Deklarácia dodávateľa (výrobcu) aplikácie pre QES, ktorou deklaruje splnenie požiadaviek pri vyhotovovaní, overovaní a validácii QES podľa nariadenia (EÚ) č. 910/2014

Formulár obsahuje prehľad vlastností aplikácie pre kvalifikovaný elektronický podpis/pečať (QES), ktoré deklaruje výrobca aplikácie a ich správnosť môže potvrdiť certifikačný orgán.

Formulár podpisuje/pečatí dodávateľ (výrobca) aplikácie a keďže certifikácia aplikácie je nepovinná, formulár môže podpísať/zapečatiť aj certifikačný orgán. Certifikačným orgánom je orgán posudzovania zhody definovaný v článku 3 ods. 18 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu. Pri certifikácii aplikácie pre QES sa postupuje primerane podľa požiadaviek článkov 27, 37, 32 a 40 nariadenia (EÚ) č. 910/2014 s ohľadom na podmienky vyžadované QSCD zariadením certifikovaným podľa čl. 30 ods. 3 nariadenia (EÚ) č. 910/2014.

Orgán dohľadu dôveryhodných služieb môže deklaráciu výrobcu aplikácie pre QES zverejniť na svojom webovom sídle a poprípade k deklarácii výrobcu uviesť aj zistenia, ktorá získal v rámci dohľadu dôveryhodných služieb a ktoré preskúmal aj v spolupráci s certifikačným orgánom.

Aplikácia pre QES musí vyhotovovať, overovať a poskytovať výsledky procesu validovania QES, len ak formát podpisu/pečate je jedným z formátov uvedených v prílohe vykonávacieho rozhodnutia Komisie (EÚ) 2015/1506 z 8. septembra 2015, 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; ďalej len „rozhodnutie (EÚ) 2015/1506“).

Mapovanie legislatívnych požiadaviek definovaných v nariadení (EÚ) č. 910/2014 do technických postupov je definované v dokumente orgánu dohľadu "schéma dohľadu", kým k niektorým článkom nariadenia (EÚ) č. 910/2014 nie sú vydané nepovinné implementačné akty. Aplikácia pre QES musí v procese validácie preveriť minimálne všetky body postupu pre tvorbu správy výsledku validácie QES definovanej v schéme dohľadu podľa článku 33 nariadenia (EÚ) č. 910/2014 definujúci kvalifikovanú službu validácie kvalifikovaných elektronických podpisov.

Príloha deklarácie dodávateľa (výrobcu) aplikácie pre QES môže obsahovať aj deklaráciu vo forme formulára definovaného v prílohe A medzinárodného štandardu ISO 14533 pre príslušný typ formátu QES.

Dodávateľ (výrobca) aplikácie	Certifikoval

1 Aplikácia pre QES

Údaje o dodávateľovi (výrobcovi)

Obchodné meno: _____

IČO: _____

Adresa: _____

Web adresa: _____

Údaje o aplikácii

Názov aplikácie: _____

Verzia: _____

Požiadavky (OS, …): _____

Web inštalačného balíku: _____

SHA256 hash inštalač. bal.: _____

Hlavný modul aplikácie: _____

SHA256 hash hl. modulu: _____

Názov a SHA256 hash ostatných modulov aplikácie, ak ich nevaliduje hlavný modul aplikácie:

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)

☐ 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 čl. 27 ods. 1 a 2 a čl. 37 od.s 1 a 2 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 nie je v súlade s prílohou rozhodnutia (EÚ) 2015/1506.

☐ Ak je v XML AdES použitý Manifest alebo iné metódy pre alternatívne formáty v súlade s čl. 27 ods. 1 a 2 a čl. 7 ods. 1 a 2 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)
☐/☐ CAdES – (externá PP)
☐/☐ XAdES – EPES (interná PP)
☐/☐ XAdES – (externá PP)
☐/☐ PAdES – EPES (interná PP)
☐/☐ PAdES – (externá PP)
☐/☐ PAdES – DTS (externá PP)
☐/☐ ASiC-S CAdES
☐/☐ ASiC-S XAdES
☐/☐ ASiC-S Time-stamp token (externá PP)
☐/☐ ASiC-E CAdES
☐/☐ ASiC-E XAdES
☐/☐ ASiC-E Time-stamp (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)
☐/☐ CAdES – T (IETF RFC 6960 STS over OCSP)
☐/☐ CAdES – LT
☐/☐ XAdES – T (IETF RFC 3161)
☐/☐ XAdES – T (IETF RFC 6960 STS over OCSP)
☐/☐ XAdES – LT
☐/☐ PAdES – T (IETF RFC 3161)
☐/☐ PAdES – T (IETF RFC 6960 STS over OCSP)
☐/☐ PAdES – LT

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

(Vyhotovuje/ Validuje)

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

Skratky a poznámky:

PP	Podpisová politika (PP) podľa § 11 ods. 1 písm. m) zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) je zverejnená na webovom sídle NBÚ (v ASN.1 formáte v DER kódovaní).
EPES	Aplikácia pracuje s ASN.1 PP, na ktorú odkaz je uvedený v QES, v položke zabezpečenej podpisom, obsahujúcej identifikáciu PP.
externá PP	Ak QES neobsahuje EPES alebo PP expirovala, tak pre validáciu aplikácia získa PP zo zoznamu PP zverejnených NBÚ, platnú v čase, v ktorom bol validovaný objekt preukázateľne vytvorený (napr. čas LTA časovej pečiatky).
STS	Časová pečiatka podpisu, ktorej profil definuje dokument schéma dohľadu.
AdES-T	QES obsahuje (kvalifikovanú elektronickú) časovú pečiatku podpisu.
AdES-DTS	Časová pečiatka dokumentu – definovaná v PDF štandarde ISO 32000.
AdES-LT	Obsahuje T + CRL alebo OCSP odpovede na overenie platnosti certifikátov.
AdES-LTA	QES obsahuje informácie na dlhodobú validáciu a zabezpečenie integrity.

* Formát AdES-LTA, vzhľadom na jeho nedostatky, nie je požadovaný v prílohe vykonávacieho rozhodnutia Komisie (EÚ) 2015/1506, ale jeho novšiu verziu je možné použiť ako jednu z alternatív v "Kvalifikovanej dôveryhodnej službe uchovávania kvalifikovaných elektronických podpisov (pečatí)" profilovanej v kapitole 5.4 v dokumente schéma dohľadu podľa aktuálneho formátu ETSI EN pre CAdES, XAdES a PAdES.

2.5 Podporované nepovinné atribúty, elementy alebo položky chránené QES

(s id- na začiatku sa označujú CMS atribúty) - (bez id- na začiatku sú XML elementy):
(Vyhotovuje/Validuje)

☐/☐ (id-aa-contentHint) ☐/☐ (DataObjektFormat)

☐/☐ (id-aa-ets-signerLocation) ☐/☐ (SignatureProductionPlace)

☐/☐ (id-aa-ets-commitmentType) ☐/☐ (CommitmentTypeIndication)

(Vyhotovuje/ Validuje - PDF entries in a signature dictionary ISO 32000-2)

☐/☐ (Location) ☐/☐ (Reason)

2.6 Vysvetlenia alebo doplňujúce informácie k predošlým bodom:

2.7 Aplikácia podporuje algoritmy a parametre

Pre strojové spracovanie sa bezpečné algoritmy zverejňujú v podpisových politikách na webovom sídle úradu. Odporúčania podľa SOGIS Agreed Cryptographic Mechanisms (pozri http://sogis.org/uk/supporting_doc_en.html).

Algoritmy:

- ☐ sha-256 OID 2.16.840.1.101.3.4.2.1
- ☐ sha-384 OID 2.16.840.1.101.3.4.2.2
- ☐ sha-512 OID 2.16.840.1.101.3.4.2.3
- ☐ sha512-256 OID 2.16.840.1.101.3.4.2.6
- ☐ sha3-256 OID 2.16.840.1.101.3.4.2.8
- ☐ sha3-384 OID 2.16.840.1.101.3.4.2.9
- ☐ sha3-512 OID 2.16.840.1.101.3.4.2.10
- ☐ dsaWithSha256 OID 2.16.840.1.101.3.4.3.2
- ☐ dsa-with-sha384 OID 2.16.840.1.101.3.4.3.3
- ☐ dsa-with-sha512 OID 2.16.840.1.101.3.4.3.4
- ☐ dsa-with-sha3-256 OID 2.16.840.1.101.3.4.3.6
- ☐ dsa-with-sha3-384 OID 2.16.840.1.101.3.4.3.7
- ☐ dsa-with-sha3-512 OID 2.16.840.1.101.3.4.3.8
- ☐ ecdsaWithSHA256 OID 1.2.840.10045.4.3.2
- ☐ ecdsaWithSHA384 OID 1.2.840.10045.4.3.3
- ☐ ecdsaWithSHA512 OID 1.2.840.10045.4.3.4
- ☐ ecdsa-with-sha3-256 OID 2.16.840.1.101.3.4.3.10
- ☐ ecdsa-with-sha3-384 OID 2.16.840.1.101.3.4.3.11
- ☐ ecdsa-with-sha3-512 OID 2.16.840.1.101.3.4.3.12
- ☐ sha256WithRSAEncryption OID 1.2.840.113549.1.1.11
- ☐ sha384WithRSAEncryption OID 1.2.840.113549.1.1.12
- ☐ sha512WithRSAEncryption OID 1.2.840.113549.1.1.13
- ☐ rsaPSS OID 1.2.840.113549.1.1.10
- ☐ rsaEncryption OID 1.2.840.113549.1.1.1
- ☐ ecPublicKey OID 1.2.840.10045.2.1
- ☐ pkcs1-v1_5 sa používa len na validovanie RSA podpisov, ale nie pre vytváranie nových podpisov
- ☐ rsassa-pkcs1-v1_5-with-sha3-256 OID 2.16.840.1.101.3.4.3.14
- ☐ rsassa-pkcs1-v1_5-with-sha3-384 OID 2.16.840.1.101.3.4.3.15
- ☐ rsassa-pkcs1-v1_5-with-sha3-512 OID 2.16.840.1.101.3.4.3.16

Parametre:

RSA veľkosť kľúča _____ minimálne, _____ maximálne.

DSA veľkosť kľúča _____ minimálne, _____ maximálne.

ECDSA veľkosť kľúča _____ minimálne, _____ maximálne.

Elliptic Curve Domain Parameter Identifiers: Brainpool (RFC5639), NIST (FIPS186-4, Appendix D.1.2), FR (JORF)

- ☐ brainpoolP256r1OID 1.3.36.3.3.2.8.1.1.7
- ☐ brainpoolP384r1OID 1.3.36.3.3.2.8.1.1.11
- ☐ brainpoolP512r1OID 1.3.36.3.3.2.8.1.1.13
- ☐ nistp256 OID 1.2.840.10045.3.1.7
- ☐ nistp384 OID 1.3.132.0.34
- ☐ nistp521 OID 1.3.132.0.35
- ☐ FRP256v1 OID 1.2.250.1.223.101.256.1

Meno a OID ďalších podporovaných algoritmov a parametrov:

3 Užívateľské rozhranie

☐ 3.1 Užívateľské rozhranie aplikácie je chránené proti zmene nastavení zobrazenia v systéme (farba, veľkosť okien a fontov, transparentnosť, názvy a veľkosť tlačidiel).

☐ 3.2 Aplikácia sa použije len v bezpečnom prostredí, ktoré je plne pod kontrolou používateľa, nie je chránená proti útokom na operačný systém (zmena fontu, odchytenie PIN, podhodenie falošnej hodnoty pre QSCD na vytvorenie QES alebo vytvorenie viacerých falošných QES).

☐ 3.3 Zmena systémových fontov môže spôsobiť odlišné zobrazenie podpisovaného obsahu pri podpisovaní na rôznych počítačoch a odlišné zobrazenie pri validácii podpisu na rôznych počítačoch.

☐ 3.4 Aplikácia komunikuje s QSCD cez bezpečný kanál, ktorý zabráni modifikácii alebo zmene údajov určených na vytvorenie QES.

☐ 3.5 Aplikácia podporuje zadávanie PIN pre QSCD cez klávesnicu na čítacom zariadení, ktoré zabráni odchyteniu PIN hodnoty (napr. PC/SC v2 with Secure PIN Entry (part 10)).

☐ 3.6 Aplikácia upozorní na nebezpečenstvo zadávania PIN na klávesnici, ak nie je použité bezpečné zadávanie PIN hodnoty (3.5).

☐ 3.7 Aplikácia obsahuje úložisko dôveryhodných certifikátov a ich parametrov pre validáciu certifikačnej cesty.

☐ 3.8 Úložisko dôveryhodných certifikátov je chránené proti neautorizovanej zmene.

Ak áno - Úložisko dôveryhodných certifikátov je chránené:

☐ Podpisom validátora ☐ Podpisom autority (Admin) ☐ Podpisom TL

☐ Inak:

☐ 3.9 Aplikácia je chránená proti zmene svojho kódu.

Ak áno - Spôsob ochrany proti zmene kódu je:

☐ Aplikácia pri štarte kontroluje hashe z komponentov podpísané aplikáciou.

☐ Hashe z komponentov sú podpísané a kontrolujú sa pri štarte aplikácie v OS.

☐ Hashe z komponentov je možné prekontrolovať aj externou aplikáciou.

URL aplikácie _____

☐ Zverejnený je zoznam hash hodnôt z komponent pre externé validovanie externou aplikáciou.

URL aplikácie _____

☐ Inak:

3.10 Vysvetlenia alebo doplňujúce informácie k predošlým bodom

4. Overovanie platnosti certifikátu pri vyhotovovaní, overovaní a validácii QES

☐ 4.1 Pred podpísaním (zapečatením) je umožnené zobraziť certifikát podpisovateľa.
☐ 4.2 Pred podpísaním (zapečatením) je overená platnosť certifikátu podpisovateľa.
☐ Overenie expirovania certifikátu podpisovateľa (tvorcu pečate).

Overenie pomocou ☐ CRL alebo ☐ OCSP.

4.3 Overovanie platnosti certifikátu je zabezpečené pomocou:
☐ CRL ☐ OCSP ☐ Nepriame CRL ☐ OCSP autorizované v TL

☐ OCSP s kontrolovanou pozitívnou odpoveďou (*certHash)*

4.4 Aplikácia má pre validáciu certifikačnej cesty[1] implementovaný nasledovný postup:
☐ 4.4.1. Aplikácia validuje a overuje platnosť kvalifikovaného certifikátu na základe dôveryhodného zoznamu http://ep.nbu.gov.sk/kca/tsl/tsl.xml, ktorý obsahuje "trust anchors" s parametrami definovanými v texte rozhodnutia (EÚ) 2015/1505, napríklad dôveryhodná služba s kvalifikovaným štatútom smie byť použitá len na validovanie a overenie používateľských certifikátov (End Entity) a certifikátov patriacich tejto službe (vydá sama pre seba - rovnaká organizácia).

☐ 4.4.2. Aktuálnosť dôveryhodného zoznamu sa kontroluje podľa času z pečate NBÚ http://ep.nbu.gov.sk/kca/tsl/tsl.xml.p7s .

☐ 4.4.3. Podľa kapitoly 10.3 (Certification path processing procedure - Path processing variables) štandardu ITU-T Rec. X.509 alebo ISO/IEC 9594-8 načíta počiatočné hodnoty premenných na kontrolu certifikačnej cesty z TL elementov definovaných v doplnkovej XSD zdokumentovanej na webovom sídle NBÚ pre TL v dokumente http://ep.nbu.gov.sk/kca/tsl/tlX509XMLSchemaDocumentation.pdf . Sú to elementy: *PrivateKeyUsagePeriod,* ktorý umožňuje skrátiť dobu použitia kľúčového páru dôveryhodnej služby na vydávanie objektov (napr. certifikátov) oproti intervalu z certifikátu dôveryhodnej služby s najdlhšou dobou platnosti počas kvalifikovaného štatútu dôveryhodnej služby, *TLPathLenConstraint*, *TLServiceIdentifier*, *ExplicitAcceptablePolicySet*, *URLContentTypeAndAuthorizedServiceList* a *TrustAnchor*. Na základe týchto údajov použije štandardné validácie podľa kapitoly 10.3 ITU-T Rec. X.509, aby zabránila napríklad chybnému overeniu cez krížové certifikáty alebo aby sa umožnilo automatizované overenie inou autorizovanou kvalifikovanou dôveryhodnou službou v súlade s § 4 zákona 272/2016 Z. z.

☐ 4.4.4. Aplikácia na základe explicitného zoznamu OID certifikačných politík vyžaduje ich prítomnosť vo všetkých certifikátoch certifikačnej cesty[2].

☐ 4.4.5. Ak je v rozšíreniach certifikátu cez *policyConstraints* vyžadované validovanie certifikačných politík cez *policyMapping*, aplikácia validuje certifikačné politiky na základe *policyConstraints*, *certificatePolicy* a *policyMapping*.

☐ 4.5 Aplikácia identifikuje typy kvalifikovaných certifikátov na základe pravidiel uvedených v dokumente schéma dohľadu v kapitole 5.2 "SD prílohy I, III a IV nariadenia (EÚ) č. 910/2014".

[1] Postup podľa "SD čl. 32 a čl. 40 nariadenia (EÚ) č. 910/2014" v dokumente schéma dohľadu.
[2] NBÚ KCA certifikačná politika OID 1.3.158.36061701.0.0.0.1.2.2

☐ 4.6 Aplikácia identifikuje typ podpisu/pečate na základe pravidiel uvedených v dokumente schéma dohľadu v kapitole 5.2 "SD prílohy I, III a IV nariadenia (EÚ) č. 910/2014".
☐ 4.7 Do položiek chránených QES je možné vloženie odkazu na podpisovú politiku.
Ak áno, ☐ pravidlá z podpisovej politiky sú použité pri vytvorení podpisu.
☐ 4.8 Aplikácia umožňuje zobrazenie obsahu podpisovej politiky prevedenej do čitateľnej podoby.
☐ 4.9 Validácia je realizovaná na základe podpisovej politiky, ktorej identifikátor je súčasťou podpisu (chránený QES).
☐ 4.10 Validácia podpisu je realizovaná na základe podpisovej politiky, ktorú si vyberie validátor, ak nie je identifikátor podpisovej politiky súčasťou podpisu.
☐ 4.11 Aplikácia umožňuje pri vytváraní podpisu vloženie časovej pečiatky.
☐ 4.12 Aplikácia umožňuje pri validácii podpisu vloženie časovej pečiatky.
☐ 4.13 Aplikácia validuje vloženú časovú pečiatku pri validácii podpisu.
☐ 4.14 Aplikácia pred vložením časovej pečiatky LTA úrovne súladu dopĺňa podpis a podpisy predošlých časových pečiatok (s vhodnými CRL, OCSP) pre ich overovanie.
☐ 4.15 Aplikácia overuje poslednú časovú pečiatku LTA úrovne (s aktuálnymi CRL, OCSP).
4.16 Vysvetlenia alebo doplňujúce informácie k predošlým bodom:

5 Bezpečný prehliadač

☐ 5.1 Jednoznačné určenie formátu podpisovaného/zapečateného dokumentu zabezpečuje aplikácia pri podpísaní a validácii dokumentu pomocou údajov chránených podpisom. Postupuje sa minimálne v súlade so schémou dohľadu v kapitole "SD čl. 26 a 36 nariadenia (EÚ) č. 910/2014" pre písmeno d) čl. 26 a 36 nariadenia (EÚ) č. 910/2014.
Ochrana formátu podpisovaného dokumentu je pomocou:

☐ MIME ***Content-Type*** reťazca v jednom riadku v CAdES *contentDescription* v *contentHint* atribúte.

Príklad: `Content-Type: text/plain; charset=UTF-8; name="Document.txt"`

☐ MIME ***Content-Type*** reťazca v jednom riadku v XAdES *Description* v *DataObjectFormat* elemente.

Príklad: `Content-Type: text/plain; charset=UTF-8; name="Document.txt"`

☐ MIME ***MimeType*** v XAdES *MimeType* v *DataObjectFormat* elemente.

Príklad: `<xades:MimeType>application/pdf</xades:MimeType>`

☐ MIME ***Content-Type*** reťazca obsahujúceho len MIME typ a parametre v položke "file comment" z "4.3.12 Central directory structure" v podpísanom ZIP súbore. ETSI EN 319 162-1, kapitola 4.3.2 a príloha B.1.3

Príklad: `mimetype=text/plain; charset=UTF-8`

☐ Iné:

☐ 5.2 Aplikácia podpisuje/validuje a zobrazuje formáty dokumentov vymenované v § 57a až § 57d výnosu č. 55/2014 Z. z. podľa prílohy č. 12 k výnosu č. 55/2014 Z. z. v bezpečnom prehliadači vo všetkých verziách aplikácie rovnako.
Hodnoty pre identifikovanie formátu podpísaného elektronického dokumentu

Podpísaný elektronický dokument podľa	**Identifikátor vo forme prípony súboru**	**Identifikátor vo forme položky "Content-type" v elektronickom podpise**
§ 57a písm. a) a b) prvého bodu	☐ .pdf	application/pdf
§ 57a písm. b) druhého bodu	☐ .txt	text/plain; charset=UTF-8
§ 57a písm. b) tretieho bodu	☐ .png	image/png
§ 57a písm. c)	☐ .xml	application/vnd.gov.sk.xmldatacontainer+xml; charset=UTF-8

Hodnoty pre identifikovanie formátu podpisového kontajnera

Podpisový kontajner	**Identifikátor vo forme prípony súboru**	**Identifikátor vo forme položky "Content-type" v elektronickom podpise**
§ 57b písm. a)	☐ .asics, .scs	application/vnd.etsi.asic-s+zip
§ 57b písm. a), podpísaný ZIP kontajner 4.3.2 a B.1.3 ETSI EN 319 162-1	☐ .zip	application/zip
§ 57b písm. a), rozšírený podpisový kontajner	☐ .asice, .sce	application/vnd.etsi.asic-e+zip

☐ 5.3 Pri podpísaní/validovaní a zobrazení iného formátu dokumentu, než je uvedený v § 57a písm. a) až c), §57b písm. a) výnosu č. 55/2014 Z. z., umožní nastaviť možnosť zobraziť upozornenie.

☐ 5.4 Aplikácia okrem predchádzajúcich formátov podpisuje/validuje a zobrazuje nasledovné formáty dokumentov. Formáty dokumentov sú uvedené v tvare (identifikátor vo forme prípony súboru, identifikátor vo forme položky "Content-type" v elektronickom podpise):

5.5 Vysvetlenia alebo doplňujúce informácie k predošlým bodom:

6 Doplňujúce informácie

6.1 Aplikácia môže byť použitá len pri splnení nasledovných obmedzení:

6.2 Podporované certifikované QSCD pre vyhotovovanie QES:

6.3 Prílohy: (napr. v tvare http adresa prílohy, hash SHA256 z prílohy):

6.4 Ďalšie prílohy: