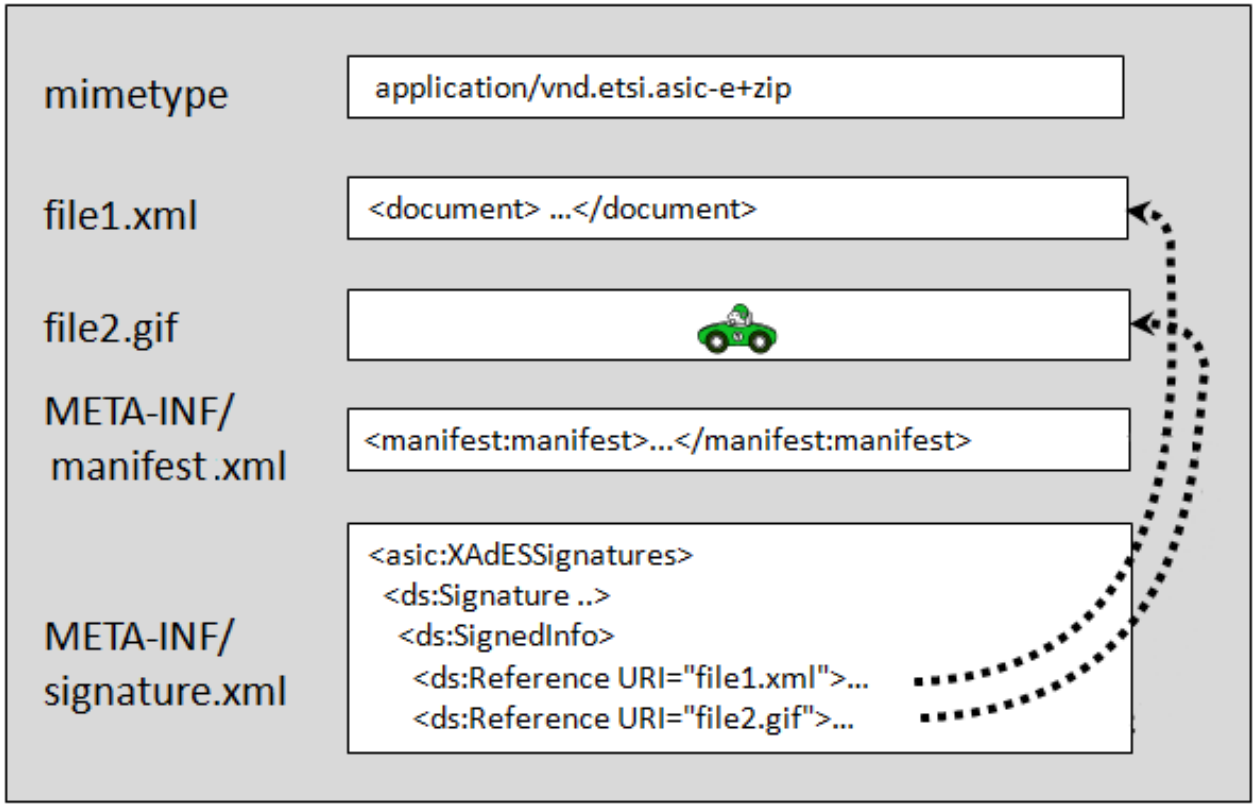
priklad.asice



Podpisové kontajnery – ASiC-E XAdES - príklad

Príklad štruktúry obsahu ASiC-E XAdES – podpísané dva súbory jedným podpisom/pečaťou

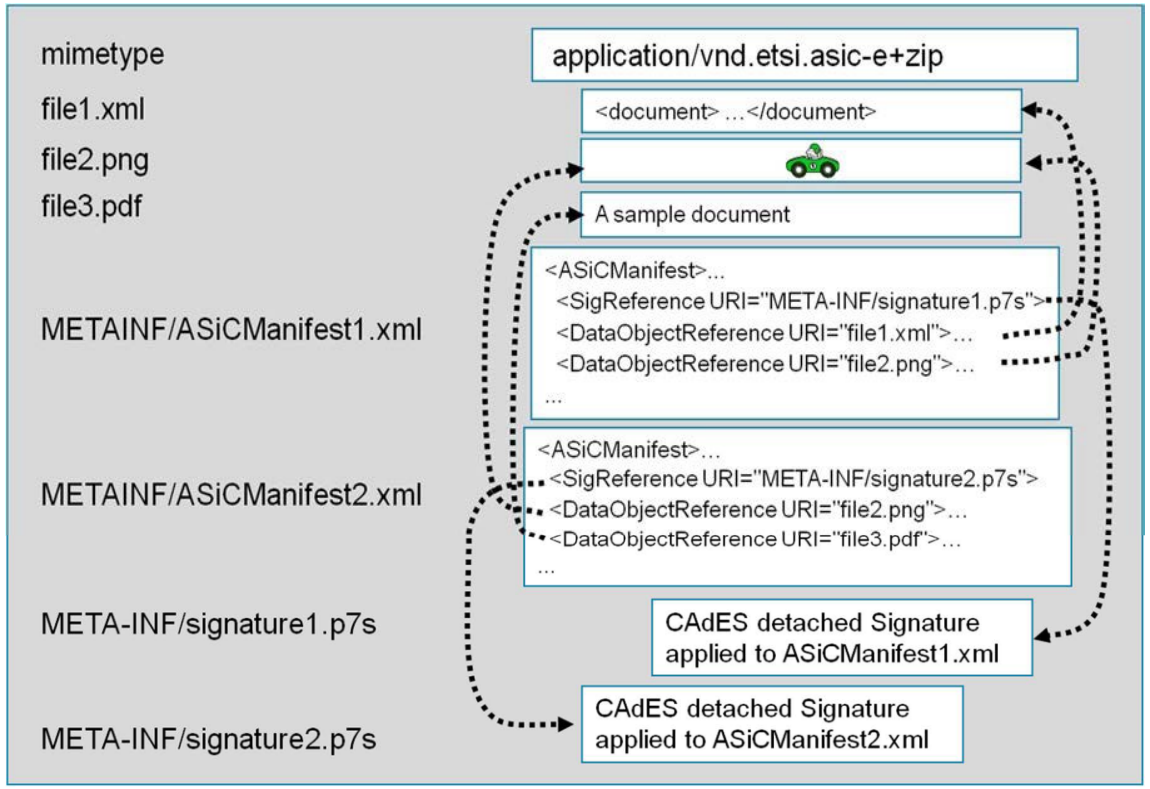
(zdroj obrázku: ETSI EN)



Podpisové kontajnery – ASiC-E CAdES - príklad

Príklad štruktúry obsahu ASiC-E XAdES – podpísané tri súbory dvoma podpismi/pečaťami

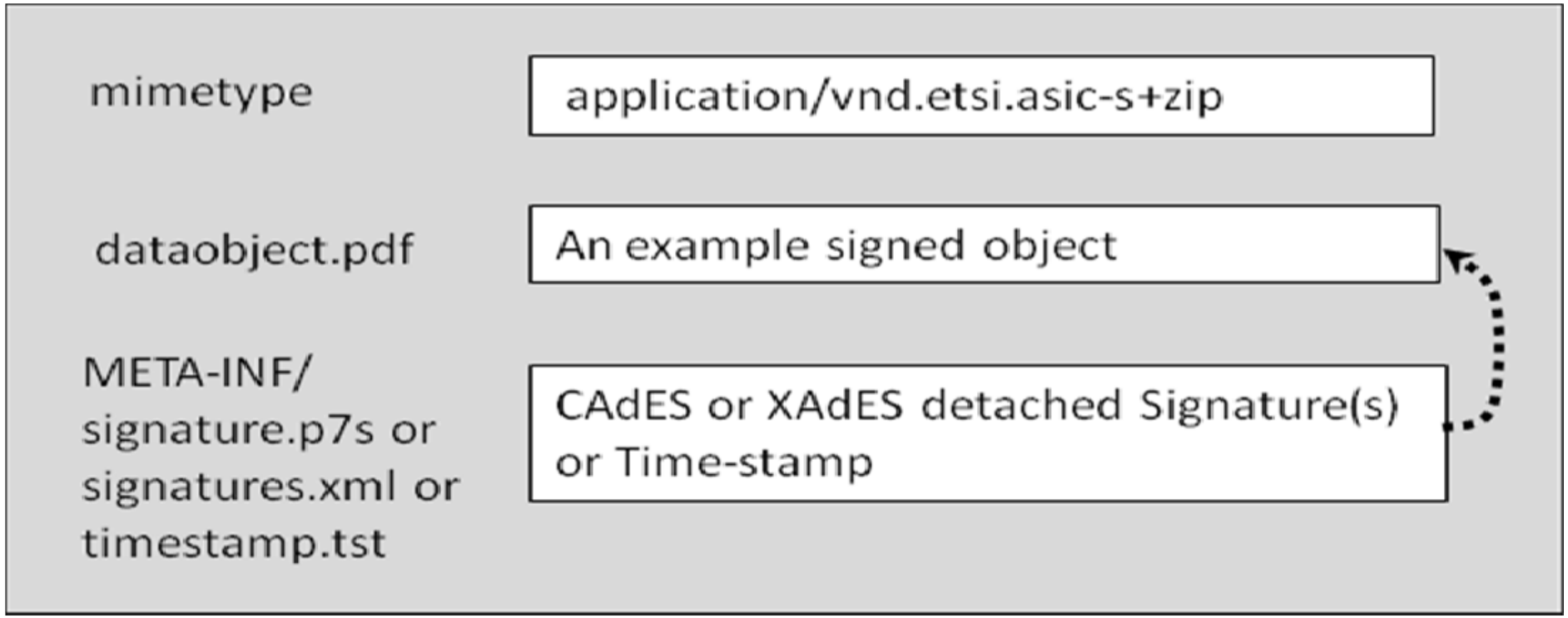
(zdroj obrázku: ETSI EN)



Podpisové kontajnery – ASiC-S - príklad

Príklad štruktúry obsahu ASiC-S – podpísaný jeden PDF súbor podpisom/pečaťou

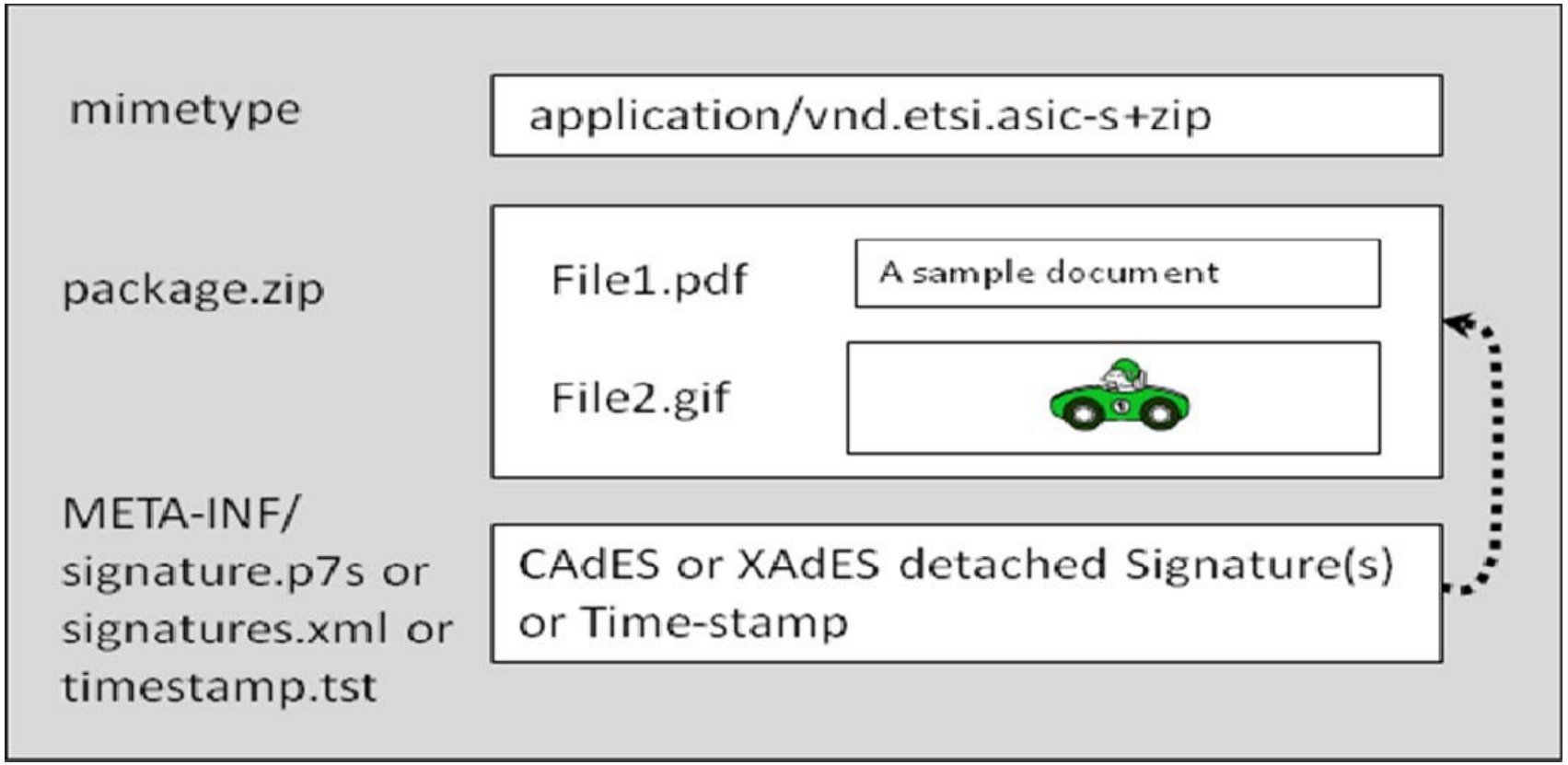
(zdroj obrázku: ETSI EN)



Podpisové kontajnery – ASiC-S - príklad

Príklad štruktúry obsahu ASiC-S – podpísaný jeden ZIP súbor podpisom/pečaťou

(zdroj obrázku: ETSI EN)



ZEPf (.zep)

application/zep
application/x-zipzepf

Podpisové kontajnery - ZEPf

Čo je ZEPf?

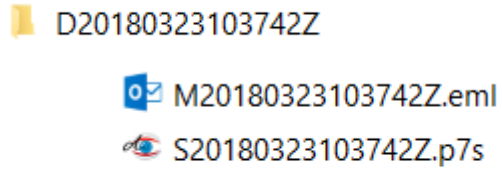
- **ZIP** súbor (.zep) - môžete ho rozbaliť cez aplikácie na prácu so ZIP a získať tak podpísaný súbor
- obsahuje dokumenty, podpisy/pečate a časové pečiatky + môže obsahovať iné údaje
- dokument obvykle vložený v jednom **.eml súbore** (prípustné aj iné možnosti)

- **špecificky slovenský**, používaný cca od roku 2004
  - **obsahuje CAdES podpis v súlade eIDAS** (môže obsahovať aj XAdES, v praxi taký variant nepoužívaný)
  - bezstratovo konvertovateľný do ASiC (bez potreby zaručenej konverzie), čo zjednodušuje overovanie podpisu/pečate, dokument však zostáva v .eml súbore, čo komplikuje jeho spracovanie
  - kontajner ZEPf nie je v súlade s eIDAS ale je jednoducho spracovateľný
- paralelné podpisy (obvykle) pri viacnásobnej autorizácii
- spoločná autorizácia viacerých dokumentov (vložené v jednom .eml), nie však podmnožiny,
  - v praxi často nepodporované

Podpisové kontajnery - ZEPf – príklad

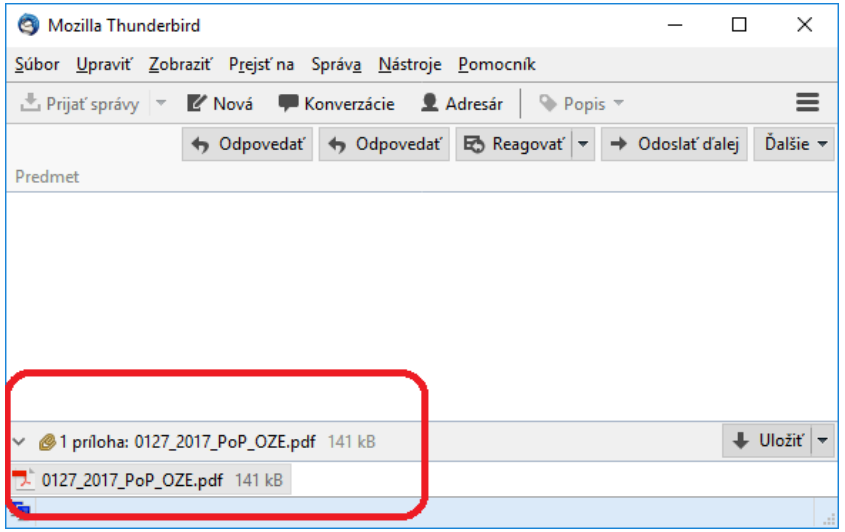
Príklad štruktúry ZEPf s podpísaným jedným PDF súborom

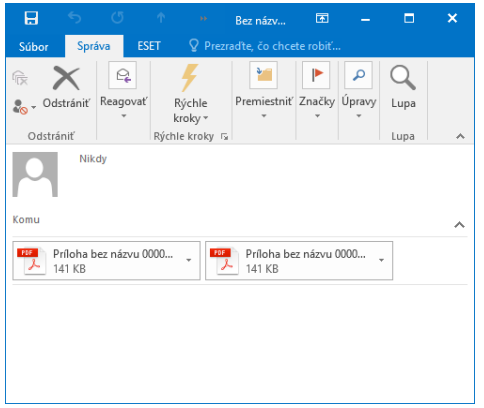
priklad.zep



.eml súbor sa dá otvoriť v e-mailovom klientovi:

(Thunderbird, Outlook)





XAdES_ZEP (.xzep, .zepx)

application/x-xades_zep
application/x-xades_zep_data_signatures
application/zepx

Podpisové formáty – XAdES_ZEP

Čo je XAdES_ZEP?

- **XML** súbor (.xzep, .zepx) - pre získanie podpísaného súboru potrebný softvér
- obsahuje dokumenty, podpisy/pečate a časové pečiatky

- **špecificky slovenský**, používaný cca od roku 2005
  - založený na XAdES 1.3.2 / 1.4.2 ale vyžaduje požiadavky nad jeho rámec, preto nie je v zahraničí plne podporovaný
  - vyžaduje vlastné požiadavky napr. pre ds.Manifest, ktoré aplikácia spoliehajúcej sa strany nemá ako poznať, preto nie je určený pre kvalifikovaný elektronický podpis pre tretie strany, je nepodporovaný v zahraničí a mimo SK eGov
  - v rozpore s eIDAS
  - nie je konvertovateľný do eIDAS formátov bez zaručenej konverzie

- paralelné podpisy (obvykle) pri viacnásobnej autorizácii
- spoločná autorizácia viacerých dokumentov, aj podmnožiny dokumentov

Podpisové formáty – XAdES_ZEP - príklad

```
175  </ds:SignedInfo>
176  <ds:SignatureValue Id="signatureId22276287SignatureValue">LAFcmxhpk9M+FDyPj4xTDj1RAx5QDe/Wl8AKfB+cW+qdyc8KvwnbYf9e
177  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xzep="http://www.ditec.sk/ep/signature_formats/xades_zep/v1.1" Id="
178   <ds:X509Data>
179    <ds:X509Certificate>MIIIJDCCBgygAwIBAgIKBITMaVUxARbvBDANBgkqhkiG9w0BAQsFADBmMQswCQYDVQQGEwJTSzETMBEGA
180    <ds:X509IssuerSerial>
181     <ds:X509IssuerName>CN=SVK eID ACA, OU=ACA-307-2007-2, O=Disig a.s., L=Bratislava, C=SK</ds:X509IssuerName>
182     <ds:X509SerialNumber>213391655469334936245 80</ds:X509SerialNumber>
183    </ds:X509IssuerSerial>
184    <ds:X509SubjectName>SERIALNUMBER=PNOSK-8008098142, C=SK, L=Bratislava-Nové Mesto, STREET=Chrasťová 1840/13, SN=I
185   </ds:X509Data>
186  </ds:KeyInfo>
187  <ds:Object>
188   <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" Target="#signatureId22276287">
189    <xades:SignedProperties xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" xmlns:xzep=
190     <xades:SignedSignatureProperties>
191      <xades:SigningTime>2018-05-07T13:23:38+02:00</xades:SigningTime>
192      <xades:SigningCertificate>
193       <xades:Cert>
194        <xades:CertDigest>
195         <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
196         <ds:DigestValue>lp6Xg8EQiwGWPvA9Yj61rHSThRNQVmdlty7elNG5NAE=</ds:DigestValue>
197        </xades:CertDigest>
198        <xades:IssuerSerial>
199         <ds:X509IssuerName>CN=SVK eID ACA, OU=ACA-307-2007-2, O=Disig a.s., L=Bratislava, C=SK</ds:X509IssuerName>
200         <ds:X509SerialNumber>213391655469334936245 80</ds:X509SerialNumber>
```

PAdES (.pdf)

application/pdf

Podpisové formáty - PAdES

Čo je PAdES?

- **PDF** súbor (.pdf)
- PDF dokument priamo v sebe obsahuje podpisy/pečate a časové pečiatky
- **predpísaný eIDAS od 1. júla 2016**
- súčasť PDF 2.0 (ISO 32000-2:2017) – plne, PDF 1.7 (ISO 32000-1:2008) - čiastočne
- v praxi rozšírené (od 2009), existujú rôzne staršie varianty (od r. 2000), ktoré nie sú PAdES
- len sériové podpisy pri viacnásobnej autorizácii

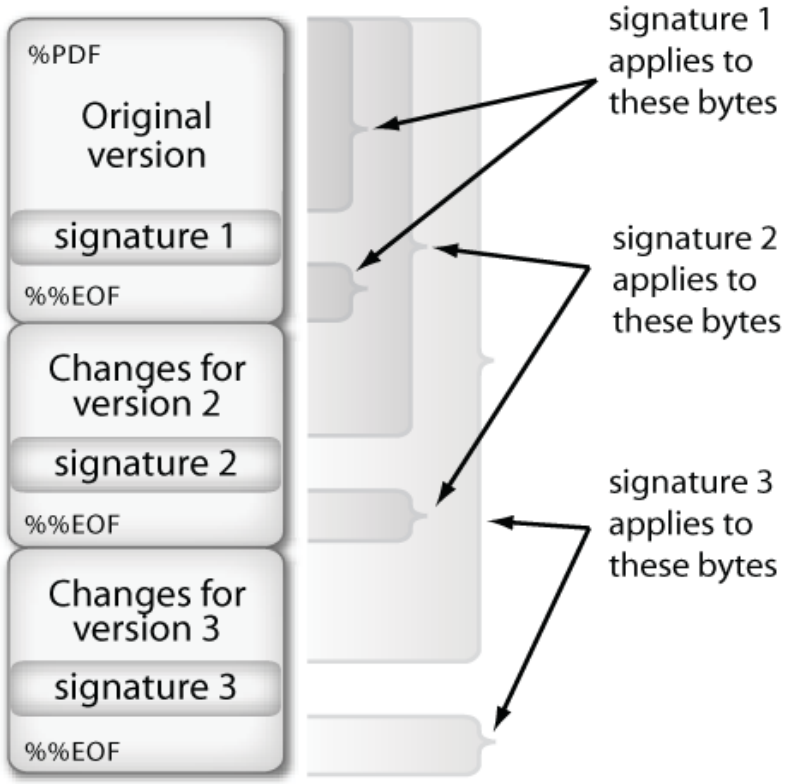
Praktické problémy:

- vo väčšine PDF prehliadačov vôbec nezistíte, že dokument obsahuje podpis
- v PDF prehliadači vidíte podobu dokumentu po poslednom podpise,
- v prípade viacnásobného podpisu sa podpisuje dokument vrátane predošlých podpisov,
  - nie je preto podľa dodávateľov 100% možné automatizované porovnanie, či všetci podpísali rovnaký obsah

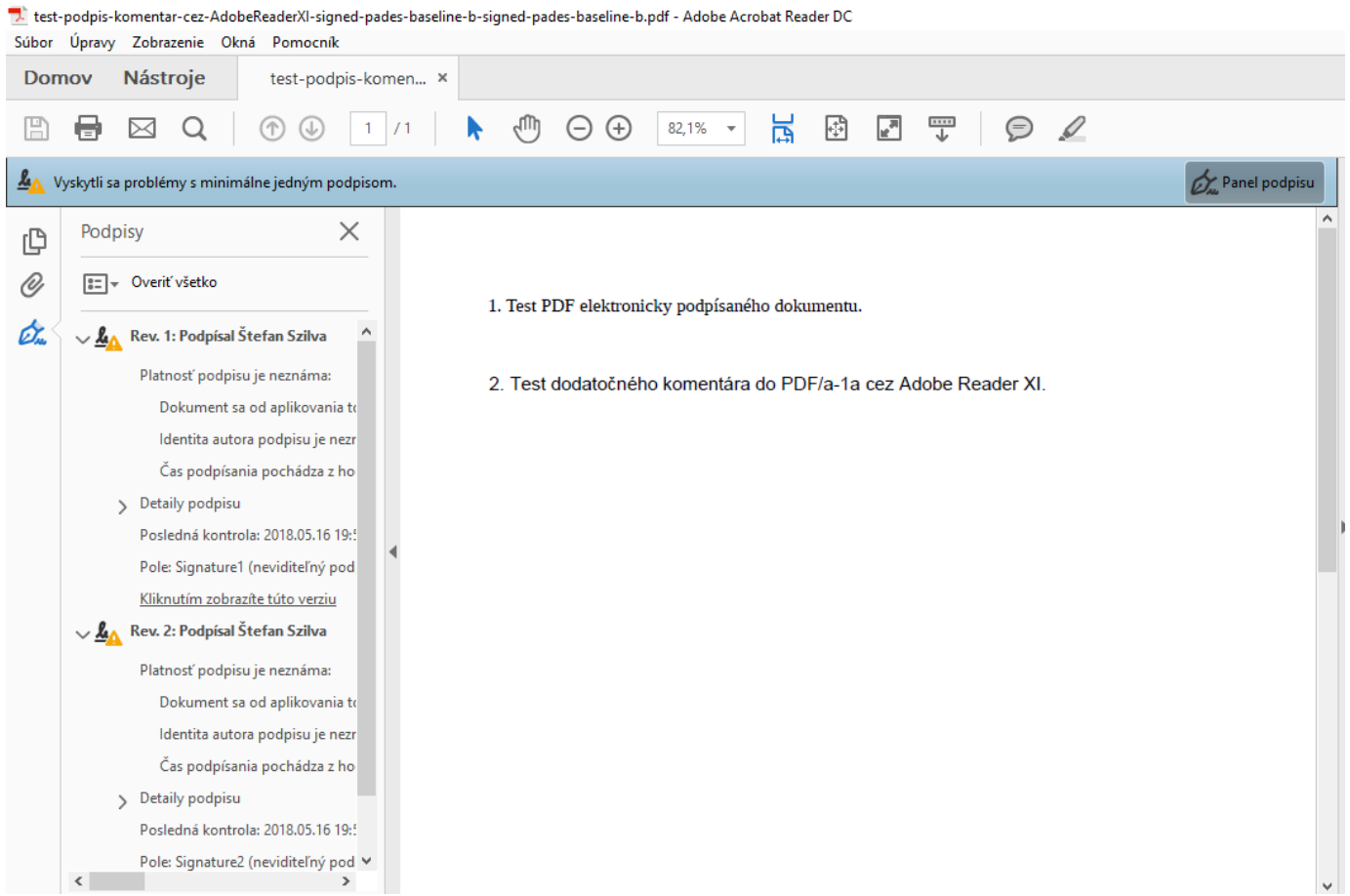
Podpisové formáty - PAdES

- Viacnásobný podpis:
  Sekvenčný podpis – každý PAdES (podpis alebo časová pečiatka dokumentu) zabezpečí okrem posledných zmien v PDF súbore (napr. zmeny v PDF formulári pred podpisom) aj všetky predchádzajúce podpisy v PDF súbore.

(zdroj obrázku: ETSI TS 102 778-1)



Podpisové formáty - PAdES - príklad



Podpisové kontajnery / podpisy

	XAdES eIDAS	**CAdES eIDAS**	**PAdES eIDAS**	**XAdES_ZEP**	**ZEPf (CAdES)**
Formáty dokumentov	Akékoľvek *	Akékoľvek *	PDF	Akékoľvek * (vyhláška 136/2009 Z.z.)	Akékoľvek * (vyhláška 136/2009 Z.z.)
Viacnásobný podpis identického dokumentu	Áno paralelné podpisy*	Áno paralelné podpisy*	Nie * sériové podpisy	Áno paralelné podpisy	Áno paralelné podpisy*
Spoločná autorizácia viacerých dokumentov	Áno * potrebný kontajner / štruktúra	Áno * potrebný kontajner / štruktúra	Nie * len dáta ako súčasť dokumentu	Áno * v praxi menej podporovaná	Nie * možná ale v praxi nepodporovaná (komerčné aplik.)
Grafická reprezentácia podpisu v dokumente	Nie * len neštandardné riešenia	Nie * len neštandardné riešenia	Áno * len nepovinná možnosť	Nie * len neštandardné riešenia	Nie * len neštandardné riešenia

Podpisové kontajnery / podpisy

Centrálna elektronická podateľňa podporuje podpisovanie len niektorých formátov dokumentov:

- **TXT - Plain Text Format** (.txt) - mimetype: text/plain
- **PDF - Portable Document Format** (.pdf) len vo verzii 1.3 alebo 1.4 - mimetype: application/pdf
- **XML - Extensible Markup Language** (.xml) - mimetype: text/xml (nepodporovaný pri ASiC-CAdES) – Výnos o štandardoch vyžaduje jeho vloženie do XMLDataContainer
- **PNG - Portable Network Graphics** (.png) - mimetype: image/png
- **XMLDataContainer** (.xml) - mimetype: application/vnd.gov.sk.xmldatacontainer+xml (nepodporovaný pri ASiC CAdES)

Zdroj: dokumentácia CEP - https://www.slovensko.sk/_img/CMS4/Dokumentacia_funkcnosti_CEP.pdf

Viacnásobné podpisy

Podpis – **paralelný**

Každý podpis podpisuje dokumenty

bez predchádzajúcich podpisov

CAdES

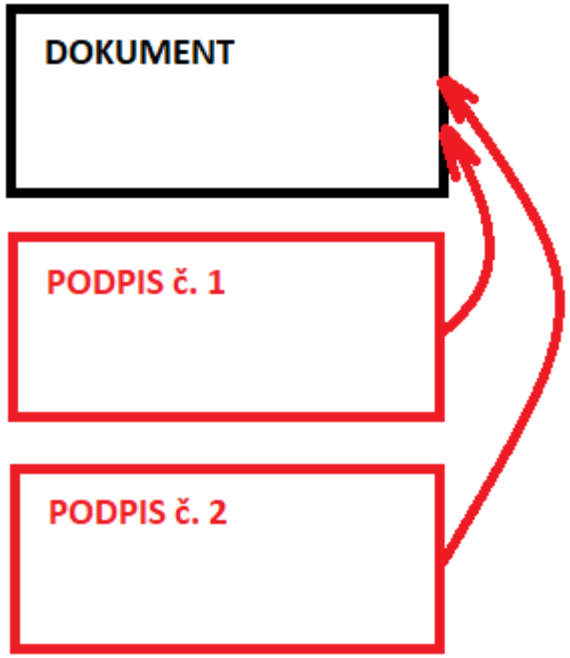
XAdES

XAdES_ZEP – v rozpore s eIDAS

<u>Vhodné prenášať v podpisovom kontajneri</u>

ASiC

ZEPf - nesúladná s eIDAS je ZIP adresárová štruktúra a prípona



Podpis – **paralelný**

Každý podpis podpisuje dokumenty
bez predchádzajúcich podpisov

CAdES

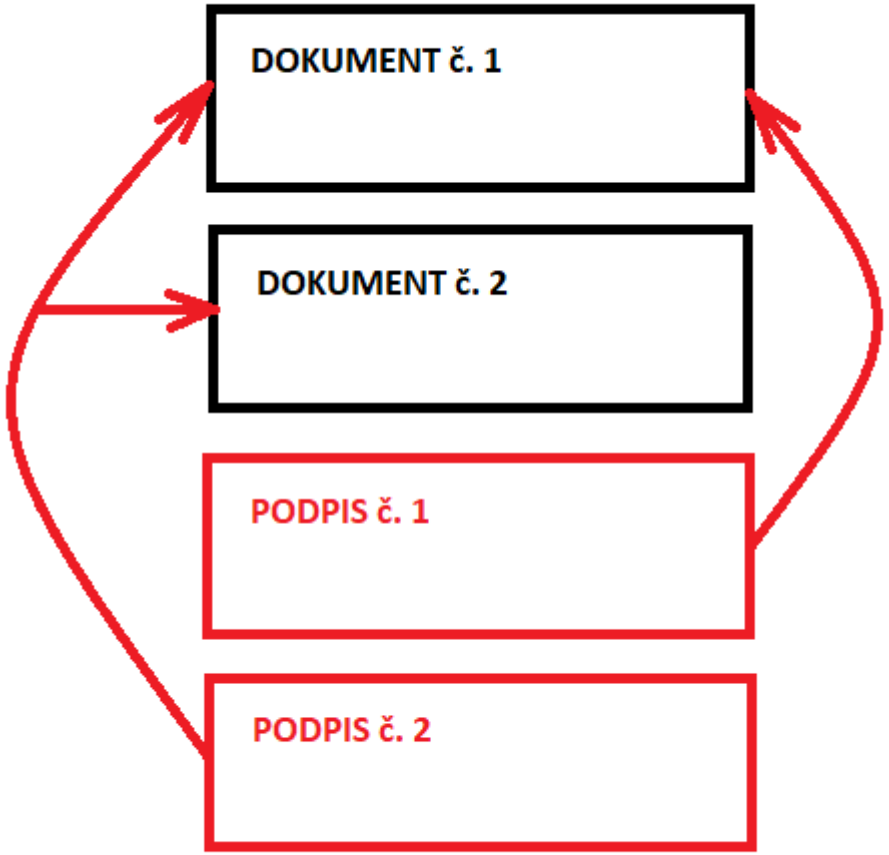
XAdES

XAdES_ZEP – v rozpore s eIDAS

<u>Vhodné prenášať v podpisovom kontajneri</u>

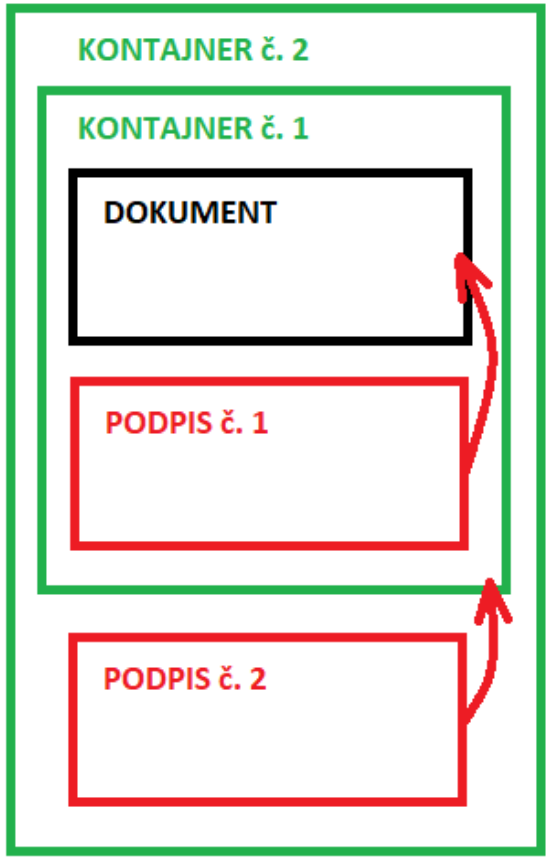
ASiC

ZEPf - nesúladná s eIDAS je ZIP adresárová štruktúra a prípona



Podpis – **sériový (vnorený)**

Každý ďalší podpis podpisuje dokument **vrátane predchádzajúcich podpisov** (podpisovaný objekt vo svojom vnútri obsahuje predchádzajúci podpis)



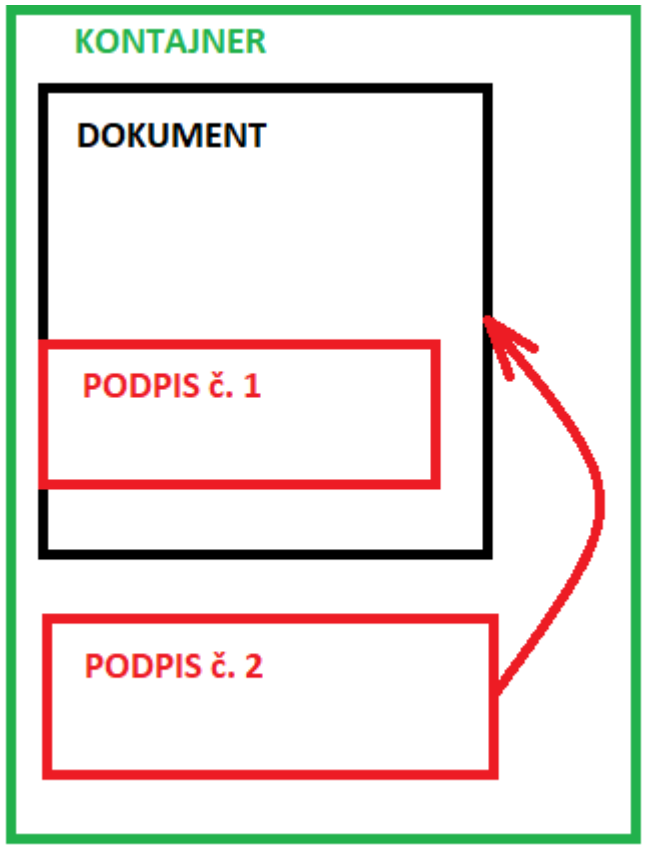
ASiC v ASiC

- Dokument.asice (príklad)

Podľa legislatívy sa **spravidla nemá vytvárať**

Podpis – **sériový (vnorený)**

Každý ďalší podpis podpisuje dokument **vrátane predchádzajúcich podpisov** (podpisovaný objekt vo svojom vnútri obsahuje predchádzajúci podpis)



ASiC obsahujúci PDF s PAdES

- Dokument.asice (príklad)

Podpis – **sériový (vnorený) - PAdES**

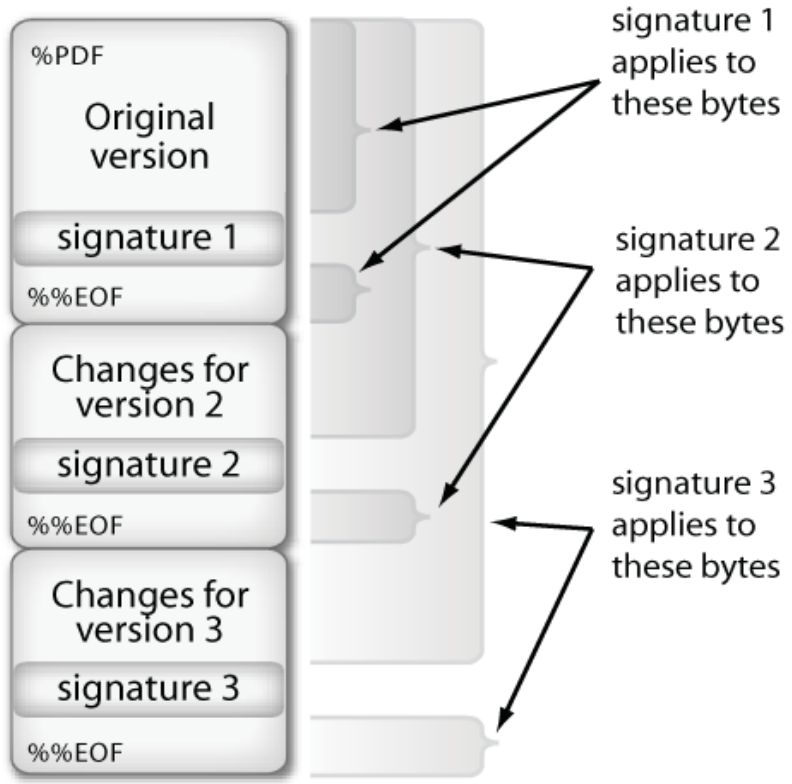
Každý ďalší podpis podpisuje dokument **vrátane predchádzajúcich podpisov** (podpisovaný objekt vo svojom vnútri obsahuje predchádzajúci podpis)

PAdES

- Dokument.pdf (príklad)

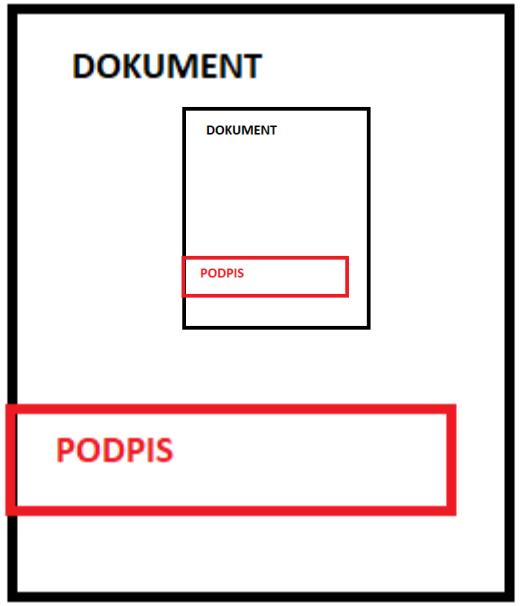
Rozšírený spôsob podpisovania.

(obrázok skopírovaný z ETSI TS 102 778-1)



Podpis – **sériový (vnorený) - PAdES**

Každý ďalší podpis podpisuje dokument
vrátane predchádzajúcich podpisov
(podpisovaný objekt vo svojom
vnútri obsahuje predchádzajúci podpis)



PAdES

- Dokument.pdf (príklad)

Rozšírený spôsob podpisovania.

Opakovaná / Spoločná autorizácia – CEP

Odporúčame nevytvárať vnorené kontajnery, kým ich CEP nebude podporovať.

Plánuje sa podpora pre vnorené kontajnery na prelome 2018/2019 (presný termín nie je určený)

CEP **neposkytuje** vo výsledku predbežného ani úplného overenia výsledok overenia pre:

- Podpisy vo vnorených kontajneroch
- PAdES v ASiC alebo v XAdES_ZEP

Opakovaná / Spoločná autorizácia

Výnos o štandardoch pre IS VS č. 55/2014 Z.z. (Posledná novela - opatrenie 11/2018)

§ 57c
„c) spravidla nevytváranie viacnásobne vnorených podpisových kontajnerov“

§ 57a
prijímanie a čítanie
***„a)* priamo podpísaných elektronických dokumentov vo formáte ...“**

... PDF/A-1, PDF/A-2, PDF 1.3 až 1.7 bez aktívnych prvkov

„f) podpísaných elektronických dokumentov podľa písmena a) podpísaných viacerými osobami, iba ak tieto osoby podpísali rovnaký informačný obsah elektronického dokumentu,“

g) podpísaných elektronických dokumentov podľa písmena a) podpísaných viacerými osobami, ak niektorá z týchto osôb podpísala iný informačný obsah tohto elektronického dokumentu ako ostatné osoby, ak sa o tom zasielateľ a prijímateľ dohodnú

Opakovaná / Spoločná autorizácia

Výnos o štandardoch pre IS VS č. 55/2014 Z.z.

§ 57b

Prijímanie a čítanie podpisových kontajnerov

Štandardom pre prijímanie a čítanie podpisových kontajnerov je prijímanie a čítanie

a) podpisového kontajneru vo formáte Associated Signature Containers (.asics, .scs, .asice, .sce) podľa osobitného predpisu11b) a podľa technických špecifikácií11ea) ***a to aj viacnásobne vnoreného****, pričom vnorený kontajner môže byť aj formát ZIP podľa technickej špecifikácie11eb) alebo formát podľa § 25 ods. 1 písm. a) prvého bodu,*

b) iných formátov podpisových kontajnerov ako uvedených v písmene a), ak sa na tom zasielateľ a prijímateľ dohodnú,

c) modulom centrálnej elektronickej podateľne externe podpísaných elektronických dokumentov alebo v ZEPf transportnom kontajneri obsahujúcom podpísaný dokument a jeho podpis CMS AdES alebo XML AdES podľa zverejnenej technickej špecifikácie11ec), pričom modul centrálnej elektronickej podateľne zabezpečuje aj overenie elektronického podpisu vyhotoveného podľa pravidiel platných do 30. júna 2016, ak takýto podpis strana spoliehajúca sa na podpis akceptuje; na overenie podpisov sa obsah transportného kontajnera ZEPf alebo samostatné podpisy a nimi podpísané dokumenty môžu uložiť do formátu ASiC, podľa písmena a), ***(účinnosť od júna 2019)***

d) priamo podpísaných elektronických dokumentov podľa § 57a písm. a), ktoré sú zároveň externe podpísanými elektronickými dokumentami v podpisových kontajneroch podľa písmena a).“ ***(účinnosť od júna 2019)***

Spoločná autorizácia

Spoločná autorizácia -zákon o e-Governmente

- **§ 28 ods. 3** – doložka právoplatnosti a vykonateľnosti neoddeliteľne spojená s elektronickým úradným dokumentom spoločnou autorizáciou (novela po MPK navrhuje aby nebola spoločná autorizácia v tomto prípade povinná)

- **§ 28 ods. 6** – elektronické úradné dokumenty zložené z údajov vyplnených podľa e-formulára a zároveň z iného elektronického dokumentu (najčastejšie PDF)

„(6) Ak obsah elektronického úradného dokumentu nie je možné alebo účelné vytvárať výlučne podľa elektronického formulára, je možné časti elektronického úradného dokumentu vytvoriť aj ako iný elektronický dokument; v takom prípade musia byť všetky časti elektronického úradného dokumentu neoddeliteľne spojené, a to tak, že sú autorizované spoločne ako jeden celok.“

- **§ 35 - § 39** – osvedčovacia doložka zaručenej konverzie autorizovaná spolu s novovzniknutým elektronickým dokumentom

Opakovaná / Spoločná autorizácia

ÚPPVII – často kladené otázky (výňatok):

5.2. Spoločná autorizácia elektronických dokumentov

„Pri spoločnej autorizácii externe podpísaného dokumentu (napr. rozhodnutie v XAdES_ZEP alebo ASiC) a nepodpísaného dokumentu (napr. XML doložka právoplatnosti) sa obvykle podpisujú iba samotné dokumenty bez ich pôvodných podpisov. Do XAdES_ZEP alebo ASiC obsahujúceho už podpísaný dokument sa len doplní ďalší dokument a ďalší paralelný podpis.

Nepodpisuje sa teda podpis pôvodného dokumentu ale len samotný pôvodný dokument bez podpisu.

(Pozn.: eIDAS však umožňuje podpisovať aj podpis pôvodného dokumentu.)

Pri spoločnej autorizácii priamo podpísaného dokumentu (napr. PDF rozhodnutie s PAdES) a nepodpísaného dokumentu (napr. XML doložka právoplatnosti) sa podpisuje aj pôvodný podpis. Obvykle sa vytvorí XAdES_ZEP, ZEPf alebo ASiC obsahujúci spoločne externe podpísané dokumenty, pričom tieto dokumenty môžu byť zároveň priamo podpísané.“

Zdroj: https://www.vicepremier.gov.sk/wp-content/uploads/2018/03/5.2..pdf

Spoločná autorizácia – CEP

Služby CEP umožňujú **vytvárať** spoločnú autorizáciu vo formátoch:

- ASiC-E XAdES/CAdES - paralelné podpisy, nie vnorené kontajnery
- PDF s PAdES v ASiC-E XAdES/CAdES (len PDF 1.3 a 1.4) – vnorené podpisy

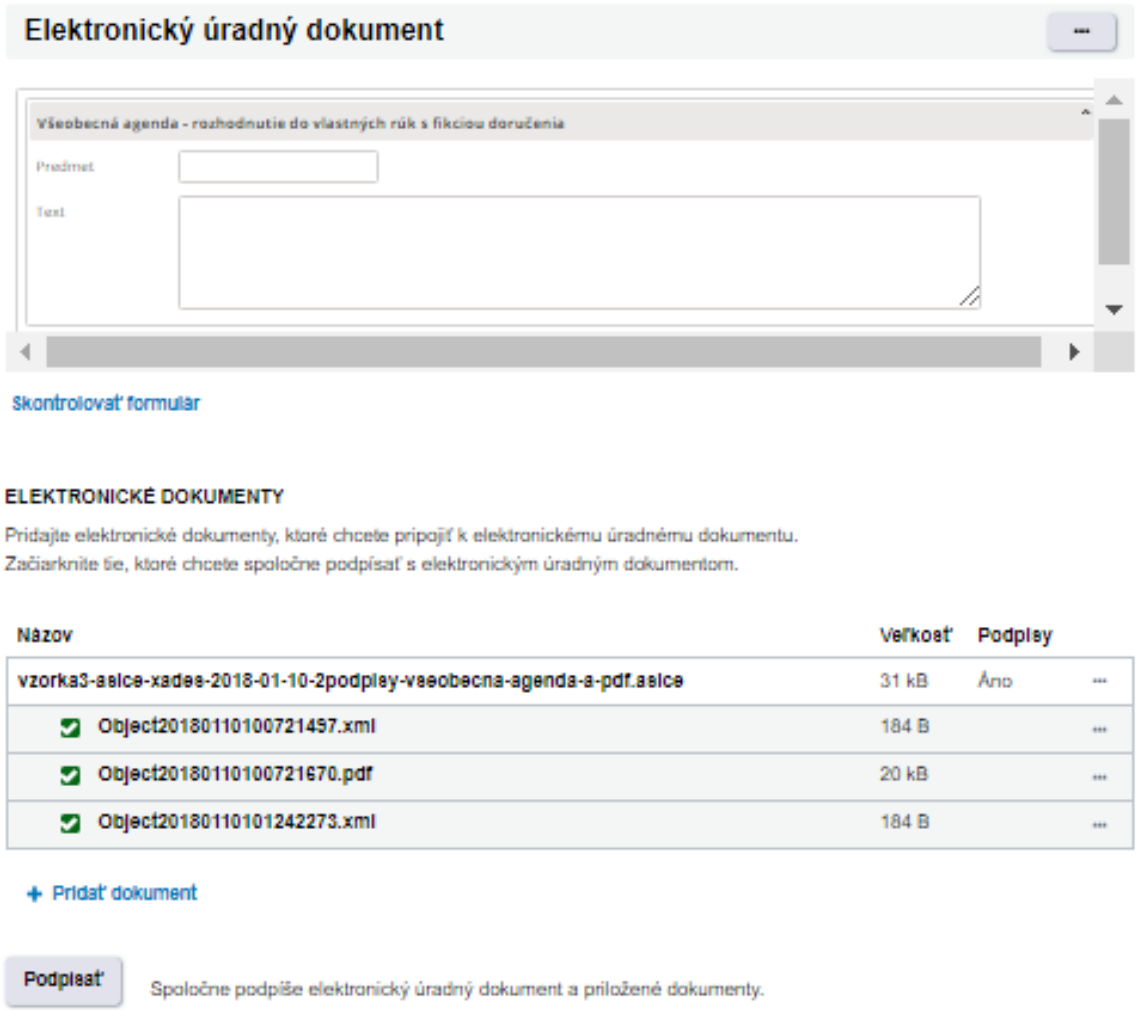
Klientske komponenty umožňujú **vytvárať** spoločnú autorizáciu (mandátnymi certifikátmi):

- XAdES_ZEP – Data Signatures - paralelné podpisy
- ASiC-E XAdES/CAdES – paralelné podpisy, nie vnorené kontajnery
- PDF s PAdES v ASiC-E XAdES/CAdES (len PDF 1.3 a 1.4) – vnorené podpisy

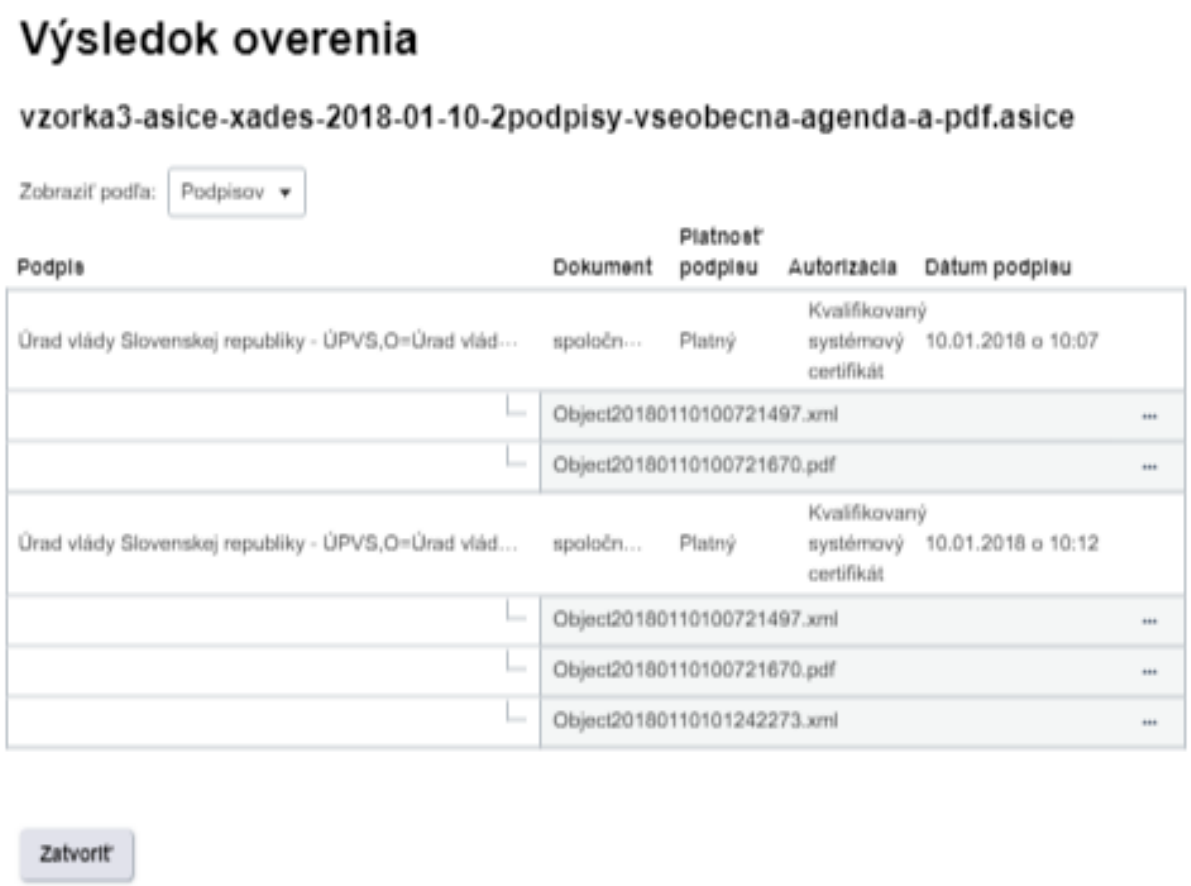
Podrobnosti sú uvedené v dokumentácii CEP:

https://www.slovensko.sk/_img/CMS4/Dokumentacia_funkcnosti_CEP.pdf

Spoločná autorizácia – CEP



Spoločná autorizácia – CEP



Výsledok overenia

vzorka3-asice-xades-2018-01-10-2podpisy-vseobecna-agenda-a-pdf.asice

Zobraziť podľa: Podpisov

Podpis	Dokument	Platnosť podpisu	Autorizácia	Dátum podpisu
Úrad vlády Slovenskej republiky - ÚPVS,O=Úrad vlád…	spoločn…	Platný	Kvalifikovaný systémový certifikát	10.01.2018 o 10:07
	Object20180110100721497.xml			…
	Object20180110100721670.pdf			…
Úrad vlády Slovenskej republiky - ÚPVS,O=Úrad vlád…	spoločn…	Platný	Kvalifikovaný systémový certifikát	10.01.2018 o 10:12
	Object20180110100721497.xml			…
	Object20180110100721670.pdf			…
	Object20180110101242273.xml			…

Zatvoriť

Spoločná autorizácia - Elektronický úradný dokument v MessageContainer

- V elektronickej úradnej správe má byť jedno elektronické podanie alebo jeden elektronický úradný dokument.
- V MessageContainer sa má prenášať v elemente Object s atribútom Class=„FORM“ a to aj v prípade, že obsahuje spoločnú autorizáciu viacerých dokumentov.
- Elektronický úradný dokument tvorený viacerými časťami (§28 ods. 6) nemá vo vyplnenom e-formulári obsahovať iba „sprievodný list“ s textom „v prílohe je rozhodnutie“. Mal by tvoriť súčasť rozhodnutia.
- Plánuje sa novela Výnosu o jednotnom formáte elektronických správ pre technické upresnenie. Pracovná verzia je na wiki UPPVII:
  - https://wiki.finance.gov.sk/download/attachments/25723226/vlastny_material_opatrenie-edit-sz23.pdf?version=1&modificationDate=1524402945240&api=v2
  - https://wiki.finance.gov.sk/display/PS1/8.+zasadnutie+PS1#id-8.zasadnutiePS1-Opatrenieojednotnomform%C3%A1teelektronick%C3%BDchspr%C3%A1vaSch%C3%A9myspr%C3%A1vSk-Talk

Aplikácie pre QES od NBÚ
- QES a LockIt

plk. Ing. Peter Rybár (NBÚ)

Aplikácie od NBÚ pre QES

- Možnosť vytvárať a spracúvať všetky formáty podpisov/pečatí podľa eIDAS
- Dostupné bezplatne na :

http://www.nbu.gov.sk/doveryhodne-sluzby/doveryhodne-zoznamy/aplikacie-tl-a-qes/index.html

  - **QES** – zatiaľ bez funkcie overovania (nová aplikácia),
  - **LockIt** – aj overovanie (staré formáty)
- Aplikácie používa NBÚ napríklad pre podpisovanie podpisových politík
- Aplikácie nie sú certifikované, avšak podľa platnej legislatívy už nie je povinnosť používať certifikované aplikácie

Podporované formáty v NBÚ aplikácii QES

Aplikácia QES podpisuje všetky typy dokumentov

- PDF dokument podpíše vo formáte PDF AdES, alebo pridá časovú pečiatku dokumentu vo formáte PDF AdES
- Ostatné typy dokumentov
    - podpíše s CMS AdES – pridá „.p7s“ k názvu súboru dokumentu (napr. pre „dokument.png“ uloží podpis do „dokument.png.p7s“ súboru)
    - časovo opečiatkuje – pridá „.tst“ k názvu súboru dokumentu (napr. pre „dokument.png“ uloží časovú pečiatku do „dokument.png.tst“)
- Ak zaškrtnete ASiC-E, dokumenty uloží do ZIP „.asice“ a podpíše ich jedným podpisom. Pre elektronické dokumenty pre ktoré existujú podpisy v „.p7s“ a časové pečiatky v „.tst“ vytvorí ASiC-S (napr. pre „dokument.png“ uloží podpis a časovú pečiatku do „dokument.png.asics“) a všetky dokumenty vrátane ASiC-S vloží do ASiC-E, ktorý podpíše s CMS AdES (napr. uloží do „dokument.png.asice“)

Aplikácia QES 32/64 bit (sha256/512) je dostupná na http://nbu.gov.sk/doveryhodne-sluzby/doveryhodne-zoznamy/aplikacie-tl-a-qes/ a testovacie kľúče s certifikátom, ak nemáte eID s čipom, si vydáte postupom https://lockit.webnode.sk/help-pictures/#tslsealorsignaturecertandkey1-png v aplikácii LockIt.

Prezeranie kontajnerov v NBÚ aplikácii QES

Aplikácia QES umožňuje prezeranie vnorených kontajnerov ASiC-S, ASiC-E, PDF a export dokumentov podpísaných podpismi CMS AdES, PDF AdES, XML AdES a opečiatkovaných časovou pečiatkou dokumentu.

Dvojklikom sa vnoríte do kontajnera PDF, ASiC-S alebo ASiC-E, ktoré máte v zozname QES aplikácie, pričom ak je v ASiC iný ASiC alebo PDF, tak sa vnoriť môžete aj doň.

- Ak ste vnorený v PDF, zadaním čísla podpisu alebo čísla časovej pečiatky sa označí podpísaný dokument vo formáte PDF AdES a zobrazí sa certifikát podpisovateľa, ktorého detaily zobrazíte klikom na ikonu certifikátu.
- Ak ste vnorený v ASiC-E, môžete v prvom vnorení pridať ďalšie dokumenty a určiť ich poradie v podpise a podpísať ich s CMS AdES, alebo časovo opečiatkovať.
- Ak ste vnorený v ASiC, zadaním čísla podpisu alebo čísla časovej pečiatky sa označia podpísané dokumenty v poradí ako boli podpísané a zobrazí sa certifikát podpisovateľa, ktorého detaily zobrazíte klikom na ikonu certifikátu.
- Klikom na tlačidlo DSId uložíte identifikátor vybraného podpisu do súboru „*.DSId“. Súbor s identifikátorom „*.DSId“ spolu s kontajnerom slúži na označenie len podpisom podpísaných dokumentov, ak kontajner obsahuje rôzne podpisy a rôzne dokumenty.

XMLDataContainer

Kontajner XML údajov

application/vnd.gov.sk.xmldatacontainer+xml; charset=UTF-8

XMLDataContainer

Výnos o štandardoch pre IS VS č. 55/2014 Z.z.

- V § 57a a § 57c vyžaduje prijímať a odosielať podpisované XML údaje len ak sú vnorené v XMLDataContainer, ktorý je podpísaný ako celok (teda dáta sa nepodpisujú samostatne)
- V prílohe č. 11 Výnosu definuje XMLDataContainer
- XSD pre XMLDataContainer je zverejnené v MetaIS

XMLDataContainer vznikol s cieľom:

- oddeliť identifikovanie schém od štruktúry podpisu
- nahradiť proprietárne riešenie XAdES_ZEP štandardizovaným (chýba medzinár. štandard)
- garantovať dostupnosť vizualizácie podpisovaných XML údajov
- garantovať dostupnosť XSD schémy podpisovaných XML údajov

XMLDataContainer

Zaregistrovaný mimetype v IANA

https://www.iana.org/assignments/media-types/application/vnd.gov.sk.xmldatacontainer+xml

XMLDataContainer obsahuje:

- Identifikačné údaje vyplneného elektronického formulára alebo iných XML údajov
- XMLData – jeden súbor XML 1.0 (includovaný)
- XSLT – referencovaná alebo vložená podpisová transformácia pre XMLData
  a metaúdaje transformácie (výstupný formát, jazyk, prostredie, mimetype)
- XSD - referencovaná alebo vložená schéma pre XMLData

XMLDataContainer

- XSLT a XSD musia byť :
  - **Referencované** – ak ide o údaje vyplnené podľa e-formulára
    - Referencovanie použitím referencovateľných identifikátorov súborov z modulu elektronických formulárov
    - Digitálny odtlačok referencovaného súboru
  - **Embedované** – ak ide o iné údaje

- Možnosť prenášať aj v XAdES_ZEP, v praxi sa používa v podstate len s ASiC

XMLDataContainer

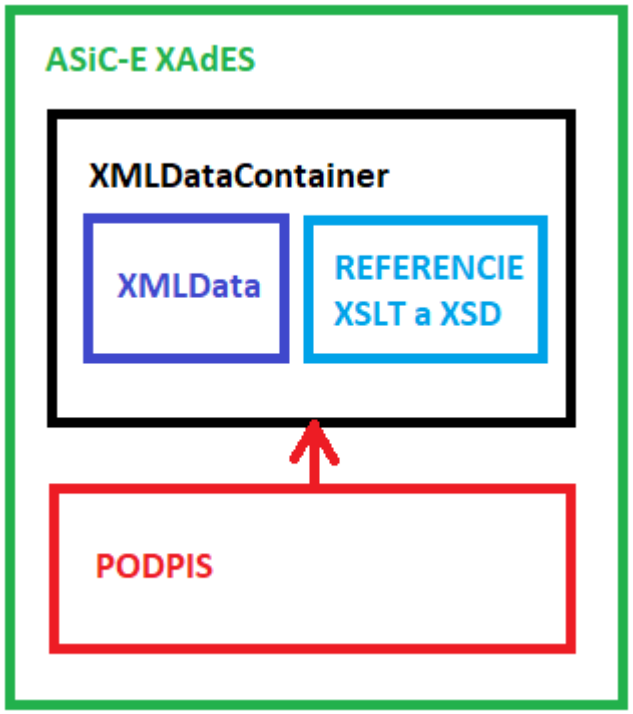
- Povinnosť prijímať len ak je podpisová transformácia do jedného z formátov: HTML, XHTML, TXT – platí pre iné údaje ako údaje e-formulára
- Pri spracúvaní údajov vyplnených podľa e-formulára sa môže používať ktorákoľvek z vizualizácií v e-formulári, nie je potrebné používať podpisovú (stačí implementovať podporu pre povinné vizualizácie HTML, XHTML, TXT)
- Pri overovaní podpisov nie je potrebné transformovanie do vizualizácie
- Za zhodu obsahu prezentačných schém zodpovedá gestor e-formulára

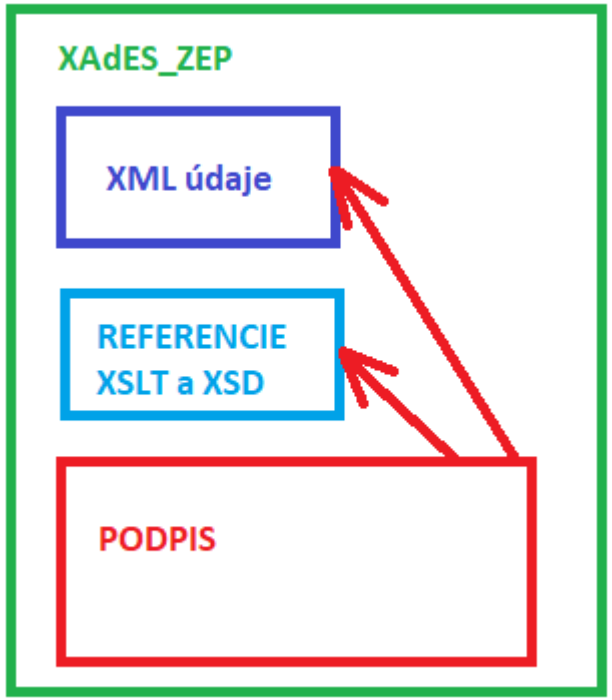
- Výnos o štandardoch 55/2014 Z.z., Príloha č. 3:

„6.3.2 Pri prijímaní a spracovaní vyplnených údajov elektronického formulára je možné použiť ktorúkoľvek z prezentácií zdokumentovaných v publikovanom elektronickom formulári podľa bodov 2.6.5 až 2.6.7, pričom nie je potrebné použiť prezentáciu použitú pri podpisovaní vyplnených údajov elektronického formulára.

6.3.3 Pri prijímaní a spracovaní vyplnených údajov elektronického formulára podpísaných elektronickým podpisom sa kontroluje, či kontajner pre XML údaje podľa prílohy č. 11 obsahuje referenciu podpisovej prezentácie zdokumentovanej v publikovanom elektronickom formulári podľa bodu 2.6.7. Jej transformovanie do prezentácie pri overovaní podpisu nie je potrebné.“

XMLDataContainer (v ASiC) vs XAdES_ZEP





Prepnutie na formát ASiC-E XAdES z formátu XAdES_ZEP

plánované na 15. 9. 2018

(NASES)

Prepnutie na formát ASiC-E XAdES na ÚPVS

Harmonogram:

- Integračný manuál pre CEP s podporou vytvárania a overovania ASiC – od júla 2016
- Oznamy o povinných formátoch a zverejnených vzorkách od novembra / decembra 2017
- Oznam o prepnutí na ASiC – máj a jún 2018

- Prepnutie na ASiC vo FIX prostredí - **od 15. augusta 2018**
- Prepnutie na ASiC v PROD prostredí - **od 15. septembra 2018**

- Integračný manuál s pomocnými funkčnosťami pre odlišovanie eIDAS formátov – september 2018 (od júla dostupný pracovný „DRAFT“ na Partner framework portáli)

Prepnutie na formát ASiC-E XAdES na ÚPVS

NASES prepne 15. septembra na formát ASiC-E XAdES:

- Konštruktor správy na ÚPVS (GUI)
  - Podpisy (eID, mandátne, ...) vytvárané v Konštruktore správy na ÚPVS
- Pečatenie cez POSP
  - Pečate jednotlivých organizácií automaticky vytvárané pre formuláre zaregistrované s možnosťou „podpisovať v mene inštitúcie)
- Pečate ÚV SR ÚPVS
  - automaticky vytvárané na doručenkách, a pod.

Subjekty integrované na CEP sa samé rozhodujú, kedy a na aký formát prepnú formát pečatí, ktoré vytvárajú pri volaní služieb CEP.

Prepnutie na formát ASiC-E XAdES na ÚPVS

Konštruktor správy na ÚPVS (GUI)

- Podanie: EGOV_APPLICATION
- Rozhodnutie: EGOV_DOCUMENT

- Všetky formuláre vypĺňané v konštruktore správy na ÚPVS (eDesk) a podpisované cez D.Signer/XAdES sa budú od 15.9. 2018 podpisovať len v ASiC-E XAdES. (Výnimka len pre spoločné podpisovanie starých XAdES_ZEP.)
  - Formuláre zaregistrované jednotlivými OVM, vypĺňateľné na ÚPVS v konštruktore správy
  - Všeobecná agenda podanie / rozhodnutie - Staré univerzálne formuláre
  - Úradný list, Rozhodnutie - Nové univerzálne formuláre

Prepnutie na formát ASiC-E XAdES na ÚPVS

Pečatenie cez POSP

- Formuláre zaregistrované s možnosťou „Podpisovať v mene inštitúcie“ sa po odoslaní v G2G automaticky pečatia pečaťou organizácie z HSM modulu ÚPVS, a to aj v prípade odoslania cez schránku alebo cez zbernicu UIR
- Neodporúčame používať, autorizácia pečaťou sa vytvára až po odoslaní správy a odosielateľ nedisponuje opečatenou verziou, čo nie je v súlade so zákonom o archívoch a registratúrach, používa sa len z historických dôvodov
- Možnosť registrovať nové formuláre s touto možnosťou **bude vypnutá v októbri 2018**
- Funkčnosť bude **nahradená tlačidlom „pečatiť“** v konštruktore správy (cca september 2018), pri zasielaní správ **cez integračné rozhranie** (UIR) **bude potrebné sa integrovať na CEP**
  - Ak sa rozhodnutie autorizuje v konštruktore správy a jeho formulár bude zaregistrovaný s „podpisovať v mene inštitúcie“, bude druhýkrát autorizované pečaťou. V takýchto prípadoch bude odporúčané preregistrovať formulár.
- Funkčnosť pečatenia cez POSP **pre existujúce formuláre bude vypnutá** – predpokladane do konca roka 2018
- Pri Centrálnom úradnom doručovaní **sa nedá používať vôbec**

Prepnutie na formát ASiC-E XAdES na ÚPVS

Pečate Úradu vlády SR - ÚPVS

- Potvrdenie o odoslaní podania: POSTING_CONFIRMATION
- Doručenka: ED_DELIVERY_REPORT
- Príkaz na úhradu: MEP_PAYMENT_ORDER_1_0
- Kópia príkazu na úhradu: MEP_PAYMENT_ORDER_COPY_1_0
- Potvrdenie o úhrade: MEP_PAYMENT_CONFIRM_1_0
- Hromadný príkaz na úhradu: MEP_MULTIPLE_PP_1_0 (týka sa iba IOM)
- Výsledok listinného doručovania: ED_DELIVERY_RESULT (v budúcnosti nahradí elektronickú doručenku)

Prepnutie na formát ASiC-E XAdES na ÚPVS

Vytváraný formát:

- ASiC-E XAdES (profil XAdES_ZEPbp – baseline profile, súladný s eIDAS)
- V prípade údajov vyplnených podľa e-formulára sú tieto vždy vnorené v XMLDataContainer (s referencovanými schémami)
- Zverejnené vzorky na ÚPVS
- Zverejnená dokumentácia a integračný manuál
- V službách CEP možnosť jeho vytvárania už od júla 2016, v praxi viac používaný od roku 2017 (DCOM)

Prepnutie na formát ASiC-E XAdES na ÚPVS

Spolupráca s integrovanými subjektami:

1. Ak je dokumentácia alebo integračný manuál nedostatočný / nejasný, kontaktujte nás aby sme ho zlepšili
2. Ak máte vážne problémy s prechodom na ASiC, prosíme o takú informáciu
3. Ak narazíte na nekompatibilitu formátov, prosíme o zaslanie vzoriek
4. Môžete nás kontaktovať na prevadzka@nases.gov.sk , stefan.szilva@nases.gov.sk
5. V prípade zistenej a overenej nefunkčnosti služieb nahlasujte prosím hneď incidenty cez portál

Služby CEP

Služby CEP – podpora pre ASiC od júla 2016

DITEC_CEP_PODPISANIE_DOKUMENTOV

- XAdES_ZEP
- CAdES_ZEP
- PAdES
- ASiC CAdES
- ASiC XAdES

DITEC_CEP_PODPISANIE_DOKUMENTOV2

- ASiC-E XAdES
- ASiC-E CAdES (len ak ide o opakované podpísanie existujúceho a nejde o XML)

Nové služby CEP (praktické ukážky)

DITEC_CEP_PODPISANIE_DOKUMENTOV2

- Opakovaná a spoločná autorizácia, vrátane možnosti určenia ktorý súbor z kontajnera sa má podpísať (ak ich obsahuje kontajner viac)
- Podpísanie existujúceho XMLDataContainer bez jeho opakovaného vyskladania (pripravované)
- Spájanie kontajnerov (pripravované, v krátkom čase) – samostatná služba rovnako ako v klientovi – ASiC Factory
- Doplnené nové možnosti - určenie konkrétnej podpisovej schémy
- Predvolené vypnutie validácie PDF/A s možnosťou jej vyžiadania

Nové služby CEP (praktické ukážky)

DITEC_CEP_VRATENIE_PODPISANYCH_DAT 2

- Doplnené názvy súborov a jedinečný identifikátor v rámci kontajnera/podpisu
- Voliteľný parameter pre vrátenie celého XMLDataContainer-a namiesto samotných XML údajov

DITEC_CEP_INFORMATIVNE_OVERENIE_ZEP 3

Doplnené:

- Voliteľný parameter pre možnosť získať podpísané dáta
- Názvy súborov a jedinečný identifikátor v rámci kontajnera/podpisu
- Či ide o kvalifikovaný / zdokonalený / podpis / pečať / ne/založený na kvalifikovanom certifikáte
- Typ certifikátu – kvalifikovaný, nekvalifikovaný, na QSCD, atď.
- Formát podpisu - XadES_ZEP, CAdES_ZEP, PAdES, XAdES-BP alebo CAdES-BP (odlíšiteľný SK/eIDAS formát)
- Typ podpisu (podľa špecifickej informácie z overovacieho komponentu)
- Ďalšie nepovinné elementy (integračný manuál sa dopĺňa, finalizácia v septembri 2018)

Nový výsledok predbežného a úplného overenia (od 10-12/2018)

Nový výsledok predbežného a úplného overenia

- Predbežné a úplné overenie podpisu: SIGN_VERIFY_RESULT
- **Oddelenie overenia podpisu od validácie podpísaných objektov**
- Zmena existujúcej XSD schémy
- Integrované subjekty budú upozornené na túto zmenu, plánovanú na 10/2018
- OVM, ktoré na ňu nebudú pripravené, musia kontaktovať NASES a budú dočasne zaradené do zoznamu subjektov, ktorý bude dostávať pôvodný formulár výsledku overenia (t.j. výsledok overenia budú mať dočasne bez zmeny)
- Zmena bude vykonaná hromadne od 10/2018

Výsledok predbežného a úplného overenia je iba informatívne overenie

- Overenie podpisov / pečatí na ÚPVS má z hľadiska legislatívy iba **informatívny charakter**, a to aj pri úplnom overení.
- **Nejde o kvalifikovanú dôveryhodnú službu validácie podpisov / pečatí** v zmysle článku 33 a 40 Nariadenia EP a Rady (EÚ) č. 910/2014.
  Plánuje sa obstarať do budúcna.
- V SR nie je podľa dostupných informácií takáto služba zatiaľ nikým bežne poskytovaná. (V TrustedList jeden poskytovateľ zo SR, neposkytované verejne.)
- Pri zaevidovaní podania (asynchrónna služba) pri predbežnom a úplnom overení si CEP zatiaľ trvalo uchováva všetky podklady potrebné pre overenie jednotlivej autorizácie.
- Pri informatívnom overení (synchrónna služba) sa podklady použité pre overenie jednotlivej autorizácie neuchovávajú.
- Neodlišuje zdokonalený podpis od kvalifikovaného podpisu.

Nové pravidlá replikácie elektronických formulárov v CEP, určovanie predvolenej podpisovej transformácie

Nový spôsob replikácie formulárov do CEP

Nasadený od: jún 2018

Dôvod zmeny:

- Nevyhovujúci algoritmus vyžadujúci jednu z možností:
  - názov súboru *.sb.xslt alebo *.html.xslt
  - hodnoty atribútu media-destination-type (text/plain, text/html, application/xhtml+xml) a zároveň media-destination (sign, view)
- Zosúladenie s Výnosom o štandardoch pre IS VS č. 55/2014 Z.z.
- Tolerancia pre rôzne kombinácie (takmer žiadny formulár nedodržiaval štandardy)
- Nové validácie pri registrácii formulárov – od 10/2018
- Čiastková dokumentácia zverejnená od roku 2017: https://wiki.finance.gov.sk/pages/viewpage.action?pageId=23990148
- Úplná dokumentácia bude zverejnená v októbri 2018 na slovensko.sk

Zoznam podpisových schém

Na slovensko.sk bude zverejňovaný zoznam podpisových schém zreplikovaných v CEP, spolu s ich identifikátormi.

Validácie formulárov v MEF

V MEF budú doplnené nové funkčnosti:

- Validácie elektronických formulárov voči štandardom pri ich registrácii (zaregistrovať bude možné len validný formulár a v prípade nevalidnosti bude do elektronickej schránky zaslaný zoznam chýb s konkrétnymi odporúčaniami na opravy formulára),

- Samostatná služba pre testovanie validnosti formulára a Zverejnenie všetkých validácií formulárov

- Dataset elektronických formulárov publikovaný každý deň

- Formulár pre vyžiadanie konverzie príkladných údajov vyplnených podľa e-formulára do PDF tlačovej vizualizácie, eDesk vizualizácie a podpisovej vizualizácie

- Zverejnenie súčastí elektronických formulárov na živých linkách v súlade so štandardmi

Zákaz používať pre pečatenie nepodpisové prezentačné schémy od októbra 2018

Zákaz používať pre pečatenie nepodpisové prezentačné schémy od 10/2018

- Replikácia formulárov kopíruje do CEP aj transformácie (do HTML/XHTML) určené pre zobrazovanie v elektronickej schránke (media-destination=view).
- Pri podpisovaní sa podľa legislatívy musia používať len podpisové schém s media-destination=sign
- Služba DITEC_CEP_PODPISANIE_DOKUMENTOV umožňuje určiť TypVizualizacie – XML (TXT), HTML, XHTML, ponúka aj tie, ktoré majú media-destination=view
- Podpisujúci preto nevedel, že nepoužíva podpisovú schému.
- V októbri 2018 sa v CEP plánuje zneprístupniť schémy s media-destination=view pre služby podpísania.
- Pre overovanie autorizácie zostanú k dispozícii aj schémy s media-destination=view a CEP ich zatiaľ bude akceptovať pri overovaní.

Zákaz používať pre pečatenie nepodpisové prezentačné schémy od 10/2018

- Pri vytváraní autorizácie použitím formulára, ktorý obsahuje viaceré podpisové schémy je potrebné uvádzať presný identifikátor danej schémy
- Nový element „IdentifikatorVizualizacie“ v oboch službách podpísania v CEP

Nové identifikátory podpisových schém
predbežne v 11-12 / 2018

Nové identifikátory podpisových schém

- Výnos o štandardoch č. 55/2014 Z.z. definoval nové URI identifikátory v § 46
- Pôvodné (dodnes používané) neštandardné identifikátory:
  - http://schemas.gov.sk/form/identifikator-formulara-v-mef/verzia/form.xslt
  - http://schemas.gov.sk/form/identifikator-formulara-v-mef/verzia/form.xsd
- Nové identifikátory, ktoré majú slúžiť aj ako živé URL:
  - https://data.gov.sk/doc/egov/eform/identifikator-formulara-v-mef/verzia/cesta/nazov-suboru.xslt
  - https://data.gov.sk/doc/egov/eform/identifikator-formulara-v-mef/verzia/schema.xsd

- Prechod na nové identifikátory bude vyžadovať koordináciu, môže sa časovo posunúť.
- Podľa príloh č. 3 a č. 11 Výnosu o štandardoch pre IS VS sa identifikátory uplatňujú od dátumu zverejneného na ÚPVS po dohode s ÚPPVII.

Časté chyby spôsobujúce nemožnosť spracovania

Časté chyby spôsobujúce nemožnosť spracovania

- *Používanie hodnoty atribútu MimeType v rozpore s formátom podpisu*
  - *Toto má za následok nemožnosť uloženia správy v schránke (a v prípade rozhodnutia do vlastných rúk vytvorenie doručenky avšak v skutočnosti nedoručenie rozhodnutia)*
- *Odosielanie súborov s nesprávnou príponou súboru*
  - *Toto sťažuje používateľom prácu so súbormi a v niektorých systémoch (mimo UPVS) môže spôsobovať problém so spracúvaním*
- *Uvádzanie hodnoty IsSigned=false alebo neuvádzanie hodnoty IsSigned*
  - *Toto má za následok, že sa podpis v danom objekte vôbec nevyhodnocuje*
  - *Často je spôsobená tým, že systémy najmä v prílohách neoverujú prítomnosť podpisu*
- *Uvádzanie hodnoty Encoding v rozpore so skutočnosťou*
  - *Ak sa uvedie Encoding=Base64 a kódovanie je XML (alebo naopak) zlyhá uloženie správy*
  - *Base64 string musí byť bez zalomení (v zmysle RFC)*
- *Používanie XML Encoding pre XAdES_ZEP - je nevhodné, niektoré systémy tretích strán narušujú integritu*
- *Uvádzanie chybných identifikátorov dátových objektov, chybných referencií na schémy e-formulárov v podpisoch a v XMLDataContainer*
- *Zaregistrovaný formulár s chybnou podpisovou transformáciou alebo s chybnou XSD schémou.*
- *Používanie certifikátov bez príznaku QcSSCD / QSCD v QcStatement, čím vzniká len zdokonalený podpis/pečať*

Platnosť časových pečiatok aj po konci platnosti certifikátu časovej pečiatky

Platnosť časových pečiatok aj po konci platnosti certifikátu časovej pečiatky

- V prípade, že ku kvalifikovanému elektronickému podpisu bola pred zrušením platnosti kvalifikovaného certifikátu podpisovateľa pripojená kvalifikovaná elektronická časová pečiatka podpisu, podpis je možné validovať ako platný počas celej doby platnosti tejto časovej pečiatky, (t.j. počas celej doby počas ktorej má služba časovej pečiatky kvalifikovaný štatút v dôveryhodnom zozname). Platnosť sa určuje podľa stavu služby časovej pečiatky v dôveryhodnom zozname zverejňovanom NBÚ a krajinami EÚ. Pre platnosť kvalifikovaných časových pečiatok je rozhodujúci stav "granted" uvedený v dôveryhodnom zozname pri príslušnej službe časových pečiatok. Dátum konca platnosti uvedený v certifikáte kvalifikovanej časovej pečiatky nemá vplyv na platnosť časových pečiatok vytvorených do tohto dátumu a obmedzuje iba poskytovateľa služby vo vytváraní nových časových pečiatok súkromným kľúčom s týmto certifikátom (napr. kapitola 9.4 technickej špecifikácie ETSI TS 119 312 V1.2.1 - 2017-05).

  (citát z FAQ na slovensko.sk)

- *Výklad aj vo zverejnenom stanovisku NBÚ:*

https://www.slovensko.sk/_img/CMS4/sposob_vyhodnocovania_QTS_a_QES.PDF

Validácia podpisov / pečatí / časových pečiatok

Výsledok overenia na UPVS je iba informatívne overenie

- Overenie podpisov / pečatí na ÚPVS má z hľadiska legislatívy iba **informatívny charakter**, a to aj pri úplnom overení.
- **Nejde o kvalifikovanú dôveryhodnú službu validácie podpisov / pečatí v zmysle eIDAS.** Plánuje sa obstarať do budúcna. (V SR nie je podľa dostupných informácií takáto služba zatiaľ nikým poskytovaná.)
- Pri zaevidovaní podania (asynchrónna služba) pri predbežnom a úplnom overení si CEP zatiaľ trvalo uchováva všetky podklady potrebné pre overenie jednotlivej autorizácie. Je teda dlhodobá preukázateľnosť / spätná overiteľnosť.
- Pri informatívnom overení (synchrónna služba) sa podklady použité pre overenie jednotlivej autorizácie neuchovávajú.
- Informatívne overenie 2, predbežné ani úplné overenie doteraz neodlišovalo zdokonalený podpis založený na kvalifikovanom certifikáte (bez príznaku QSCD) od kvalifikovaného podpisu, odlíšenie až v nových službách

Validácia podpisov / pečatí

„validácia“ je proces overenia a potvrdenia, že elektronický podpis alebo elektronická pečať sú platné.

(článok 3 eIDAS)

Validácia podpisov / pečatí

Článok 32

Požiadavky na validáciu kvalifikovaných elektronických podpisov

1. Procesom validácie kvalifikovaného elektronického podpisu sa potvrdí platnosť kvalifikovaného elektronického podpisu, ak:

*a) certifikát, ktorý potvrdzuje podpis, bol v čase podpísania **kvalifikovaným certifikátom** pre elektronický podpis v súlade s prílohou I;*

*b) kvalifikovaný certifikát **vydal kvalifikovaný poskytovateľ** dôveryhodných služieb a v čase podpísania **bol platný**;*

*c) údaje na validáciu podpisu **zodpovedajú údajom** poskytnutým spoliehajúcej sa strane;*

*d) sa jedinečný súbor údajov reprezentujúcich podpisovateľa **v certifikáte** správne poskytol spoliehajúcej sa strane;*

e) sa použitie pseudonymu jasne oznámilo spoliehajúcej sa strane v prípade, že sa v čase podpísania použil pseudonym;

*f) bol elektronický podpis vyhotovený **zariadením** na vyhotovenie **kvalifikovaného** elektronického podpisu; (QSCD)*

*g) **nebola narušená integrita** podpísaných údajov; (podpísaný digitálny odtlačok)*

*h) v čase podpísania boli dodržané **požiadavky** stanovené v článku 26.*

Overovanie podpisov

- Kvalifikovaný certifikát (predpísané náležitosti certifikátu)
- Certifikát vydal kvalifikovaný poskytovateľ (podľa dôveryhodného zoznamu)
- Platnosť certifikátu

- Nenarušenosť digitálneho odtlačku podpísaného dokumentu
  (zhoda v podpise s aktuálnym výpočtom)

- Správny formát podpisu (podporovaný podateľňou)

- Staré SK formáty:
  - Povinná platnosť časovej pečiatky
  - Validnosť podpísaného dokumentu podľa validátora určeného Ditec
  - Použitie predpísaných identifikátorov a popisov dokumentov alebo formulárov

Dôveryhodný zoznam – Trusted list (TL)

Článok 22

Dôveryhodné zoznamy

1. Každý členský štát vytvorí, vedie a uverejňuje dôveryhodné zoznamy vrátane informácií týkajúcich sa kvalifikovaných poskytovateľov dôveryhodných služieb, pre ktorých je príslušný, spolu s informáciami týkajúcimi sa kvalifikovaných dôveryhodných služieb, ktoré poskytujú.

*2. **Členské štáty zabezpečeným spôsobom vytvoria, vedú a uverejňujú elektronicky podpísané alebo zapečatené dôveryhodné zoznamy uvedené v odseku 1 vo forme vhodnej na automatizované spracovanie.***

3. Členské štáty poskytnú Komisii bez zbytočného odkladu informácie o orgáne zodpovednom za vytvorenie, vedenie a uverejňovanie národných dôveryhodných zoznamov, ako aj údaje o tom, kde sa tieto zoznamy uverejňujú, informácie o certifikátoch použitých na podpísanie alebo zapečatenie dôveryhodných zoznamov a oznámia jej všetky ich zmeny.

4. Komisia prostredníctvom zabezpečeného kanálu sprístupňuje verejnosti informácie uvedené v odseku 3 v elektronicky podpísanej alebo zapečatenej forme vhodnej na automatizované spracovanie.

5. Komisia do 18. septembra 2015 prostredníctvom vykonávacích aktov spresní informácie uvedené v odseku 1 a vymedzí technické špecifikácie a formáty pre dôveryhodné zoznamy uplatniteľné na účely odsekov 1 až 4. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Dôveryhodný zoznam - trusted list podľa eIDAS

https://webgate.ec.europa.eu/tl-browser/#/

http://ep.nbu.gov.sk/kca/tsl/tsl.xml

http://tlbrowser.tsl.website/tools/index.jsp

Certifikáty – obmedzená platnosť

- ETSI TS 119 312 (2017-05)

Table 9 summarizes the recommendations from tables above.

Table 9: Recommended signature suites for algorithm resistance during X years

Entry name of the signature suite	1 year	3 years	6 years
sha256-with-rsa	≥ 1 900	≥ 1 900	not recommended
sha512-with-rsa	≥ 1 900	≥ 1 900	not recommended
rsa-pss with mgf1SHA-256Identifier	≥ 1 900	≥ 1 900	≥ 3 000
rsa-pss with mgf1SHA-512Identifier	≥ 1 900	≥ 1 900	≥ 3 000
rsa-pss with mgf1SHA3-Identifier	≥ 1 900	≥ 1 900	≥ 3 000
sha256-with-dsa	2 048	2 048	3 072
sha512-with-dsa	2 048	2 048	3 072
sha224-with-ecdsa	legacy		
sha2-with-ecdsa	recommended		
sha2-with-ecsdsa	recommended		
sha3-with-ecdsa	recommended		
sha3-with-ecsdsa	recommended		

NOTE 2: Because sha224-with-rsa has no security or performance advantages or disadvantages compared with the stronger sha256-with-rsa it is not listed here for interoperability reasons only.

Table 10 provides the absolute dates for the recommendations from table 9.

Table 10: Recommended signature suites for a resistance up to X years

Entry name of the signature suite	2020	2025
sha256-with-rsa	≥ 1 900	not recommended
sha512-with-rsa	≥ 1 900	not recommended
rsa-pss with mgf1SHA-256Identifier	≥ 1 900	≥ 3 000
rsa-pss with mgf1SHA-512Identifier	≥ 1 900	≥ 3 000
rsa-pss with mgf1SHA3-Identifier	≥ 1 900	≥ 3 000
sha256-with-dsa	2 048	3 072
sha512-with-dsa	2 048	3 072
sha224-with-ecdsa	legacy	
sha2-with-ecdsa	recommended	
sha2-with-ecsdsa	recommended	
sha3-with-ecdsa	recommended	
sha3-with-ecsdsa	recommended	

Platnosť certifikátov

CRL – Certificate Revocation List

- súbor, obvykle aktualizovaný raz za „x“ hodín (napr. 8 hodín)
- napr. pre eID – 8,5 MB CRL súbor

OCSP – Online Certificate Status Protocol

- služba (request/response), online odpoveď
- napr. pre eID – 7 kB OCSP
- môže sa stať, že obsahuje informácie platné k skoršiemu času ako je čas z časovej pečiatky (položka thisUpdate z OCSP a CRL)

vtedy overovač na ÚPVS použije CRL namiesto OCSP

- prípadné čakanie (napr. 20 s) kým sa vyšle request

Platnosť certifikátov

Zákon 272/2016 Z.z. (§ 18)

„(5) Informácie o štatúte platnosti alebo zrušenia kvalifikovaných certifikátov18) v Online Certificate Status Protocol (OCSP) odpovedi32) ktorá musí obsahovať pozitívne prehlásenie o existencii a správnosti údajov31) sa povinne poskytujú od 1. januára 2018.“

eIDAS

Čl. 24

„4. Pokiaľ ide o odsek 3, kvalifikovaní poskytovatelia dôveryhodných služieb, ktorí vydávajú kvalifikované certifikáty, každej spoliehajúcej sa strane poskytnú informácie o štatúte platnosti alebo zrušenia kvalifikovaných certifikátov, ktoré vydali. Tieto informácie sa poskytujú aspoň, pokiaľ ide o jednotlivé certifikáty, kedykoľvek, a to aj po uplynutí doby platnosti certifikátu, ***automatizovaným spôsobom, ktorý je spoľahlivý, bezplatný a efektívny****.“*

Platnosť certifikátov

NBÚ:

Napríklad ochrana pred útokom na DigiNotár, kedy na falošné neznáme certifikáty sa odpovedalo, že sú platné. Teraz OCSP server musí vypočítať hash z certifikátu a v OCSP odpovedi o stave certifikátu musí zaslať aj hash z certifikátu.

Platnosť certifikátov

NBÚ stanovisko:

Povinnosť podľa nariadenia eIDAS je poskytnúť informácie do 24 hodín (thisUpdate) od požiadania zrušenia.

Podľa eIDAS sa stav poskytuje na základe databázy certifikátov, ktorá obsahuje aj stav certifikátu.

OCSP odpoveď musí obsahovať hash certifikátu, ktorého stav odpoveď vracia, ak kvalifikovaný štatút pre CA bol udelený úradom.

V aktuálnom dôveryhodnom zozname už všetky CA obsahujú odkaz na OCSP službu, aj keď v kvalifikovanom certifikáte adresa na OCSP môže chýbať.

http://ep.nbu.gov.sk/kca/tsl/tsl.xml

Údaje v certifikáte – CRL / OCSP

Citát z certifikátu z eID:

#2: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
[
accessMethod: ocsp
accessLocation: URIName: http://svkeidaca-ocsp.disig.sk/ocsp/svkeidaca
,
accessMethod: caIssuers
accessLocation: URIName: http://eidrep1.disig.sk/svkeidaca/cert/svkeidaca.p7c
,
accessMethod: caIssuers
accessLocation: URIName: http://eidrep2.disig.sk/svkeidaca/cert/svkeidaca.p7c
]
]
#5: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
[DistributionPoint:
[URIName: http://eidrep1.disig.sk/svkeidaca/crl/svkeidaca.crl]
, DistributionPoint:
[URIName: http://eidrep2.disig.sk/svkeidaca/crl/svkeidaca.crl]
]]

Platnosť certifikátov – príklad OCSP odpovede

OCSP Response
HASH(SHA256:2 16 840 1 101 3 4 2 1)= DF92104F900FBB643321819C834E2DF5A3D0B3A98F5C9819030A62C15F1490B5
OCSP responder name:
 SK - countryName(2.5.4.6)
 Bratislava - localityName(2.5.4.7)
 NTRSK-35975946 - serialNumber(2.5.4.5)
 Disig a.s. - organizationName(2.5.4.10)
 Responder 1_1 - organizationalUnitName(2.5.4.11)
 OCSP SVK eID ACA - commonName(2.5.4.3)
Signature Algorithm: SHA-256 with RSA encryption
Produced At: **27. 2. 2018 23:12:50** UTC
Response Count: 1

Response: 1
Hash Algorithm: SHA-256
Issuer Name Hash: F023C106BEA693C29048B0D7A088AD37E33BEB3E6F712BF7358857E00367BB51
Issuer Key Hash: 4B270A07AB75CEF985314B9D6D5F2F7CB73CE60570ED790631479F303DB6D5A0
Serial Number: 04D22174B9C80112CDA1
Certificate Status: Revoked
  Revocation Time: 31. 10. 2017 17:23:32 UTC
  Revocation Reasons: -
This Update: **27. 2. 2018 23:12:42** UTC
Next Update: 27. 2. 2018 23:22:42 UTC
Extensions:
Positive statement - OID of Hash alg. and Certificate Hash:
SEQUENCE {
 SEQUENCE {
  OBJECT IDENTIFIER 2.16.840.1.101.3.4.2.1 sha-256
  NULL
 }
 OCTET STRING x205B436EEE7F4893FFE3D1C4C7832475C6B61D433F36535ED81403D36B56FC8C
}

Platnosť certifikátov – príklad OCSP odpovede

OCSP Response
HASH(SHA256:2 16 840 1 101 3 4 2 1)= 122A7B5001D1B756A4297F6BD93EEAC8901F9351BFE04ADEB8A7CA3BE40CB0CC
OCSP responder name:
 SK - countryName(2.5.4.6)
 Bratislava - localityName(2.5.4.7)
 NTRSK-35975946 - serialNumber(2.5.4.5)
 Disig a.s. - organizationName(2.5.4.10)
 Responder 1_1 - organizationalUnitName(2.5.4.11)
 OCSP SVK eID ACA - commonName(2.5.4.3)
Signature Algorithm: SHA-256 with RSA encryption
Produced At: **27. 2. 2018 23:23:30** UTC
Response Count: 1

Response: 1
Hash Algorithm: SHA-256
Issuer Name Hash: F023C106BEA693C29048B0D7A088AD37E33BEB3E6F712BF7358857E00367BB51
Issuer Key Hash: 4B270A07AB75CEF985314B9D6D5F2F7CB73CE60570ED790631479F303DB6D5A0
Serial Number: 04119F81AB9201174AAA
Certificate Status: Good
This Update: **27. 2. 2018 23:23:26** UTC
Next Update: 27. 2. 2018 23:33:26 UTC
Extensions:
Positive statement - OID of Hash alg. and Certificate Hash:
SEQUENCE {
 SEQUENCE {
  OBJECT IDENTIFIER 2.16.840.1.101.3.4.2.1 sha-256
  NULL
 }
 OCTET STRING xF64D58F6F46B32160D05E54847612FA77BA443A966E6115D317844EE2E040EDA
}

Platnosť certifikátov – príklad CRL

Zoznam zrušených certifikátov (CRL)
HASH(SHA256:2 16 840 1 101 3 4 2 1)= C333C9FE0D2B62F81DD9690D4ADD136770EC72D0452EF3E1E24F967D0B36BEBE
CRL Vydavatel:
SK - countryName(2.5.4.6)
Bratislava - localityName(2.5.4.7)
Narodny bezpecnostny urad - organizationName(2.5.4.10)
SIBEP - organizationalUnitName(2.5.4.11)
SNCA2 - commonName(2.5.4.3)
Čas poslednej zmeny: 27. 4. 2018 18:01:05 UTC
Next update: 28. 4. 2018 18:00:05 UTC
Signature algorithm: SHA-256 with RSA encryption
Cert Items 328
Cert #0
6740
Revocation Date 28. 4. 2015 13:17:09 UTC
Revocation Reason Unspecified can be used to revoke certificates for reasons other than the specific codes
Cert #1
6764
Revocation Date 4. 5. 2015 9:19:23 UTC
Revocation Reason Unspecified can be used to revoke certificates for reasons other than the specific codes
Cert #2
6754
Revocation Date 4. 5. 2015 12:29:01 UTC
Revocation Reason Unspecified can be used to revoke certificates for reasons other than the specific codes
...

Platnosť certifikátov – príklad CRL

```
Certificate Revocation List (CRL):
        Version 2 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: /C=SK/L=Bratislava/O=Disig a.s./OU=ACA-307-2007-2/CN=SVK eID ACA
        Last Update: Apr 27 17:30:00 2018 GMT
        Next Update: Apr 28 17:30:00 2018 GMT
        CRL extensions:
            X509v3 CRL Number:
                8812
            X509v3 Authority Key Identifier:
                keyid:B1:CA:C6:A5:DA:EF:A9:AF:A3:BE:D3:DB:40:C9:E9:EA:A1:6F:91:61
                DirName:/C=SK/L=Bratislava/O=Narodny bezpecnostny urad/OU=SIBEP/CN=KCA NBU SR 3
                serial:06:DA

            X509v3 Issuing Distrubution Point: critical
                Full Name:
                  URI:http://eidrep1.disig.sk/svkeidaca/crl/svkeidaca.crl
                  URI:http://eidrep2.disig.sk/svkeidaca/crl/svkeidaca.crl

Revoked Certificates:
    Serial Number: 0400008B79450113859E
        Revocation Date: Oct 31 17:23:32 2017 GMT
    Serial Number: 0400008B79450113983F
        Revocation Date: Oct 31 17:23:32 2017 GMT
    Serial Number: 040000EF1D1901122184
        Revocation Date: Oct 31 17:23:32 2017 GMT
    Serial Number: 0400014B843F0114955A
        Revocation Date: Oct 31 17:23:32 2017 GMT...
```

Ďakujem za pozornosť

stefan.szilva@nases.gov.sk

prevadzka@nases.gov.sk