Povinné formáty kvalifikovaných elektronických podpisov a pečatí (QES) pre subjekt verejného sektora pri vyhotovovaní a validácii

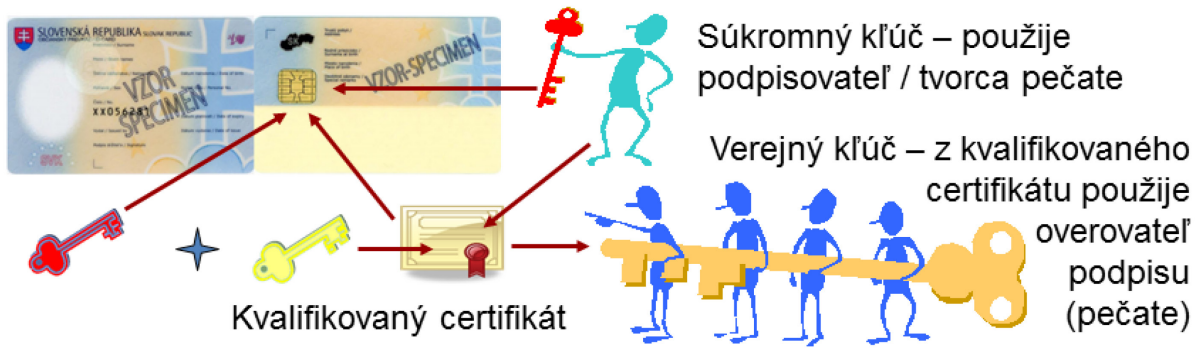
Formát pre QES je od 1.7.2016 definovaný v prílohe vykonávacieho rozhodnutia Komisie č. 2015/1506.

Subjekt verejného sektora musí podľa článkov 27 a 37 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu vedieť validovať všetky 4 formáty QES a vyhotovovať minimálne jeden formát QES z nasledovného zoznamu formátov:

- CMS AdES - Základný profil CAdES ETSI TS 103173 v.2.2.1
- PDF AdES - Základný profil PAdES ETSI TS 103172 v.2.2.2
- XML AdES - Základný profil XAdES ETSI TS 103171 v.2.1.1
- ASiC - Základný profil podpisového kontajnera vo formáte ASiC ETSI TS 103174 v.2.2.1

QES je zdokonalený elektronický podpis (alebo pečať), ktorý je založený na kvalifikovanom certifikáte a súkromný kľúč slúžiaci na uzamknutie (podpísanie alebo zapečatenie) elektronického dokumentu je uložený v zariadení na vyhotovenie kvalifikovaných elektronických podpisov alebo pečatí (QSCD). Kvalifikovaný certifikát obsahuje minimálne meno podpisovateľa (alebo tvorcu pečate), verejný kľúč na odomknutie (overenie podpisu alebo pečate) elektronického dokumentu, informáciu o uložení párového súkromného kľúča v QSCD zariadení a informácie o vydavateľovi kvalifikovaného certifikátu. Vydavateľ kvalifikovaného certifikátu zodpovedá za správnosť údajov v certifikáte – overenie identity, overenie kľúčového páru, overenie použitia certifikovaného QSCD s jeho správnou konfiguráciou podľa certifikácie QSCD, za možnosť zrušiť certifikát (skrátiť platnosť certifikátu v dobe platnosti uvedenej v certifikáte) a za podpísanie alebo zapečatenie kvalifikovaného certifikátu. Vydavateľ certifikátu musí mať kvalifikovaný štatút v dôveryhodnom zozname, ktorý zverejňuje Národný bezpečnostný úrad, pozri http://www.nbu.gov.sk/doveryhodne-sluzby/index.html.

Základné pravidlo: Čo jeden kľúč zamkne, to odomkne len druhý kľúč z páru a žiaden iný kľúč. Kľúčový pár je uložený v zariadení na vyhotovenie kvalifikovaných elektronických podpisov alebo pečatí (QSCD), ktoré len po autentifikácii vlastníka kľúča určeného na uzamknutie (súkromného kľúča) umožní použitie súkromného kľúča, a teda nikto iný nemôže a ani nesmie súkromný kľúč použiť, čo je znázornené na nasledujúcom obrázku.



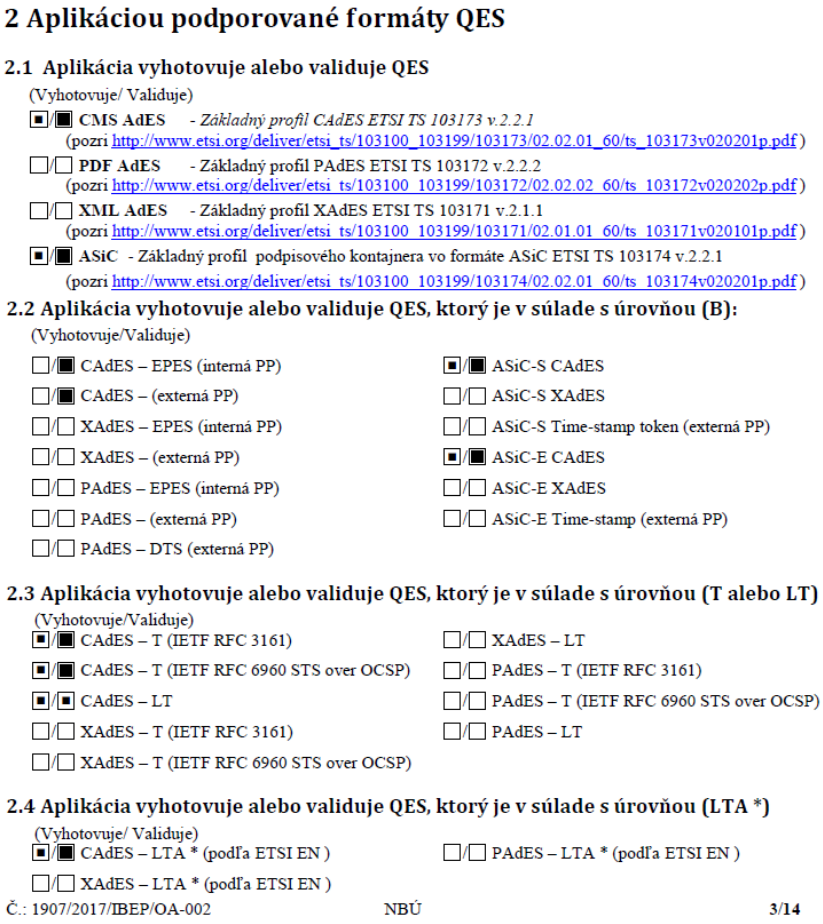
Aplikácia pre QES musí splniť požiadavky pre zdokonalený elektronický podpis uvedené v prílohe vykonávacieho rozhodnutia Komisie č. 2015/1506, ktorým sa ustanovujú špecifikácie týkajúce sa

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.

Validovanie QES

Subjekty verejného sektora si musia aktualizovať svoje aplikácie pre QES, aby boli v súlade s nariadením (EÚ) č. 910/2014, ak ich aplikácie boli posúdené podľa legislatívy platnej pred 1.7.2016.

To či aplikáciu, ktorú používa subjekt verejného sektora, je potrebné aktualizovať alebo doplniť aj inou aplikáciou, si môže subjekt verejného sektora overiť na základe vyplneného formulára "Deklarácia dodávateľa aplikácie (výrobcu) pre kvalifikovaný elektronický podpis/pečať (QES)" zverejneného NBÚ a to najmä podľa zaškrtnutia všetkých štyroch políčok druhého stĺpca v kapitole 2.1 "Aplikácia vyhotovuje alebo validuje QES". Zaškrtnutím výrobca aplikácie deklaruje, že aplikácia vie validovať daný formát podpisu alebo pečate. Ak v deklarácii jednej aplikácie pre QES niektoré políčko druhého stĺpca z kapitoly 2.1 nie je zaškrtnuté, subjekt verejného sektora musí mať aj ďalšie aplikácie pre QES, aby spoločne boli zaškrtnuté všetky políčka druhého stĺpca z kapitoly 2.1. Nasledujúci obrázok znázorňuje, že aplikácia deklaruje validovanie pre dva formáty QES: CMS AdES a ASiC. Pre validovanie QES formátov PDF AdES a XML AdES je potrebná ďalšia aplikácia.



2 Aplikáciou podporované formáty QES

2.1 Aplikácia vyhotovuje alebo validuje QES

(Vyhotovuje/ Validuje)

☑/☑ **CMS AdES** - *Základný profil CAdES ETSI TS 103173 v.2.2.1*
(pozri http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf)

☐/☐ **PDF AdES** - Základný profil PAdES ETSI TS 103172 v.2.2.2
(pozri http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf)

☐/☐ **XML AdES** - Základný profil XAdES ETSI TS 103171 v.2.1.1
(pozri http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf)

☑/☑ **ASiC** - Základný profil podpisového kontajnera vo formáte ASiC ETSI TS 103174 v.2.2.1
(pozri http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf)

2.2 Aplikácia vyhotovuje alebo validuje QES, ktorý je v súlade s úrovňou (B):

(Vyhotovuje/Validuje)

☐/☑ CAdES – EPES (interná PP)	☑/☑ ASiC-S CAdES
☐/☑ CAdES – (externá PP)	☐/☐ ASiC-S XAdES
☐/☐ XAdES – EPES (interná PP)	☐/☐ ASiC-S Time-stamp token (externá PP)
☐/☐ XAdES – (externá PP)	☑/☑ ASiC-E CAdES
☐/☐ PAdES – EPES (interná PP)	☐/☐ ASiC-E XAdES
☐/☐ PAdES – (externá PP)	☐/☐ ASiC-E Time-stamp (externá PP)
☐/☐ PAdES – DTS (externá PP)	

2.3 Aplikácia vyhotovuje alebo validuje QES, ktorý je v súlade s úrovňou (T alebo LT)

(Vyhotovuje/Validuje)

☑/☑ CAdES – T (IETF RFC 3161)	☐/☐ XAdES – LT
☑/☑ CAdES – T (IETF RFC 6960 STS over OCSP)	☐/☐ PAdES – T (IETF RFC 3161)
☑/☑ CAdES – LT	☐/☐ PAdES – T (IETF RFC 6960 STS over OCSP)
☐/☐ XAdES – T (IETF RFC 3161)	☐/☐ PAdES – LT
☐/☐ XAdES – T (IETF RFC 6960 STS over OCSP)	

2.4 Aplikácia vyhotovuje alebo validuje QES, ktorý je v súlade s úrovňou (LTA *)

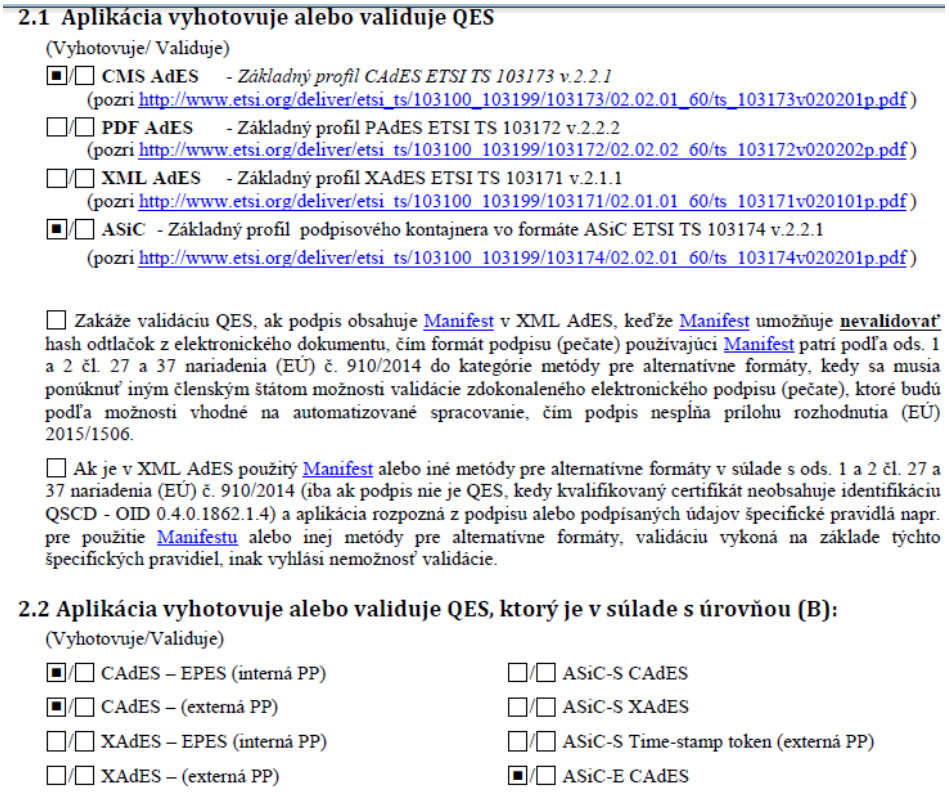
(Vyhotovuje/ Validuje)

☑/☑ CAdES – LTA * (podľa ETSI EN)	☐/☐ PAdES – LTA * (podľa ETSI EN)
☐/☐ XAdES – LTA * (podľa ETSI EN)	

Č.: 1907/2017/IBEP/OA-002 NBÚ 3/14

Vyhotovovanie QES

Každý subjekt, ktorý vyhotovuje kvalifikovaný elektronický podpis (alebo pečať) elektronického dokumentu, ktoré sa vyžadujú pri používaní služieb online ponúkaných prostredníctvom alebo v mene subjektu verejného sektora, musí od 1.7.2016 pri vyhotovovaní QES používať aplikácie spĺňajúce požiadavky prílohy vykonávacieho rozhodnutia Komisie č. 2015/1506. Overenie splnenia tejto požiadavky na aplikácie pre QES je možné na základe výrobcom (dodávateľom) aplikácie vyplneného formulára "Deklarácia dodávateľa aplikácie (výrobcu) pre kvalifikovaný elektronický podpis/pečať (QES)" zverejnenom NBÚ, kde musí byť pre formát podpisu alebo pečate, ktorý aplikácia vyhotovuje, zaškrtnuté políčko prvého stĺpca v kapitole 2.1 "Aplikácia vyhotovuje alebo validuje QES", kde zaškrtnutím výrobca aplikácie deklaruje, že aplikácia vie vyhotoviť daný formát podpisu alebo pečate. Nasledujúci obrázok znázorňuje, že aplikácia deklaruje vyhotovovanie dvoch formátov QES: CMS AdES a ASiC.



2.1 Aplikácia vyhotovuje alebo validuje QES

(Vyhotovuje/ Validuje)

☑/☐ **CMS AdES** - *Základný profil CAdES ETSI TS 103173 v.2.2.1*
(pozri http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf)

☐/☐ **PDF AdES** - Základný profil PAdES ETSI TS 103172 v.2.2.2
(pozri http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf)

☐/☐ **XML AdES** - Základný profil XAdES ETSI TS 103171 v.2.1.1
(pozri http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf)

☑/☐ **ASiC** - Základný profil podpisového kontajnera vo formáte ASiC ETSI TS 103174 v.2.2.1
(pozri http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf)

☐ Zakáže validáciu QES, ak podpis obsahuje Manifest v XML AdES, keďže Manifest umožňuje **nevalidovať** hash odtlačok z elektronického dokumentu, čím formát podpisu (pečate) používajúci Manifest patrí podľa ods. 1 a 2 čl. 27 a 37 nariadenia (EÚ) č. 910/2014 do kategórie metódy pre alternatívne formáty, kedy sa musia ponúknuť iným členským štátom možnosti validácie zdokonaleného elektronického podpisu (pečate), ktoré budú podľa možnosti vhodné na automatizované spracovanie, čím podpis nespĺňa prílohu rozhodnutia (EÚ) 2015/1506.

☐ Ak je v XML AdES použitý Manifest alebo iné metódy pre alternatívne formáty v súlade s ods. 1 a 2 čl. 27 a 37 nariadenia (EÚ) č. 910/2014 (iba ak podpis nie je QES, kedy kvalifikovaný certifikát neobsahuje identifikáciu QSCD - OID 0.4.0.1862.1.4) a aplikácia rozpozná z podpisu alebo podpísaných údajov špecifické pravidlá napr. pre použitie Manifestu alebo inej metódy pre alternatívne formáty, validáciu vykoná na základe týchto špecifických pravidiel, inak vyhlási nemožnosť validácie.

2.2 Aplikácia vyhotovuje alebo validuje QES, ktorý je v súlade s úrovňou (B):

(Vyhotovuje/Validuje)

☑/☐ CAdES – EPES (interná PP)	☐/☐ ASiC-S CAdES
☑/☐ CAdES – (externá PP)	☐/☐ ASiC-S XAdES
☐/☐ XAdES – EPES (interná PP)	☐/☐ ASiC-S Time-stamp token (externá PP)
☐/☐ XAdES – (externá PP)	☑/☐ ASiC-E CAdES

Rozpoznanie typov kvalifikovaných elektronických podpisov, pečatí a kvalifikovaných elektronických časových pečiatok.

CMS kvalifikovaný elektronický podpis

1. Ak je koncovka súboru (*.**p7m**), CMS podpis obsahuje podpísaný elektronický dokument, jeden podpis alebo viacero paralelných podpisov, (kvalifikované) elektronické časové pečiatky, certifikáty, CRL a OCSP odpovede.
2. Ak je koncovka súboru (*.**p7s**), CMS podpis je zhodný s (*.p7m), len neobsahuje podpísaný elektronický dokument. Podpísaný elektronický dokument je uložený externe (napr. v súbore). Zaužívané je, že názov súboru, obsahujúci podpis, vznikne spojením názvu podpísaného elektronického dokumentu (súboru) s koncovkou mena súboru „.p7s“. Teda ak

názov súboru s podpísaným elektronickým dokumentom je „dokument.png“, tak názov súboru s podpisom je „dokument.png.**p7s**“.

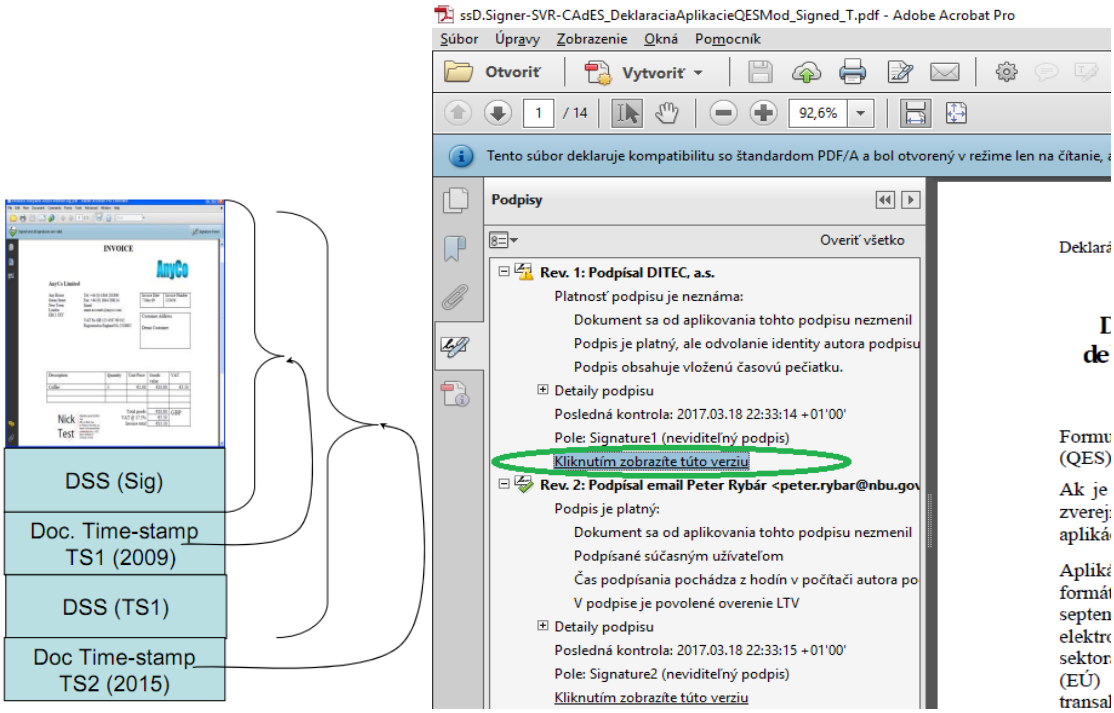
3. Ak je koncovka súboru (*.**tst**), ide o časovú pečiatku (TS) súboru. TS je CMS podpis obsahujúci podpísaný el. dokument typu TSTInfo definovaný v IETF RFC 3161. TSTInfo obsahuje dátum a čas spojený s hash hodnotou časovo opečiatkovaného externého objektu (súboru).

PDF kvalifikovaný elektronický podpis - koncovka súboru (*.**pdf**). Podpis v PDF je realizovaný pomocou CMS podpisu. Každý podpis sa pridáva na koniec PDF súboru a zabezpečuje celý predošlý PDF súbor. Pred podpisom je možné na koniec PDF súboru uložiť zmeny PDF objektov, ktoré menia objekty na stranách PDF dokumentu ako incremental update, teda nespôsobia poškodenie predchádzajúcich podpisov PDF dokumentov. PDF súbor môže obsahovať x+1 rôznych PDF dokumentov, kde x je počet PDF podpisov v PDF súbore. Schéma dohľadu zaviedla identifikátor **SRId** na identifikáciu podpísaného dokumentu na základe hash hodnoty z digitálneho podpisu. SRId je možné použiť pre všetky typy zdokonalených elektronických podpisov, pričom pri PDF podpisoch SRId umožňuje vyhnúť sa nepríjemným situáciám, ak by sa pracovalo s nesprávnym PDF dokumentom z PDF súboru (za podpisovateľa), exportom PDF dokumentu z PDF súboru na základe SRId identifikácie.

Podľa štandardu ISO 32000 – 1(2) rozlišujeme nasledovné formáty PDF elektronického podpisu, pečate a elektronickej časovej pečiatky PDF dokumentu:

- Vizuálne viditeľný podpis v PDF dokumente.
- Vizuálne neviditeľný podpis v PDF dokumente.
- Vizuálne neviditeľná časová pečiatka PDF dokumentu.

V obrázku nižšie je uvedený príklad pridávaných údajov na koniec PDF súboru do Document Security Store (DSS) obsahujúci napr. certifikáty, informácie o platnosti certifikátu vo forme CRL alebo OCSP odpovede a rovnako je možné vložiť aj zmeny napríklad textu alebo obrázkov na konkrétnej strane v PDF dokumente.



XML kvalifikovaný elektronický podpis má koncovku súboru (*.**xml**). XML podpis je podpis definovaný v XML dokumente https://www.w3.org/TR/xmldsig-core/. ETSI ESI XAdES štandard dopĺňa XML podpis o elementy, ktoré pridávajú možnosti definované v CMS podpisoch do XML podpisov. XML podpis môže podpisovať:

1. priamo XML element, do ktorého je XML podpis vložený,
2. konkrétny XML element v XML dokumente (jeden XML element alebo samostatne viacero XML elementov jedným podpisom) a aj
3. externý objekt, napr. súbor "dokument.png".

XML podpis umožňuje do jedného podpisu zahrnúť odtlačky (hash hodnoty) viacerých elektronických dokumentov, ale nedefinuje možnosť paralelných podpisov, tak ako je to v CMS podpisoch. Z toho dôvodu ETSI ESI ASiC štandard zadefinoval XML schému pre paralelné XML podpisy. XML podpis je náchylný k nekončiacim problémom s metódami kanonikalizácie, ktorá špecifikuje kanonikalizačný algoritmus uplatňovaný ešte pred vykonaním výpočtu podpisu. XML podpis umožňuje aj zadefinovanie vlastných pravidiel overenia, kedy podpísané dokumenty nie je potrebné prekontrolovať pri použití elementu typu Manifest odkazujúceho na tieto dokumenty. Element typu Manifest je určený hlavne pre uzatvorené systémy, ktoré nariadenie (EÚ) č. 910/2014 neupravuje. Ak je element typu Manifest použitý v aplikáciách podľa nariadenia (EÚ) č. 910/2014, tak len ako alternatívna metóda podľa článku 27 ods. 1 a 2 a 37 ods. 1 a 2 nariadenia (EÚ) č. 910/2014 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. Teda XML podpis s elementom typu Manifest sa nesmie použiť na vytváranie QES pre dôveryhodné služby poskytované verejnosti, ktoré majú vplyv na tretie strany.

ASiC kontajner obsahuje elektronické dokumenty a ich kvalifikované elektronické podpisy, pečate alebo kvalifikované elektronické časové pečiatky dokumentov.

ASiC kontajner je ZIP kontajner so zmenenou koncovkou súboru zo (*.zip) na ASiC koncovky súboru (*.asics, *.scs, *.zip, *.asice, *.sce) a s presne definovanou adresárovou štruktúrou.

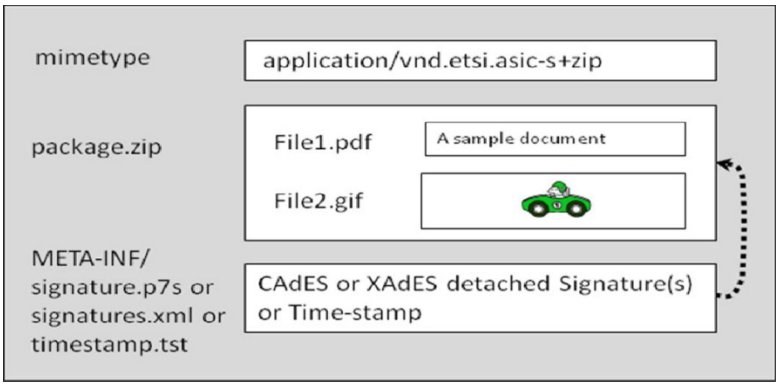
- Podpisy a časové pečiatky dokumentu sú v ZIP adresári „META-INF“.
- Podpísané elektronické dokumenty sú v koreňovom ZIP adresári.

Výhodou ASiC je možnosť komprimovať jeden alebo viacero dokumentov, ktoré sa podpíšu buď spolu v jednom samostatnom ZIP súbore napr. „package.zip“ alebo oddelene ako samostatné súbory pomocou XML podpisu alebo v CMS podpise prostredníctvom súboru „ASiCManifest*.xml“. Dokumenty je možné samostatne alebo prostredníctvom súboru „ASiCManifest*.xml“ časovo opečiatkovať s časovou pečiatkou dokumentu.

ASiC-S CMS/XML kvalifikovaný elektronický podpis alebo kvalifikovaná elektronická časová pečiatka iba z jedného elektronického dokumentu. ASiC-S koncovky súboru (*.asics, *.scs, *.zip)

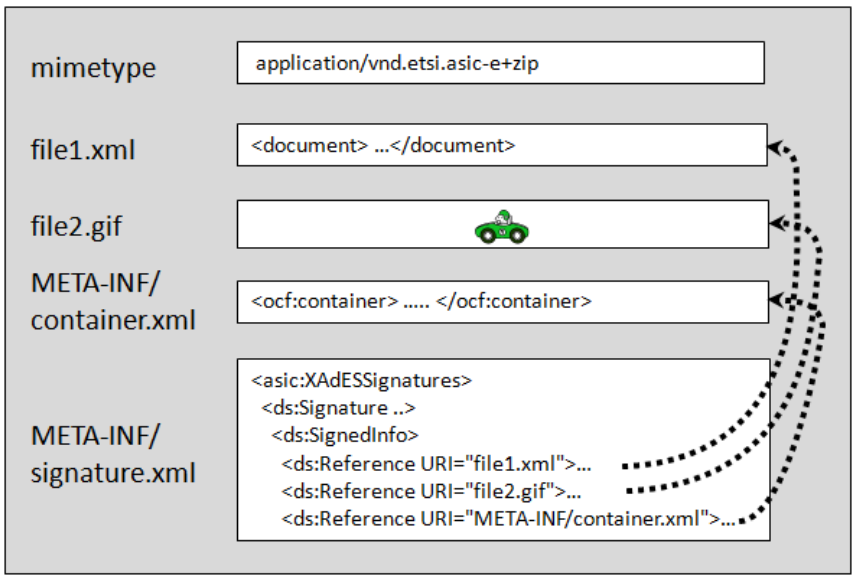
Nasledujúci obrázok znázorňuje obsah ASiC-S ZIP súboru, ktorý obsahuje podpísaný súbor (package.zip). Súbor (mimetype) obsahuje identifikátor ASiC kontajnera. Súbor (package.zip)

obsahuje nasledovné súbory: elektronický dokument (File1.pdf) a elektronický dokument (File2.gif). Súbor (package.zip) je uložený v hlavnom ZIP adresári a je podpísaný CMS podpisom (signature.p7s), XML podpisom (signatures.xml) a časovo opečiatkovaný elektronickou časovou pečiatkou (timestamp.tst). Podpisy a časové pečiatky sú uložené v ZIP adresári (META-INF).



ASiC-E CMS/XML kvalifikovaný elektronický podpis alebo kvalifikovaná elektronická časová pečiatka viacerých elektronických dokumentov. ASiC-E koncovky súboru (*.zip, *.asice, *.sce).

Nasledujúci obrázok znázorňuje obsah ASiC-E ZIP súboru, ktorý obsahuje podpísané elektronické dokumenty v súbore (file1.xml), v súbore (file2.gif) a v súbore (container.xml). Súbor (signature.xml) v adresári (META-INF) obsahuje XML podpis. Súbor (mimetype) obsahuje identifikátor ASiC kontajnera.



Ak sú dokumenty uložené v podpísanom alebo zapečatenom ZIP súbore s názvom „package.zip“, tak uložený elektronický dokument má chránený nielen obsah ale aj názov súboru s koncovkou mena súboru elektronického dokumentu. ASiC definuje aj ďalšiu ochranu v ZIP súbore s názvom „package.zip“ a to ochranu formátu podpisovaného dokumentu pred nesprávnou interpretáciou pomocou MIME *Content-Type* reťazca obsahujúceho len MIME typ a MIME parametre v ZIP položke "file comment" zo ZIP "Central directory structure" podľa kapitoly 4.3.12 ZIP špecifikácie v podpísanom ZIP súbore „package.zip“.

Príklad obsahu ZIP položky "file comment": `mimetype=text/plain; charset=UTF-8`