SPRÁVA ZÁKLADNÍCH REGISTRŮ	SZRAX003VJ2W prvotní identifikátor	
	SZR- 5090-2/Ř-2022	
	POL028--2022	
POLITIKA	počet stran	18
	přílohy	1

NCA – Politika ověřování podpisu NCA QVerify v 1.0

Oblast působnosti:
Zaměstnanci vybraných subjektů veřejné správy, mezi které patří bezpečností složky, zpravodajské služby a vybrané útvary resortu Ministerstva vnitra.

Gestor: Ing. Radovan PÁRTL	**Nahrazuje:** -
Zpracovatel: Ing. Jitka VÁLOVÁ	**Klasifikace:** VEŘEJNÝ
Odborný garant: RNDr. Miroslav ŠEDIVÝ	**Schváleno dne:** 09. 09. 2022
Schvalovatel: *podepsáno elektronicky* Ing. Michal PEŠEK	**Účinnost od dne:** 12. 09. 2022

HISTORIE DOKUMENTU:

ID	Verze	Datum	Autor	Popis
-	1.00	23.08.2022	První certifikační autorita, a.s.	Vytvoření první verze dokumentu.

OBSAH

1 ÚVOD

1.1 Přehled

Tento dokument popisuje politiku ověřování podpisu (signature validation policy) používanou v rámci služby pro ověřování elektronického podpisu NCA QVerify.

Dokument specifikuje omezení a kontroly, které jsou aplikovány v rámci procesu ověřování elektronického podpisu a na jejichž vyhodnocení závisí výsledek ověření.

1.2 Název a identifikace dokumentu

Název a identifikace dokumentu: Politika ověřování podpisu NCA QVerify v1.0

OID politiky: 1.2.203.72054506.20.1.0

1.3 Reference

[EN319102] ETSI EN 319 102-1 V1.3.1 (2021-11): „Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation“

[eIDAS] Nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářející důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES

[TS103171] ETSI TS 103 171 V2.1.1 (2012-03): „Electronic Signatures and Infrastructures (ESI);XAdES Baseline Profile“

[TS103172] ETSI TS 103 172 V2.2.2 (2013-04): „Electronic Signatures and Infrastructures (ESI);PAdES Baseline Profile“

[TS103173] ETSI TS 103 173 V2.2.1 (2013-04): „Electronic Signatures and Infrastructures (ESI);CAdES Baseline Profile“

[EN319122] ETSI EN 319 122-1 V1.2.1 (2021-10): “Electronic Signatures and Infrastructures (ESI) CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures”

[EN319132] ETSI EN 319 132-1 V1.2.1 (2022-02): “Electronic Signatures and Infrastructures (ESI) XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures”

[EN319142] ETSI EN 319 142-1 V1.1.1 (2016-04): “Electronic Signatures and Infrastructures (ESI) PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures”

[RFC5280] IETF RFC 5280 (May 2008): „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“

[FIPS1804] FIPS Publication 180-4 (August 2015): „Secure Hash Standard (SHS)“

[RFC8017] Specifications	IETF RFC 8017 (November 2016): „PKCS #1: RSA Cryptography Version 2.2“
[RFC3161] Infrastructure	IETF RFC 3161 (August 2001): „Internet X.509 Public Key Time-Stamp Protocol (TSP)“
[TS119172] table of	ETSI TS 119 172-1 V1.1.1 (2015-07): „Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and contents for humanreadable signature policy documents“
[EN319411-2] Service	ETSI EN 319 411-2 V2.4.1 (2021-11): „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates“
[ANSX962]	ANS X9.62-2005: „Public Key Cryptography for the Financial Services Industry; The Elliptic Curve Digital Signature Algorithm (ECDSA)“
[TR102272]	ETSI TR 102 272 V1.1.1 (2003-12): „Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies“

1.4 Zkratky

AdES	Advanced Electronic Signature
BSP	Business Scoping Parameter
CA	Certifikační Autorita
CAdES	CMS Advanced Electronic Signature
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DA	Driving Application
eIDAS	Nařízení Evropského parlamentu a Rady č. 910/2014
EU	Evropská Unie
LoA	Level of Assurance
NCA	Národní certifikační autorita
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
PAdES	PDF Advanced Electronic Signature
PKIX	Public-Key Infrastructure (X.509)
QVerify	Aplikace realizující ověřování podpisů popsaných v tomto dokumentu
SVA	Signature Validation Application
TA	Trust Anchor
TSP	Trust Service Provider
XAdES	XML Advanced Electronic Signature
XML	eXtensible Markup Language

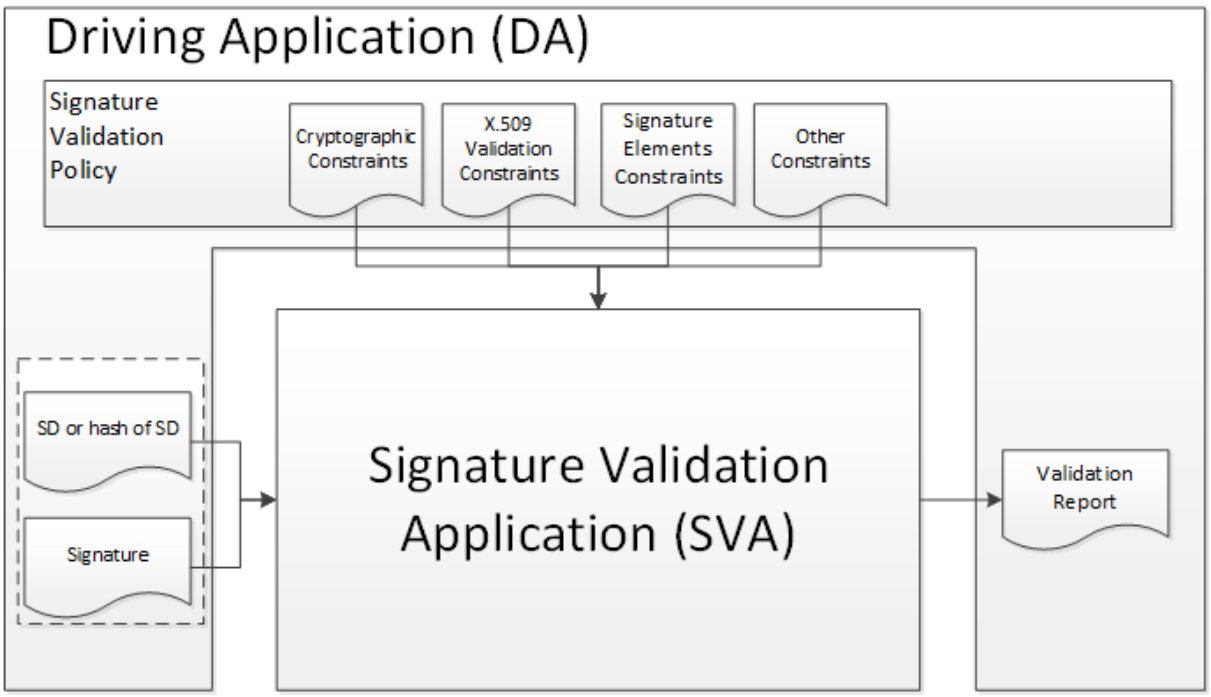
2 OVĚŘOVÁNÍ PODPISU

Realizace ověřování elektronického podpisu v NCA QVerify je řešena v souladu s ETSI EN 319 102-1 [EN319102] a je určena pro ověřování elektronických podpisů založených na

certifikátech jejichž certifikační autorita je provozována v souladu s normou ETSI EN 319 411-2 [EN319411-2].

V této kapitole jsou dále popsány způsoby realizace jednotlivých ověřovacích procesů a stavebních bloků normy ETSI EN 319 102-1 [EN319102].

2.1 Model ověřování podpisu



Obrázek 1: Konceptuální model ověřování podpisu (převzato z [EN319102])

Služba NCA QVerify respektuje model z obrázku 1, tedy rozdělení na Driving Application (DA) a Signature Validation Application (SVA), přičemž DA je realizována serverovou aplikací a klientskou komponentou. SVA je pak tvořena definovaným rozhraním výkonných knihoven ICACrypt2, ICAPades2 a ICACryptXML.

Tato politika se nadále zabývá procesy probíhajícími v SVA.

2.2 Vstupy ověření

2.2.1 Ověřovaný podpis

NCA QVerify pracuje v tzv. rozděleném modelu ověřování, což znamená, že do SVA neputují kompletní podepisovaná data, ale pouze jejich reprezentace v podobě proprietární datové struktury zvané SignedDataSummary. Přesná podoba této datové struktury se liší podle ověřovaného formátu podpisu. V každém případě je tato struktura připravená klientskou komponentou tedy DA a obsahuje vždy minimálně ověřovaný elektronický podpis (případně elektronické podpisy) a kryptografický otisk (dále hash) podepisovaných dat ve formátu použitelném pro další proces ověřování.

2.3 Podporované formáty ověření

NCA QVerify dle této politiky podporuje ověřování podpisů formátů

- XAdES dle ETSI TS 103 171 [TS103171] v úrovni shody B, T a LT,
- PAdES dle ETSI TS 103 172 [TS103172] v úrovni shody B, T, LT a LTA,
- CAdES dle ETSI TS 103 173 [TS103173] v úrovni shody B, T a LT,
- CAdES dle ETSI EN 319 122-1 [EN319122] v úrovni shody B-B, B-T, B-LT a B-LTA,
- XAdES dle ETSI EN 319 132-1 [EN319132] v úrovni shody B-B, B-T a B-LT,
- PAdES dle ETSI EN 319 142-1 [EN319142] v úrovni shody B-B, B-T, B-LT a B-LTA,

se specifickými omezeními uvedenými níže.

2.3.1 Omezení ověřovaných podpisů formátu XAdES

NCA QVerify dle této politiky podporuje podpisy XAdES v úrovni shody B, T a LT resp. B-B, B-T a B-LT, přičemž jsou podporovány properties `xades:SigningCertificate`, `xades:SigningTime`, `xades:SignatureTimeStamp`, `xades:CertificateValues` a `xades:RevocationValues`. Dále je podporována property `xades:SignaturePolicyIdentifier`, přičemž rozsah podporovaných podpisových politik je specifikován níže. Ve specifikaci použité podpisové politiky nejsou podporovány transformace viz ETSI EN 319 132 [EN319132] kapitola 5.2.9.1.

Jakékoliv jiné properties v XAdES podpisu jsou během procesu ověření ignorovány a neprovádí se jejich kontrola.

2.3.2 Omezení ověřovaných podpisů formátu PAdES

NCA QVerify dle této politiky podporuje podpisy PAdES v úrovni shody B, T, LT a LTA resp. B-B, B-T, B-LT a B-LTA, přičemž ve vložené CMS podpisové struktuře jsou podporovány atributy `content-type`, `signing-certificate` (tedy `ESS signing-certificate` resp. `ESS signing-certificate v2`), `message-digest` a `signature-time-stamp`. Dále je prováděna kontrola přítomnosti `signature-policy-identifier`, nicméně podpisy s definovanou podpisovou politikou nejsou podporovány. Uvnitř struktury PDF se dále kontroluje přítomnost dokumentového časového razítka (`document-time-stamp`), které je taktéž akceptováno pro úrovně T a B-T. Validační data pro LT resp. B-LT úroveň podpisu jsou pro ověření extrahovány ze struktury PDF z dictionary DSS.

Podpisy v úrovni shody T a B-T vyžadují přítomnost alespoň jednoho časového razítka. Do množiny časových razítek pro daný podpis jsou zařazena a) časová razítka umístěná uvnitř vložené CMS podpisové struktury (atribut `signature-time-stamp`), b) dokumentová časová razítka (`document-time-stamp`) vložená do dokumentu po příslušném podpisu, a tedy pokrývající daný podpis.

NCA QVerify provádí kontrolu, že PAdES podpis pokrývá celou revizi PDF dokumentu. U posledního vloženého podpisu se navíc provádí kontrola, že pokrývá celý PDF dokument. Příslušné normy nicméně povolují dodatečné přidání validačních dat do dokumentu po posledním podpisu - v takovém případě už poslední podpis nebude pokrývat celý dokument. NCA QVerify proto v případě, že poslední podpis nepokrývá celý dokument, provádí kontrolu, zda změny provedené v PDF dokumentu po posledním podpisu skutečně zahrnují pouze

přidání validačních dat. V rámci přidání validačních je též povolena úprava metadat uložených v PDF dokumentu.

Jakékoliv jiné atributy ve vložené CMS struktuře jsou během procesu ověření ignorovány a neprovádí se jejich kontrola.

2.3.3 Omezení ověřovaných podpisů formátu CAdES

NCA QVerify dle této politiky podporuje podpisy CAdES v úrovni shody B,T a LT resp. B-B, B-T, B-LT a B-LTA, přičemž jsou v podpisech podporovány atributy `content-type`, `signing-time`, `signing-certificate` (tedy `ESS signing-certificate` resp. `ESS signing-certificate v2`), `message-digest`, `signature-time-stamp`, `ats-hash-index-v3` a `archive-time-stamp-v3`. Dále je prováděna kontrola přítomnosti `signature-policy-identifier`, nicméně podpisy s definovanou podpisovou politikou nejsou podporovány. Validační data pro LT resp. B-LT úroveň podpisu jsou pro ověření extrahovány z položek `SignedData.certificates`, `SignedData.crls.crl` a `SignedData.crls.other`.

Jakékoliv jiné atributy v CAdES podpisu jsou během procesu ověření ignorovány a neprovádí se jejich kontrola.

2.3.4 Omezení podpory podpisových politik.

Podpisové politiky jsou podporovány pouze v DER formátu dle ETSI TR 102 272 [TR102272], přičemž z možný parametrů podpisové politky jsou podporovány pouze:

- V sekci signerAndVerifierRules/signerRules:
  - externalSignedData
  - mandatedSignedAttr
  - mandatedUnsignedAttr
  - mandatedCertificateInfo
  - mandatedCertificateRef
- V sekci signerAndVerifierRules/verfierRules:
  - mandatedUnsignedAttr
- V sekci timeStampTrustContition:
  - cautionPeriod
- Sekce algorithmConstraintSet

Jelikož služba NCA QVerify nikam nevrací ověřovaný podpis, není možné aplikovat případná pravidla požadující doplnění nepodepisovaných atributů během ověřování (VerifierRules/mandatedUnsignedAttr), tyto pravidla jsou proto ignorována.

Vzhledem k tomu, že ASN.1 podpisová politika je určena primárně pro podpisy typu CMS, je pro podpisy XAdES aplikováno mapování ASN.1 atributů na XML elementy shodného významu podle tabulky v příloze 4.1.

2.4 Výběr validačního procesu

Validační proces pro daný ověřovaný podpis je volitelný z DA. NCA QVerify dle této politiky podporuje tři validační procesy a to Validační proces pro základní podpisy (Validation Process for Basic Signatures), Validační proces pro podpisy s časem a podpisy s validačními daty

(Validation proces for Signatures with Time and Signatures with Long-Term Validation Material) a Validační proces pro podpisy poskytující dlouhodobou dostupnost a integritu validačních dat (Validation process for Signatures providing Long Term Availability and Integrity of Validation Material). Požadavek na ověření pomocí jiného validačního procesu není v souladu s touto politikou a bude zamítnut.

2.5 Základní stavební bloky (Basic building blocks)

Tato kapitola popisuje realizaci a specifika zpracování jednotlivých základních stavebních bloků

2.5.1 Kontrola formátu (Format Checking)

Tento stavební blok provádí základní kontrolu formátu. Pokud je vstupní podpis možné naparsovat pro další zpracování je výsledkem bloku indikace PASSED.

2.5.2 Identifikace podpisového certifikátu (Identification of the signing certificate)

Tento stavební blok provádí určení podpisového certifikátu pomocí podepisovaného atributu (elementu), který je součástí podpisu. Identifikovaný podpisový certifikát se hledá primárně přímo v podpisu, je však možné jej předat do SVA i externě.

2.5.3 Inicializace validačního kontextu (Validation context initialization)

Blok inicializace validačního kontextu provádí kontrolu na přítomnost elementu/atributu SignaturePolicyIdentifier. Pokud je tento v podpisu přítomen, tak je v případě XAdES podpisu referencovaná podpisová politika získána a ověřena vůči otisku podpisové politiky uvedeném v elementu SignaturePolicyIdentifier. Obsah této politiky je následně ověřen vůči omezením podpory podpisových politik (viz 2.3.4). Pokud se nepodaří získat referencovanou podpisovou politiku, tak je výsledkem bloku indikace INDETERMINATE se subindikací SIGNATURE_POLICY_NOT_AVAILABLE. Pokud otisk získané podpisové politiky neodpovídá naplnění elementu SignaturePolicyIdentifier, nebo tato podpisová politika obsahuje nepodporované položky, tak je výsledkem tohoto bloku indikace INDETERMINATE se subindikací POLICY_PROCESSING_ERROR.

Pokud je u výše neuvedených formátů podpisů nalezen element/atribut SignaturePolicyIdentifier, tak je výsledkem bloku indikace INDETERMINATE se subindikací POLICY_PROCESSING_ERROR.

Tato politika nedefinuje přímo množiny důvěryhodných kotev (důvěryhodných kořenových certifikátů) pro podpisy a časová razítka. Množiny důvěryhodných kotev jsou nastavovány při inicializaci SVA z DA a to separátně pro ověření elektronických podpisů a pro ověření časových razítek. Přičemž tato politika klade požadavek, aby se v případě důvěryhodných kotev pro elektronické podpisy vždy jednalo pouze o certifikační autority poskytující kvalifikované certifikáty dle [eIDAS] a v případě důveryhodných kotev pro časová razítka o poskytovatele služeb kvalifikovaných časových razítek nebo elektronických časových razítek dle [eIDAS].

Validační kontext je tvořen sloučením pravidel definovaných touto politikou a důvěryhodných kotev definovaných z DA.

2.5.4 Kontrola čerstvosti revokačních dat (Revocation freshness checker)

Tento stavební blok provádí kontrolu čerstvosti validačních dat. Realizace v SVA NCA QVerify provádí kontrolu čerstvosti čistě na základě položky nextUpdate. Pokud je čas ověření podpisu mezi thisUpdate a nextUpdate je výsledkem bloku indikace PASSED. Pokud není součástí nejaktuálnějšího dostupného CRL nebo OCSP položka nextUpdate je výsledkem bloku indikace FAILED.

2.5.5 Ověření certifikátu (X.509 certificate validation)

Blok ověření platnosti certifikátu probíhá dle PKIX Certification Path Validation z IETF RFC 5280 [RFC5280], kapitola 6.1 dle shell modelu, tedy modelu kdy všechny certifikáty jsou platné v okamžiku ověřování.

V případě spuštění s parametrizací pro ověřování elektronického podpisu:

Podpisový certifikát musí obsahovat položku KeyUsage s nastavenými bity digitalSignature(0) a nonRepudiation(1). Pokud je v podpisovém certifikátu uvedena položka ExtendedKeyUsage (stejně jako KeyUsage definována v IETF RFC 5280 [RFC5280]) musí být buďto nastavena na hodnotu anyExtendedKeyUsage, nebo musí obsahovat alespoň jednu z hodnot emailProtection (1.3.6.1.5.5.7.3.4) a msDocumentSigning (1.3.6.1.4.1.311.10.3.12). Nesplnění těchto požadavků způsobí výslednou indikaci tohoto bloku INDETERMINATE se subindikací CHAIN_CONSTRAINTS_FAILURE.

Podpisový certifikát musí obsahovat rozšíření esi4-qcStatement-1 (id-etsi-qcs-QcCompliance) (0.4.0.1862.1.1). Nesplnění tohoto požadavku způsobí výslednou indikaci tohoto bloku INDETERMINATE se subindikací CHAIN_CONSTRAINTS_FAILURE.

Pokud je v podpisovém certifikátu uvedeno rozšíření esi4-qcStatement-6 (id-etsi-qcs-QcType) (0.4.0.1862.1.6), tak musí obsahovat hodnotu id-etsi-qct-esign (0.4.0.1862.1.6.1) nebo hodnotu id-etsi-qct-eseal (0.4.0.1862.1.6.2). Nesplnění tohoto požadavku způsobí výslednou indikaci tohoto bloku INDETERMINATE se subindikací CHAIN_CONSTRAINTS_FAILURE.

Certifikát je kontrolován proti množině důvěryhodných kotev (předané z DA) určených pro ověření elektronických podpisů.

V případě spuštění s parametrizací pro ověřování časového razítka:

Podpisový certifikát musí obsahovat položku KeyUsage s nastavenými bity digitalSignature(0) a nonRepudiation(1). V podpisovém certifikátu musí být v položce ExtendedKeyUsage uvedena hodnota timestamping (1.3.6.1.5.5.7.3.8). Nesplnění tohoto požadavku způsobí výslednou indikaci tohoto bloku INDETERMINATE se subindikací CHAIN_CONSTRAINTS_FAILURE.

Certifikát časového razítka musí být uveden na seznamu důvěryhodných TSU certifikátů (předaném z DA). Nesplnění tohoto požadavku způsobí výslednou indikaci tohoto bloku INDETERMINATE se subindikací CHAIN_CONSTRAINTS_FAILURE.

Certifikát je kontrolován proti množině důvěryhodných kotev (předané z DA) určených pro ověření časových razítek.

2.5.6 Kryptografické ověření (Cryptographic verification)

Blok kryptografického ověření podpisu probíhá v NCA QVerify zpravidla vůči hashi podepsaných dat. Samotné ověření probíhá dle specifikace norem ETSI TS 103 171 [TS103171], ETSI TS 103 172 [TS103172], ETSI TS 103 173 [TS103173], ETSI TS 103 174 [TS103174] potažmo ETSI EN 319 122-1 [EN319122], ETSI EN 319 132-1 [EN319132], ETSI EN 319 142-1 [EN319142] a ETSI EN 319 162-1 [EN319162].

2.5.7 Ověření akceptace podpisu (Signature Acceptance validation)

NCA QVerify dle této politiky akceptuje podpisy realizované pomocí následujících algoritmů:

- Hash algoritmy rodiny SHA-2 (SHA-224, SHA-256, SHA-384 a SHA-512) definované ve FIPS 180-4 [FIPS1804]
- Podpisový algoritmus RSA o velikosti klíče minimálně 2048b definovaný v RFC 8017 [RFC8017]
- Podpisový algoritmus RSASSA-PSS o velikosti klíče minimálně 2048b definovaný v RFC 8017 [RFC8017]
- Podpisový algoritmus ECDSA o velikosti klíče minimálně 224b definovaný v ANS X9.62-2005 [ANSX962] (pouze pro PAdES, CAdES)

Pro podpisy realizované pomocí jiného algoritmu bude výsledkem tohoto bloku indikace INDETERMINATE se subindikací CRYPTO_CONSTRAINTS_FAILURE_NO_POE.

Zpracování atributu/elementu SigningCertificate je v souladu s příslušnými normami pro daný formát podpisu. Pokud element SigningCertificate obsahuje více referencí na certifikáty a minimálně jeden z těchto certifikátů není součástí certifikační cesty k podpisovému certifikátu je výsledkem tohoto bloku indikace INDETERMINATE se subindikací SIG_CONSTRAINTS_FAILURE. Vyjímku z tohoto pravidla tvoří atributové certifikáty, kdy přítomnost jejich reference v SigningCertificate je tolerována za předpokladu, že se tentýž atributový certifikát nachází mezi atributovými certifikáty v podpisu. Atributové certifikáty však nejsou dále nijak zpracovávány ani ověřovány.

Atribut/element SigningTime (položka M SignatureDictionary v případě PAdES) není přímo zpracovávána pomocí SVA, ale její hodnota je zpřístupněna DA pro případné další zpracování.

Pokud byla v předchozích blocích získána podpisová politika, tak v tomto bloku dojde ke kontrole podpisu vůči jejím parametrům. V případě, že neodpovídá nějaký předepsaný parametr ze sekce signerAndVerifierRules je výsledkem tohoto bloku indikace INDETERMINATE se subindikací SIG_CONTRAINTS_FAILURE. Pokud neodpovídá nějaký předepsaný parametr sekce algorithmConstraintSet je výsledkem tohoto bloku indikace INDETERMINATE se subindikací CRYPTO_CONSTRAINTS_FAILURE_NO_POE.

Žádné další AdES atributy z kapitoly 5.2.8.4.2 normy ETSI EN 319 102-1 [EN319102] nejsou dle této politiky zpracovávány a jejich přítomnost v podpisu je ignorována.

Vzhledem k závislosti množiny důvěryhodných kotev pro ověření elektronického podpisu na best-signature-time, který není možné před spuštěním ověřovacího procesu určit je v rámci tohoto bloku provedena kontrola důvěryhodnosti vydavatele podpisového certifikátu vůči času best-signature-time. Pokud tato kontrola prokáže, že daný podpisový certifikát nelze v okamžiku best-signature-time považovat za důvěryhodný je výsledkem tohoto bloku indikace INDETERMINATE se subindikací SIG_CONSTRAINTS_FAILURE.

2.5.8 Prezentace ověření podpisu (Signature validation presentation)

Blok prezentace ověření podpisu není dle této politiky součástí ověřovacího procesu SVA NCA QVerify.

2.6 Validační proces pro základní podpisy (Validation Process for Basic Signatures)

Realizace validačního procesu pro základní podpisy probíhá dle ETSI EN 319 102-1 [EN319102], kapitola 5.3 kde realizace jednotlivých stavebních bloků v souladu s touto politikou je uvedena v předchozích kapitolách.

Validační process může být spuštěn s parametrizací ověřovaného podpisu buďto pro ověřování elektronického podpisu, nebo pro ověřování časového razítka.

2.7 Stavební blok ověření časového razítka (Time-stamp validation building block)

Blok ověření časového razítka provádí ověření časových razítek dle normy RFC 3161 [RFC3161] a to pomocí validačního procesu pro základní podpisy parametrizovaného pro ověřování časového razítka.

V případě aplikace podpisové politiky (podmínky aplikace výše v dokumentu) obsahující specifikaci timeStampTrustCondition/cautionPeriod je ověření v rámci tohoto bloku prováděno s aplikováním příslušné cautionPeriod.

2.8 Validační proces pro podpisy s časem a podpisy s validačními daty (Validation proces for Signatures with Time and Signatures with Long-Term Validation Material)

Realizace validačního procesu pro podpisy s časem a podpisy s validačními daty probíhá dle ETSI EN 319 102-1 [EN319102], kapitola 5.5 kde realizace jednotlivých stavebních bloků v souladu s touto politikou je uvedena v předchozích kapitolách.

Jako zdroj důkazu existence v čase pro podpisy s časem (Signatures with Time) je využíván obsah atributů/elementů SignatureTimeStamp v souladu s příslušnými normami pro daný formát. V případě PAdES podpisů jsou taktéž akceptovány dokumentová časová razítka (Document TimeStamp) umístěná ve struktuře podpisu. Jedno dokumentové časové razítko může být využito jako důkaz existence v čase pro více samostatných podpisů v souladu s principem realizace dokumentového časového razítka dle příslušných norem.

Pokud je validační proces spuštěn na podpis bez časových razítek, nebo není žádné z časových razítek vyhodnoceno jako platné je výsledkem validačního procesu výsledek validačního procesu pro základní podpisy.

Tato politika nedefinuje žádná dodatečná omezení na platnost vložených časových razítek (tj. neplatné časové razítko bude v dalším procesu ověřování ignorováno) ani na time-stamp delay.

2.9 Validační proces pro podpisy poskytující dlouhodobou dostupnost a integritu validačních dat (Validation process for Signatures providing Long Term Availability and Integrity of Validation Material)

Tato kapitola popisuje realizaci a specifika validačního procesu pro podpisy poskytující dlouhodobou dostupnost a integritu validačních dat. Proces využívá dodatečné stavební bloky definované v kapitole 2.9.1.

2.9.1 Dodatečné stavební bloky (Additional building blocks)

2.9.2 Ověření certifikátu v minulosti (Past certificate validation)

Tento stavební blok provádí ověření certifikátu vůči času v minulosti. Realizace stavebního bloku probíhá dle ETSI EN 319 102-1 [EN319102], kapitola 5.6.2.1.

2.9.3 Posun času ověření (Validation time sliding process)

Tento stavební blok provádí posun času ověření z aktuálního času na nějaký čas v minulosti pokaždé, když narazí na revokovaný certifikát, kryptografický algoritmus, který není nadále považovaný za bezpečný, nebo revokační informaci, pro níž selže kontrola čerstvosti. Realizace stavebního bloku probíhá dle ETSI EN 319 102-1 [EN319102], kapitola 5.6.2.2.

2.9.4 Extrakce POE (POE extraction)

Tento stavební blok provádí odvození hodnoty POE z příslušného časového razítka. Časové razítko poskytuje POE pro všechny objekty, které jsou tímto razítkem pokryty. Realizace stavebního bloku probíhá dle ETSI EN 319 102-1 [EN319102], kapitola 5.6.2.3.

2.9.5 Ověření podpisu v minulosti (Past signature validation building block)

Tento stavební blok se používá pro ověření podpisu v minulosti. Realizace stavebního bloku probíhá dle ETSI EN 319 102-1 [EN319102], kapitola 5.6.2.4.

2.9.6 Validační proces pro podpisy poskytující dlouhodobou dostupnost a integritu validačních dat (Validation Process for Signatures providing Long Term Availability and Integrity of Validation Material)

Realizace validačního procesu pro podpisy poskytující dlouhodobou dostupnost a integritu validačních dat probíhá dle ETSI EN 319 102-1 [EN319102], kapitola 5.6.3, kde realizace jednotlivých stavebních bloků v souladu s touto politikou je uvedena v předchozích kapitolách.

Evidenční záznamy (Evidence Records) dle RFC 4998 a RFC 6283 nejsou podporovány. I v případě, že validační proces pro podpisy s časem a podpisy s validačními daty provedený

v kroku 2 skončí výsledkem PASSED, provedou se všechny zbývající kroky validačního procesu pro podpisy poskytující dlouhodobou dostupnost a integritu validačních dat.

3 OMEZENÍ DEFINOVANÁ V ETSI TS 119 172-1

Tato kapitola popisuje realizaci omezení definovaných v normě ETSI TS 119 172-1 [TS119172].

3.1 Identita podepisujícího

Tato kapitola popisuje realizaci omezení BSP (m) – Identity of signers, kapitola A.4.2.1, tabulka A.2.

Constraint(s)	Constraint value at signature validation (SVA or DA)
(m)1. X509CertificateValidationConstraints: This set of constraints indicates requirements for use in the certificate path validation process as defined in IETF RFC 5280 [i.13]. These constraints may be different for different certificate types (e.g. certificates issued to signer, to CAs, to OCSP responders, to CRL Issuers, to Time-Stamping Units). Semantic for a possible set of requirement values used to express such requirements is defined as follows:	
• (m)1.1. SetOfTrustAnchors: This constraint indicates a set of acceptable trust anchors (TAs) as a constraint for the validation process. Such TAs should be provided in the form of (self-signed) certificates (see clause 6.1.1 of IETF RFC 5280 [i.13] on how to treat such certificates as conveyor of TA information) and a time until when these trust anchors were considered reliable.	Sada důvěryhodných kotev předávaná z DA.
• (m)1.2. CertificationPath: This constraint indicates a certification path required to be used by the SVA for validation of the signature. The certificate path is of length 'n' from the trust anchor (TA) down to the certificate used in validating a signed object (e.g. the signer's certificate or a time stamping certificate). This constraint can include the path to be considered or indicate the need for considering the path provided in the signature if any.	Certifikační cesta se sestavuje z certifikátů obsažených v podpisu a certifikátů poskytnutých z DA.
• (m)1.3. user-initial-policy-set: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (c) [i.13].	Ne
• (m)1.4. initial-policy-mapping-inhibit: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (e) [i.13].	Ne
• (m)1.5. initial-explicit-policy: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (f) [i.13].	Ne

• (m)1.6. initial-any-policy-inhibit: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (g) [i.13].	Ne
• (m)1.7. initial-permitted-subtrees: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (h) [i.13].	Ne
• (m)1.8. initial-excluded-subtrees: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (i) [i.13].	Ne
• (m)1.9. path-length-constraints: This constraint indicates restrictions on the number of CA certificates in a certification path [i.13]. This may need to define initial values for this or to handle such constraint differently (e.g. ignore it).	Ne
• (m)1.10. policy-constraints: This constraint indicates requirements for certificate policies referenced in the certificates [i.13]. This may need to define initial values for this or to handle such constraint differently (e.g. ignore it). This should also allow the ability to require a (possible set of) specific certificate policy extension value(s) in end-entity certificates (without requiring such values appearing in certificate of authorities in the certification path).	Ne
(m)2. RevocationConstraints: This set of constraints indicates requirements applicable when verifying the certificate validity status of the certificates during the certificate path validation process [i.13]. These constraints may be different for different certificate types (e.g. certificates issued to signer, to CAs, to OCSP responders, to CRL Issuers, to Time-Stamping Units). Semantic for a possible set of requirement values used to express such requirements is defined as follows:	
• (m)2.1. RevocationCheckingConstraints: This constraint indicates requirements for checking certificate revocation. Such constraints may specify if revocation checking is required or not and if OCSP responses or CRLs have to be used. Semantic for a possible set of requirement values used to express such requirements is defined as follows: − clrCheck: Checks shall be made against current CRLs (or Authority Revocation Lists); − ocspCheck: The revocation status shall be checked using OCSP IETF RFC 6960 [i.14]; − bothCheck: Both OCSP and CRL checks shall be carried out; − eitherCheck: Either OCSP or CRL checks shall be carried out; − noCheck: No check is mandated.	eitherCheck
• (m)2.2. RevocationFreshnessConstraints: This constraint indicates time requirements on revocation information. The constraints may indicate the maximum accepted difference between the issuance date of the revocation status information of a certificate and the time of validation (see [i.4]) or require the SVA to only accept revocation information issued a certain time after the signature has been created.	Ne

• (m)2.3. RevocationInfoOnExpiredCerts: This constraint mandates the signer's certificate used in validating the signature to be issued by a certification authority that keeps revocation notices for revoked certificates even after they have expired for a period exceeding a given lower bound.	Ne
(m)3. LoAOnTSPPractices: This constraint indicates the required LoA on the practices implemented by the TSP(s) having issued the certificates to be validated during the certificate path validation process [i.13], i.e. the certificates present in the certificate path of the signer's certificate, and optionally those present in all or some of the other certificate chains validated during the signature validation process.	Ne

3.2 Omezení v kontextu legislativy EU

Tato kapitola popisuje realizaci omezení z přílohy C – Constraints in the context of EU legislation [TS119172].

Constraint(s)	Constraint value at signature validation (SVA or DA)
a) **EUQualifiedCertificateRequired**: This constraint indicates that the signer's certificate used in validating the signature is required to be a qualified certificate as defined in the applicable EU legislation; expressed as a boolean.	Ano
b) **EUQualifiedCertificateSigRequired**: This constraint indicates that the signer's certificate used in validating the signature is required to be a qualified certificate for electronic signature as defined in [i.1]; expressed as a boolean.	Ano, jinak musí platit c).
c) **EUQualifiedCertificateSealRequired**: This constraint indicates that the signer's certificate used in validating the signature is required to be a qualified certificate for electronic seal as defined in [i.1]; expressed as a boolean.	Ano, jinak musí platit b).
d) **EUSSCDRequired**: This constraint indicates that the private key corresponding to the public key in the signer's certificate used in validating the signature is required to reside in an secure signature creation device as defined in [i.1]; expressed as a boolean.	Ne, ale indikace je k dispozici pro další rozhodnutí DA.
e) **EUAdESigRequired**: This constraint indicates that the signature is required to be an advanced electronic signature as defined in the applicable EU legislation; expressed as a boolean.	Ano, jinak musí platit f).

f) **EUAdESealRequired**: This constraint indicates that the signature is required to be an advanced electronic seal as defined in [i.1]; expressed as a boolean.	Ano, jinak musí platit e).
g) **EUQSigCDRequired**: This constraint indicates that the private key corresponding to the public key in the signer's certificate used in validating the signature is required to reside in a qualified signature creation device as defined in [i.1]; expressed as a boolean.	Ne, ale indikace je k dispozici pro další rozhodnutí DA.
h) **EUQSealCDRequired**: This constraint indicates that the private key corresponding to the public key in the signer's certificate used in validating the signature is required to reside in a qualified seal creation device as defined in [i.1]; expressed as a boolean.	Ne, ale indikace je k dispozici pro další rozhodnutí DA.

4 PŘÍLOHY

4.1 Mapování ASN.1 atributů podpisové politiky na XML elementy

ASN.1 atribut	XML element
`(id-contentType)`	*(DataObjectFormat)+*
`(id-aa-contentHint)` `.(contentDescription)`	*(DataObjectFormat)+* *.(Description)*
`(id-messageDigest)`	*DigestValue* jako souhrnná hodnota z elementů *Reference*. Viz *https://www.w3.org/TR/xmldsig-core/* .
`(id-signingTime)`	*(SigningTime)*
`(id-aa-ets-signingCertificateV2)` nebo `(id-aa-signingCertificate)`	*(SigningCertificate)*
`(id-aa-ets-sigPolicyId)`	*(SignaturePolicyIdentifier)*
`(id-aa-ets-contentTimestamp)*`	*(AllDataObjectsTimeStamp)** nebo *(IndividualDataObjectsTimeStamp)**
`(id-aa-ets-signerLocation)?`	*(SignatureProductionPlace)?*
`(id-aa-ets-certificateRefs)`	*(CompleteCertificateRefs)*
`(id-aa-ets-revocationRefs)`	*(CompleteRevocationRefs)*
`(id-aa-signatureTimeStampToken)+`	*(SignatureTimeStamp)+*
`((id-aa-ets-escTimeStamp)*` `(id-aa-ets-certCRLTimestamp)*)+`	*((SigAndRefsTimeStamp)* (RefsOnlyTimeStamp)*)+*
`(id-aa-ets-archiveTimestamp)+`	*(ArchiveTimeStamp)+*
`(id-aa-ets-certValues)`	*(CertificatesValues)*
`(id-aa-ets-revocationValues)`	*(RevocationValues)*
`(id-aa-ets-signerAttr)`	*(SignerRole)*