Verzia 1.3

Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu

3.3.2017

Odbor metodiky | Sekcia kybernetickej bezpečnosti
Budatínska č. 30 | 851 06 Bratislava | Slovenská republika
tel.: +421 2 6869 1111 | fax: +421 2 6869 1700
e-mail: podatelna@nbu.gov.sk | http://www.nbu.gov.sk/

Obsah

1 Úvod

Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu (ďalej len "SD" alebo "schéma") sa uplatňuje podľa kapitoly II prílohy I vykonávacieho rozhodnutia Komisie (EÚ) 2015/1505 z 8. septembra 2015, ktorým sa ustanovujú technické špecifikácie a formáty týkajúce sa dôveryhodných zoznamov podľa čl. 22 ods. 5 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu.

SD slúži pre zabezpečenie spoločných základných požiadaviek v oblasti dohľadu s cieľom zabezpečiť porovnateľnú úroveň bezpečnosti kvalifikovaných dôveryhodných služieb v celej Únii. SD zabezpečuje tento cieľ mapovaním právnych požiadaviek do technických postupov, čím sa splní cieľ, uľahčiť konzistentné uplatňovanie týchto požiadaviek v celej Únii a umožní členským štátom prijať porovnateľné postupy na základe vzájomnej výmeny informácií o svojich činnostiach dohľadu a najlepších postupoch v tejto oblasti.

Upozornenie: Text schémy bude priebežne dopĺňaný. Z dôvodu jednoznačného odlíšenia legislatívnych požiadaviek od technických požiadaviek, sa pred zloženou zátvorkou "{}" uvádza legislatívna požiadavka, ktorej povinné technické plnenie je uvedené v zloženej zátvorke.

2 Predmet dokumentu

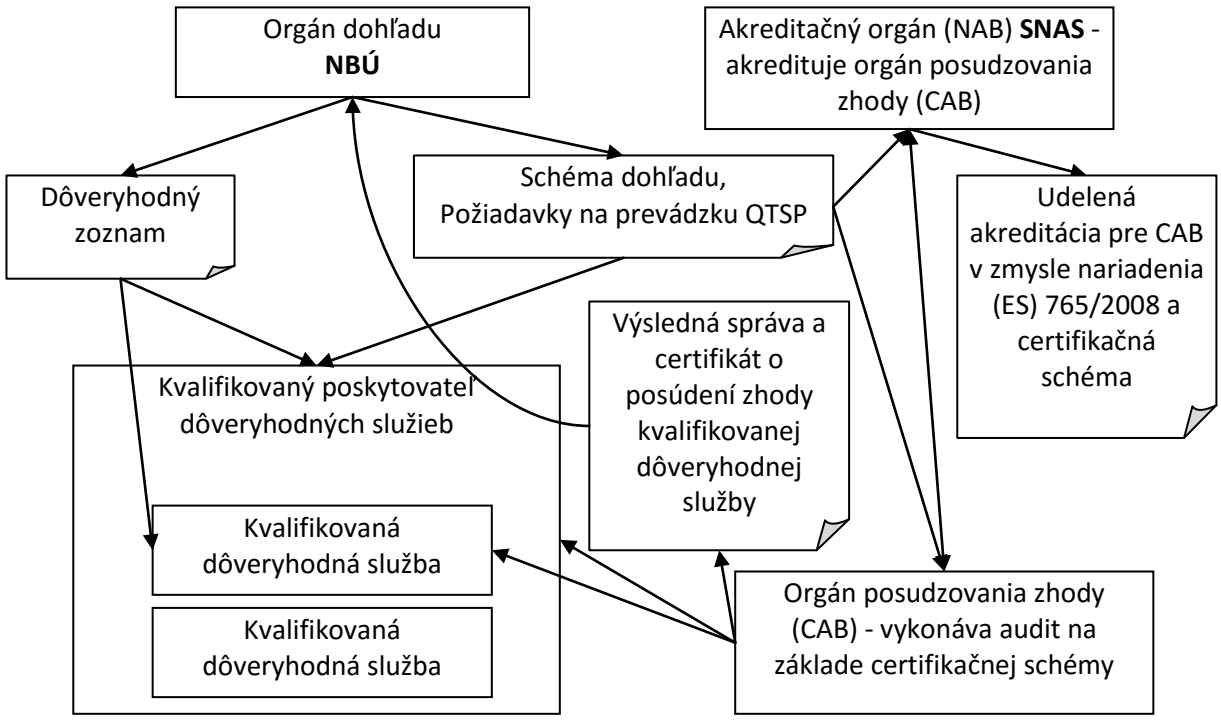
SD definuje pravidlá uplatňované orgánom dohľadu pri dohľade kvalifikovaných dôveryhodných služieb a je základom pre certifikačnú schému orgánu posudzovania zhody.

Podľa čl. 3 ods. 18 nariadenia (EÚ) č. 910/2014 [1], orgán posudzovania zhody je orgán vymedzený v čl. 2 bode 13 nariadenia (ES) č. 765/2008 [2], pričom tento orgán je v súlade s uvedeným nariadením akreditovaný ako orgán príslušný na posudzovanie zhody kvalifikovaných poskytovateľov dôveryhodných služieb a kvalifikovaných dôveryhodných služieb, ktoré poskytujú.

Certifikačná schéma orgánu posudzovania zhody je vytvorená NBÚ v spolupráci s orgánmi posudzovania zhody a akreditačným orgánom podľa požiadaviek uvedených v SD, ISO/IEC 17065 [3], zákone 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) [4], nariadení (EÚ) č. 910/2014 a v akreditačnej schéme Slovenskej národnej akreditačnej služby (ďalej len "SNAS").

Akreditačnú schému MSA-CP/05 pre Slovensko definuje SNAS primerane podľa ETSI EN 319 403 v2.2.2 (Requirements for conformity assessment bodies assessing Trust Service Providers) [5] a podľa požiadaviek legislatívy pre dôveryhodné služby, z ktorých špecifické legislatívne požiadavky pre jednotlivé kvalifikované dôveryhodné služby mapuje do technických postupov SD.

SNAS akredituje orgán posudzovania zhody podľa čl. 3 ods. 18 nariadenia (EÚ) č. 910/2014. SNAS pri akreditácii postupuje podľa akreditačnej schémy a udelenú akreditáciu, aj s prílohou obsahujúcou odkaz na certifikačnú schému, zverejní na webovom sídle SNAS.



Obrázok 1 — Schéma dohľadu

Podľa nariadenia (EÚ) č. 910/2014 kvalifikovaný štatút môže byť udelený 9 dôveryhodným službám:

1. Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis (pozri kapitolu 5.2)
2. Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov pre elektronickú pečať (pozri kapitolu 5.2)
3. Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov pre autentifikáciu webových sídiel (pozri kapitolu 5.2)
4. Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických podpisov (pozri kapitolu 5.3)
5. Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických pečatí (pozri kapitolu 5.3)
6. Kvalifikovaná dôveryhodná služba uchovávania kvalifikovaných elektronických podpisov (pozri kapitolu 5.4)
7. Kvalifikovaná dôveryhodná služba uchovávania kvalifikovaných elektronických pečatí (pozri kapitolu 5.4)
8. Kvalifikovaná dôveryhodná služba vyhotovovania kvalifikovaných elektronických časových pečiatok (pozri kapitolu 5.5)
9. Kvalifikovaná dôveryhodná elektronická doručovacia služba pre registrované zásielky (pozri kapitolu 5.6)

3 Odkazy

Odkazy na dokumenty, ktoré definujú použité typy a postupy.

[1] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.

[2] Nariadenie Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93 (Text s významom pre EHP).

[3] ISO/IEC 17065 Conformity assessment -- Requirements for bodies certifying products, processes and services

[4] Zákon 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)

[5] ETSI EN 319 403 v2.2.2 Requirements for conformity assessment bodies assessing Trust Service Providers

[6] Výnos Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy

[7] ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[8] ETSI EN 319 411-(1, 2, 3) Policy and security requirements for TSP issuing certificates

[9] NBÚ Dokumentácia TL X.509 XML schémy pre dôveryhodný zoznam (Pozri http://ep.nbusr.sk/kca/tsl/tlX509XMLSchemaDocumentation.pdf)

[10] RFC 6960 X.509 PKI Online Certificate Status Protocol 6-2013

[11] ITU-T RECOMMENDATION X.509 | ISO/IEC 9594-8

[12] RFC 5280 X.509 PKI Certificate and Certificate Revocation List Profile 5-2008

[13] Schéma dohľadu - orgánu dohľadu NBÚ (pozri http://ep.nbusr.sk/kca/tsl/SchemaDohladu.pdf)

[14] ETSI TR 102 272 ASN.1 format for signature policies

[15] ETSI TS 119 612 Trusted Lists

[16] RFC 5652 Cryptographic Message Syntax 9-2009

[17] RFC 3161 Time-Stamp Protocol (TSP) 8-2001

[18] Vykonávacie rozhodnutie 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.

[19] Vykonávacie rozhodnutie Komisie (EÚ) 2015/1505 z 8. septembra 2015, ktorým sa ustanovujú technické špecifikácie a formáty týkajúce sa dôveryhodných zoznamov podľa článku 22 ods. 5 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu.

[20] ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

4 Skratky

ASN.1	Abstract Syntax Notation 1
CA	Certifikačná autorita (Certification Authority)
CAB	Conformity Assessment Body (orgán posudzovania zhody)
CAdES	CMS Advanced Electronic Signature
DRId	Document Relative Identifier (relatívny identifikátor dokumentu)

Poznámka 1: Štruktúra DRId je rovnaká ako je definovaná pre SRId a obsahuje identifikátor hash algoritmu s parametrami a hash hodnotu z elektronického dokumentu.

CMS	Cryptographic Message Syntax
CP	Certificate Policy (certifikačná politika)
CP KCA NBÚ	Certifikačná politika koreňovej certifikačnej autority NBÚ http://ep.nbusr.sk/kca/cp_kca.html
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules (for ASN.1)
eIDAS	Nariadenie Európskeho parlamentu a Rady o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu
ENISA	European Union Agency for Network and Information Security https://www.enisa.europa.eu/topics/trust-services
ESS	Enhanced Security Services (enhances CMS)
GMT	Greenwich Mean Time
HTTP	Hyper Text Transfer Protocol
ISO	International Organization for Standardization
MIME	Multipurpose Internet Mail Extensions
NBÚ	Národný bezpečnostný úrad
OCSP	Online Certificate Status Protocol
OID	Object Identifier (objektový identifikátor, v bodkovom zápise napr. 1.2.3)
PAdES	PDF Advanced Electronic Signature
PKCS	Public Key Cryptographic Standards, Standards published by RSA, Labs.
PKIX	Internet X.509 Public Key Infrastructure
QC	Qualified Certificate
QCP SK	Qualified Certificate Policy of Slovakia
QSCD	Qualified Electronic Signature/Seal Creation Devices (zariadenia na vyhotovenie kvalifikovaného elektronického podpisu/pečate)
QTS	Qualified Trust Service (kvalifikovaná dôveryhodná služba)

QTSP	Qualified Trust Service Provider (kvalifikovaný poskytovateľ dôveryhodných služieb)
SD	Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu
SNAS	Slovenská národná akreditačná služba
SRId	Signature Relative Identifier (relatívny identifikátor podpisu)

Poznámka 2: SRId je DER kódovaný ASN.1 type *MessageImprint*, definovaný v IETF RFC 3161, obsahujúci hash hodnotu z digitálneho podpisu (DER kódovaného výsledku asymetrickej funkcie). Ak SRId sa použije na implementáciu časovej pečiatky podpisu (STS) nad OCSP, SRId sa vloží do *nonce* OCSP položky (IETF RFC 6960) ako údaje spojené s hodnotou času nachádzajúcou sa v položke *producedAt* OCSP odpovede.

STS	Signature Time-Stamp
TSA	Time-Stamping Authorities
TSP	Time Stamp Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
XAdES	XML Advanced Electronic Signature
XML	Extensible Markup Language
QES	Qualified Electronic Signature or Qualified Electronic Seal (kvalifikovaný elektronický podpis alebo kvalifikovaná elektronická pečať)

5 Mapovanie požiadaviek

5.1 Spoločné požiadavky na poskytovateľov kvalifikovaných dôveryhodných služieb

5.1.1 SD čl. 27 ods. 5 a čl. 37 ods. 5 nariadenia (EÚ) č. 910/2014

Ak členský štát na využívanie služby online, ktorú ponúka subjekt verejného sektora, alebo ktorá sa ponúka v jeho mene, vyžaduje elektronický podpis (pečať) aj nižšej úrovne bezpečnosti ako kvalifikovaný elektronický podpis, nariadením (EÚ) č. 910/2014 sa zavádza povinnosť uznávať alternatívne formáty, ktorých metódy sú vymedzené vo vykonávacích aktoch uvedených v čl. 27 ods. 5 a čl. 37 ods. 5 nariadenia (EÚ) č. 910/2014.

{ Aby sa predišlo stavu, kedy sa nepredvídateľný počet alternatívnych formátov musí uznávať, vyžaduje sa elektronický podpis (pečať), ktorý nie je nižšej úrovne bezpečnosti ako kvalifikovaný elektronický podpis (pečať), ak subjekt verejného sektora pre službu ktorú ponúka, alebo ktorá sa ponúka v jeho mene, neuvedie inak (ak subjekt verejného sektora je kvalifikovaný poskytovateľ dôveryhodných služieb, túto informáciu môže uviesť v podmienkach využívania tejto služby podľa čl. 24 ods. 2 písm. d) nariadenia (EÚ) č. 910/2014).

Subjekty, na ktoré sa vzťahuje zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, postupujú pri vytváraní a overovaní podpisu/pečate aj podľa § 57a až § 57e výnosu Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy [6]. }

5.1.2 SD čl. 19 a 24 nariadenia (EÚ) č. 910/2014

Dôveryhodné služby s kvalifikovaným štatútom sa poskytujú v súlade s článkami 19 a 24 nariadenia (EÚ) č. 910/2014.

{ Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť (ďalej len "ENISA") pripravila odporúčania najmä pre čl. 19 a čl. 24 ods. 2 nariadenia (EÚ) č. 910/2014, ktoré sú zverejnené na webovom sídle ENISA https://www.enisa.europa.eu/topics/trust-services/guidelines. Spoločné požiadavky na prevádzku poskytovateľov kvalifikovaných dôveryhodných služieb (ďalej len "QTSP") definované orgánom dohľadu sú uvedené v dokumente "Požiadavky na prevádzku kvalifikovaných poskytovateľov dôveryhodných služieb definované orgánom dohľadu" (ďalej len "Požiadavky na QTSP", pozri http://ep.nbusr.sk/kca/tsl/PoziadavkyPrevadzkyTSP.pdf). Dokument "Požiadavky na QTSP" je súčasťou tejto schémy dohľadu a vzhľadom na svoj rozsah a definovanie spoločných postupov pre všetky dôveryhodné služby je zverejnený v samostatnom dokumente. Dokument "Požiadavky na QTSP" pokrýva najmä mapovanie právnych požiadaviek čl. 19 a čl. 24 ods. 2 nariadenia (EÚ) č. 910/2014 do technických postupov, týkajúcich sa najmä objektov, personálu, technického a programového vybavenia kvalifikovaných dôveryhodných služieb kvalifikovaných poskytovateľov dôveryhodných služieb a primerane aj orgánov posudzovania zhody. Súčasťou dokumentu "Požiadavky na QTSP" je aj definovanie minimálnych položiek formulárov, ktoré musia byť uvedené pri postupoch vyžadovaných legislatívou, ako je napríklad zoznam položiek formulára zasielaného úradu podľa čl. 21 ods. 1 nariadenia (EÚ) č. 910/2014 a § 3 ods. 1 zákona č. 272/2016 Z. z.
Dôveryhodné služby primerane spĺňajú požiadavky uvedené v ETSI EN 319 401 (Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers) [7]. }

5.2 Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis, elektronickú pečať a autentifikáciu webových sídiel

{ URI Identifikácia v dôveryhodnom zozname *ServiceTypeIdentifier*:
"http://uri.etsi.org/TrstSvc/Svctype/CA/QC"

URI Identifikácia v dôveryhodnom zozname v elementoch *ServiceInformationExtensions – Extension – AdditionalServiceInformation,* ak služba vyhotovuje certifikát pre:

- elektronický podpis: "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures"
- elektronickú pečať: "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals"
- autentifikáciu webových sídiel: "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication"

}

5.2.1 SD čl. 17 ods. 5, čl. 24, 28, 38 a 45 nariadenia (EÚ) č. 910/2014

Služba sa poskytuje najmä v súlade s článkami 24 a 28 nariadenia (EÚ) č. 910/2014 a požiadavkami národnej legislatívy v súlade s čl. 17 ods. 5 nariadenia (EÚ) č. 910/2014.

{ Postup plnenia požiadaviek národnej legislatívy je uvedený najmä v kapitole 10 v certifikačnej politike koreňovej certifikačnej autority NBÚ (CP KCA NBÚ) OID (1.3.158.36061701.0.0.0.1.2.2), ktorá profiluje ETSI EN 319 411-2 V2.1.1 (2016-02) [8] certifikačné politiky pre vydávanie kvalifikovaných certifikátov. Plnenie CP KCA NBÚ pri vydávaní a overovaní kvalifikovaných certifikátov sa uvedie pre každú kvalifikovanú dôveryhodnú službu v dokumente "Pravidlá na výkon certifikačných činností" (Certification Practice Statement - CPS).
Informácie v dôveryhodnom zozname, podľa čl. 22 nariadenia (EÚ) č. 910/2014, úrad aktualizuje na základe posúdenia zaslanej správy o posúdení zhody podľa čl. 20 a čl. 21 nariadenia (EÚ) č. 910/2014, ktorá vychádza najmä z postupov uvedených v dokumente CPS. Úrad postupuje podľa predchádzajúcej vety pri každej požiadavke na zmenu údajov v dôveryhodnom zozname, napríklad pri požiadavke o autorizáciu alebo zmenu autorizácie vydávania OCSP odpovedí (čiastková kvalifikovaná dôveryhodná služba overovania (verification) kvalifikovaných certifikátov kvalifikovanej dôveryhodnej služby vyhotovovania kvalifikovaných certifikátov), ktorá sa uvádza v dôveryhodnom zozname v elemente *AuthorizedService*, ktorý je súčasťou elementu *URLContentTypeAndAuthorizedServiceList* definovaného v doplnkovej XSD schéme podľa dokumentácie http://ep.nbusr.sk/kca/tsl/tlX509XMLSchemaDocumentation.pdf [9].
}

5.2.2 SD čl. 28 ods. 3 a čl. 38 ods. 3 nariadenia (EÚ) č. 910/2014

Podľa čl. 28 ods. 3 a čl. 38 ods. 3 nariadenia (EÚ) č. 910/2014 kvalifikované certifikáty pre elektronické podpisy (pečate) môžu obsahovať nepovinné dodatočné osobitné atribúty. Týmito atribútmi sa neovplyvní interoperabilita a uznávanie kvalifikovaných elektronických podpisov (pečatí).
Podľa odôvodnenia 54 nariadenia (EÚ) č. 910/2014 cezhraničná interoperabilita a uznávanie kvalifikovaných certifikátov je predpokladom pre cezhraničné uznávanie kvalifikovaných elektronických podpisov. Kvalifikované certifikáty by preto nemali podliehať žiadnym povinným požiadavkám prekračujúcim požiadavky stanovené v tomto nariadení. Na vnútroštátnej úrovni by sa však malo povoliť začlenenie konkrétnych atribútov, akými sú napríklad jedinečné identifikátory, do kvalifikovaných certifikátov, a to za predpokladu, že tieto konkrétne atribúty nebudú prekážkou pre cezhraničnú interoperabilitu ani uznávanie kvalifikovaných certifikátov a elektronických podpisov.

{
Nepovinné dodatočné osobitné atribúty sú najmä údaje pre jednoznačnú identifikáciu, umožňujúce vopred pripraviť najmä informačné systémy na automatické spracovanie aspoň minimálnej množiny typov identifikátorov, ktoré sa uvádzajú v položke *Subject* certifikátu v jednej alebo viacerých položkách *serialNumber* identifikovaných objektovým identifikátorom (ďalej len OID) (2.5.4.5). Jedna položka *serialNumber* obsahuje iba jednu hodnotu zloženú z nasledovných znakov:

3 znaky

1. „PAS“ pre identifikáciu na základe čísla pasu
2. „IDC“ pre identifikáciu na základe čísla identifikačnej karty

3. „PNO“ pre identifikáciu na základe osobného čísla (aktuálne rodného čísla u občanov SR alebo cudzincov, ktorí majú pridelené rodné číslo podľa zákona č. 301/1995 Z. z. o rodnom čísle)
4. „NTR“ pre identifikáciu na základe identifikačného čísla organizácie.

2 znaky obsahujú kód krajiny podľa ISO 3166 (pre Slovensko „SK“)
1 znak „-“ (ASCII 0x2D)
Nepovinné spresňujúce 4 znaky, ktorých typ určujú prvé tri úvodné znaky a kód krajiny, napr.:
3 znaky
1. „JUS“ spresnenie pre „IDC“ pre identifikáciu na základe čísla identifikačnej karty sudcov a iných kariet v správe a formáte podľa postupu na http://www.justice.gov.sk/, napríklad "IDCSK-JUS-123123",
2. „NSA“ spresnenie pre „IDC“ pre identifikáciu na základe čísla identifikačnej karty príslušníkov NBÚ a iných kariet v správe a formáte podľa postupu na http://www.nbu.gov.sk/,
3. „POL“ spresnenie pre „IDC“ pre identifikáciu na základe čísla identifikačnej karty polície a iných kariet v správe a formáte podľa postupu na http://www.minv.sk/,
4. „MIL“ spresnenie pre „IDC“ pre identifikáciu na základe čísla identifikačnej karty ozbrojených síl Slovenskej republiky a iných kariet v správe a formáte podľa postupu na http://www.mod.gov.sk/.

1 znak „-“ (ASCII 0x2D)
Znaky údajov, ktorých typ určujú prvé tri úvodné znaky a kód krajiny (a voliteľné 4 znaky).

Identifikácia na základe „NTR“ môže byť uvedená aj v *organizationIdentifier* OID (2.5.4.97) v súlade s postupom definovaným pre položku *serialNumber*.
Ak by položka *serialNumber* obsahovala iné typy údajov než sú definované vyššie, nesmú sa použiť, ak by boli prvé tri znaky zhodné so znakmi definovanými vo vyššie uvedených bodoch 1 až 4.
Ak je kvalifikovaný certifikát vydaný pre osobu mladšiu ako 18 rokov a položka *serialNumber* OID (2.5.4.5) neobsahuje rodné číslo, musí sa uviesť dátum narodenia v rozšírení certifikátu *subjectDirectoryAttributes* OID (2.5.29.9) v položke *DateOfBirth* OID (1.3.6.1.5.5.7.9.1).

Nepovinné dodatočné osobitné atribúty sú aj informácie v položke *Subject* certifikátu, v položke *commonName* o maximálnej dĺžke 64 znakov, obsahujúce napríklad text s informáciou na uľahčenie neautomatizovanej manipulácii s certifikátom, ako napríklad skrátené meno subjektu alebo aj reťazec "QES xy" pre odlíšenie certifikátov pre podpis (alebo pečať) vydaných tomu istému subjektu s dodatočným poradovým číslom xy, ak sa napríklad na QSCD zariadení (čipová karta) nachádza viacero certifikátov.
}

5.2.3 SD prílohy I, III a IV nariadenia (EÚ) č. 910/2014

Tabuľka T1 - SD prílohy I, III a IV nariadenia (EÚ) č. 910/2014

Id. riadku	Kvalifikované certifikáty obsahujú: { realizácia požiadavky nariadenia }

T1.I,III,IV (a)	Označenie, prinajmenšom vo forme vhodnej na automatizované spracovanie, že certifikát sa vydáva ako kvalifikovaný.
	{
	1. rozšírenie *QCStatements* OID (1.3.6.1.5.5.7.1.3) obsahuje položku *QcCompliance* OID (0.4.0.1862.1.1) a
	2. certifikáty vydané na základe kvalifikovaného štatútu, ktorý kvalifikovanej dôveryhodnej službe udelil úrad, musia obsahovať rozšírenie certifikátu *certificatePolicies* OID (2.5.29.32) (kapitoly 8.1.1 a 8.2.2.6 Rec. ITU-T X.509), ktoré musí minimálne obsahovať OID certifikačnej politiky NBÚ OID (1.3.158.36061701.0.0.0.1.2.2).
	}
	Označenie, prinajmenšom vo forme vhodnej na automatizované spracovanie, že

	certifikát sa vydáva pre elektronický podpis.
	{
	Položka *Subject* certifikátu obsahuje aspoň jednu položku identifikovanú cez OID položky: *pseudonym* OID (2.5.4.65), *surname* OID (2.5.4.4), *givenName* OID (2.5.4.42).
	}
	Označenie, prinajmenšom vo forme vhodnej na automatizované spracovanie, že certifikát sa vydáva pre elektronickú pečať.
	{
	Položka *Subject* certifikátu obsahuje minimálne položku *organizationName* OID (2.5.4.10) a nesmie obsahovať ani jednu položku identifikovanú cez OID položky: *pseudonym* OID (2.5.4.65), *surname* OID (2.5.4.4), *givenName* OID (2.5.4.42).
	}
	Označenie, prinajmenšom vo forme vhodnej na automatizované spracovanie, že certifikát sa vydáva pre autentifikáciu webových sídiel.
	{
	Rozšírenie certifikátu *extendedKeyUsage* OID (2.5.29.37) obsahuje minimálne položku *serverAuthentication* OID (1.3.6.1.5.5.7.3.1).
	}

T1. I,III,IV (b)	Súbor údajov jednoznačne reprezentujúcich kvalifikovaného poskytovateľa dôveryhodných služieb, ktorý vydáva kvalifikované certifikáty, zahŕňajúci aspoň členský štát, v ktorom je tento poskytovateľ usadený, a — v prípade právnickej osoby: názov a prípadné registračné číslo, ako sa uvádza v úradných záznamoch, — v prípade fyzickej osoby: meno osoby. { Položka certifikátu *Issuer* obsahuje súbor údajov jednoznačne reprezentujúcich kvalifikovaného poskytovateľa dôveryhodných služieb, ktorý vydáva kvalifikované certifikáty, zahŕňajúci aspoň členský štát, v ktorom je tento poskytovateľ usadený v X.520 položke *countryName* OID (2.5.4.6), a — v prípade právnickej osoby: minimálne názov v položke *organizationName* OID (2.5.4.10) a prípadne registračné číslo v položke *serialNumber* OID (2.5.4.5) alebo v položke *organizationIdentifier* OID (2.5.4.97), ako sa uvádza v úradných záznamoch vo formáte uvedenom v "SD článku 28 ods. 3 a čl. 38 ods. 3 nariadenia (EÚ) č. 910/2014", — v prípade fyzickej osoby: minimálne meno osoby v položkách *surname* OID (2.5.4.4) a *givenName* OID (2.5.4.42). }
T1.I(c)	Aspoň meno podpisovateľa alebo pseudonym; ak sa použije pseudonym, musí to byť jasne uvedené. { Položka certifikátu *subject* minimálne obsahuje v X.520 položkách aspoň meno podpisovateľa v položkách *surname* OID (2.5.4.4) a *givenName* OID (2.5.4.42) alebo pseudonym v položke *pseudonym* OID (2.5.4.65); ak sa pseudonym použije v položke *commonName* OID (2.5.4.3), musí to byť jasne uvedené (v položke *commonName* sa minimálne uvedie text "PSEUDONYM"). }
T1.III(c)	Aspoň meno vyhotoviteľa pečate a prípadné registračné číslo, ako sa uvádza v úradných záznamoch. { Položka certifikátu *subject* minimálne obsahuje v X.520 položkách aspoň meno (názov) vyhotoviteľa pečate v položke *organizationName* OID (2.5.4.10) a prípadne registračné číslo v položke *serialNumber* OID (2.5.4.5) alebo v položke *organizationIdentifier* OID (2.5.4.97), ako sa uvádza v úradných záznamoch vo formáte uvedenom v "SD článku 28 ods. 3 a čl. 38 ods. 3 nariadenia (EÚ) č. 910/2014". }
T1.IV(c)	V prípade fyzických osôb: aspoň meno osoby, ktorej sa certifikát vydal, alebo jej pseudonym. Ak sa používa pseudonym, táto skutočnosť sa musí jednoznačne uviesť. V prípade právnických osôb: aspoň názov právnickej osoby, ktorej sa certifikát vydáva, a prípadne registračné číslo tak, ako sa uvádza v úradných záznamoch.

	{ Položka certifikátu *subject* minimálne obsahuje v X.520 položkách - v prípade fyzických osôb: aspoň meno osoby, ktorej sa certifikát vydal - v *surname* OID (2.5.4.4) a *givenName* OID (2.5.4.42) alebo pseudonym v položke *pseudonym* OID (2.5.4.65); ak sa pseudonym použije v *commonName* OID (2.5.4.3), musí to byť jasne uvedené (v položke *commonName* sa minimálne uvedie text "PSEUDONYM"); - v prípade právnických osôb: aspoň názov právnickej osoby, ktorej sa certifikát vydáva v položke *organizationName* OID (2.5.4.10) a prípadne registračné číslo v položke *serialNumber* OID (2.5.4.5) alebo v položke *organizationIdentifier* OID (2.5.4.97), ako sa uvádza v úradných záznamoch vo formáte v "SD článku 28 ods. 3 a čl. 38 ods. 3 nariadenia (EÚ) č. 910/2014". }
T1.I, III(d)	Údaje na validáciu elektronického podpisu / elektronickej pečate, ktoré zodpovedajú údajom na vyhotovenie elektronického podpisu / elektronickej pečate. { Podľa kapitoly 7.2 Rec. ITU-T X.509. *SubjectPublicKeyInfo ::= SEQUENCE {* *algorithm AlgorithmIdentifier,* *subjectPublicKey BIT STRING }* Algoritmus musí byť v zozname algoritmov a veľkostí uvedených v platných podpisových politikách zverejnených na webovom sídle NBÚ pre obdobie, v ktorom bol párový súkromný kľúč použitý. Poznámka: Vzhľadom na definíciu podľa nariadenia (EÚ) č. 910/2014 kvalifikovaný certifikát pre autentifikáciu webových sídiel nemusí obsahovať údaje na validáciu. Formát spĺňa aj definíciu Rec. ITU-T X.509 pre atribútový certifikát. }
T1.IV (d)	Prvky adresy, prinajmenšom vrátane mesta a štátu, fyzickej alebo právnickej osoby, ktorej sa certifikát vydáva, a prípadne tak ako sa uvádza v úradných záznamoch.
T1.IV (e)	Názvy domén prevádzkovaných fyzickou alebo právnickou osobou, ktorej sa certifikát vydáva.
T1.I,III (e) T1.IV (f)	Údaje o začiatku a konci obdobia platnosti certifikátu. { Uvedené sú v položke *Validity* - podľa kapitoly 7.2 Rec. ITU-T X.509. *Validity ::= SEQUENCE {* *notBefore Time,* *notAfter Time }* Údaje na vyhotovenie elektronického podpisu (pečate) musia byť použité v intervale uvedenom v položke *Validity.* }
T1.I,III (f) T1.IV (g)	Identifikačný kód certifikátu, ktorý musí byť jedinečný pre kvalifikovaného poskytovateľa dôveryhodných služieb. {Kladné číslo maximálnej veľkosti 20 byte podľa kapitoly 7.2 Rec. ITU-T X.509. *CertificateSerialNumber ::= INTEGER* }
T1.I,III(g) T1.IV (h)	Zdokonalený elektronický podpis alebo zdokonalenú elektronickú pečať vydávajúceho kvalifikovaného poskytovateľa dôveryhodných služieb. { Digitálny podpis, ktorý sa validuje podľa kapitoly 6.2 Rec. ITU-T X.509. *SIGNATURE{ToBeSigned} ::= SEQUENCE {* *algorithmIdentifier AlgorithmIdentifier{{SupportedAlgorithms}},* *encrypted ENCRYPTED-HASH{ToBeSigned},* *... }* Algoritmus kľúčového páru a hash funkcie musí byť v zozname algoritmov a veľkostí uvedených v platných podpisových politikách zverejnených podľa § 11 ods. 1 písm. m) zákona č. 272/2016 Z. z. na webovom sídle NBÚ pre obdobie, v ktorom bol súkromný kľúč použitý. }
T1.I,III (h) T1.IV (i)	Lokalitu, na ktorej je certifikát pre zdokonalený elektronický podpis alebo zdokonalenú elektronickú pečať podľa písmena g) dostupný bezplatne. { Rozšírenie *id-pe-authorityInfoAccess* OID (1.3.6.1.5.5.7.1.1) IETF RFC 5280 sekcia 4.2.2.1 obsahujúce v položke *id-ad-caIssuers* OID (1.3.6.1.5.5.7.48.2) 1) http adresu na CA certifikát vydavateľa ".cer" alebo krížové certifikáty vydavateľa

	".p7c" v CMS obálke IETF RFC 2797 sekcia 7.1. 2) Môže obsahovať jednoznačný identifikátor kvalifikovanej dôveryhodnej služby uvedenej v národnom dôveryhodnom zozname v elemente 'TLServiceIdentifier'. Formát identifikátora TL služby 'TLIxx-y' sa skladá z hodnoty xx, ktorá predstavuje kód krajiny TL vydavateľa (pozri 5.1.5 ETSI TS 119 612) a hodnoty y, obsahujúcej sekvenčné číslo služby v danom TL. Hodnotu identifikátora digitálnej služby v 'TLServiceIdentifier' elemente prideľuje TLSO v TL (pozri http://ep.nbusr.sk/kca/tsl/tlX509XMLSchemaDocumentation.pdf a 5.5.3 ETSI TS 119 612). Hodnota 'TLServiceIdentifier' položky tejto služby môže byť zahrnutá do odkazov na túto službu v tvare 'TLIxx-y' v rozšírení kvalifikovaného certifikátu *AuthorityInformationAccess* v položke *accessMethod*, ktorá obsahuje *id-ad-caIssuers*. Identifikátor dôveryhodného zoznamu služby vydavateľa je zahrnutý v položke *accessLocation* typu *GeneralName* ako *directoryName*, komponent typu *X520SerialNumber*. Príklad: *X520SerialNumber* = "TLISK-4". Pozri http://ep.nbusr.sk/kca/tsl/tsl.xml Pozri: https://tools.ietf.org/html/rfc5280#section-4.2.2.1 https://tools.ietf.org/html/rfc2797 }
T1.I,III (i) T1.IV (j)	Lokalitu služieb, ktoré možno využiť na zistenie štatútu platnosti kvalifikovaného certifikátu. { Certificate Revocation List (CRL definované v Rec. ITU-T X.509) je voliteľné a Online Certificate Status Protocol (OCSP definované v IETF RFC 6960) je povinné po skončení prechodného obdobia podľa § 18 ods. 5 zákona č. 272/2016 Z. z. CRL musí byť úplné. OCSP a CRL musia obsahovať aj informáciu o expirovanom certifikáte, čo nie je nutné, ak na základe autorizácie, uvedenej v dôveryhodnom zozname, informáciu o expirovanom kvalifikovanom certifikáte poskytuje kvalifikovaný poskytovateľ dôveryhodných služieb, ktorého autorizoval na vydávanie napr. OCSP odpovede: 1. vydavateľ kvalifikovaného certifikátu, alebo 2. je autorizovaný zo zákona, napr. NBÚ podľa § 11 ods. 1 písm. g) zákona č. 272/2016 Z. z. Identifikácia, že CRL obsahuje aj expirované certifikáty: *expiredCertsOnCRL* OID (2.5.29.60) CRL extension (pozri https://www.itu.int/rec/T-REC-X.509). OCSP odpoveď musí obsahovať podľa § 18 ods. 5 zákona č. 272/2016 Z. z. aj *CertHash* OID (1.3.36.8.3.13) OCSP single extension (pozri http://www.common-pki.org/uploads/media/Common-PKI_v2.0.pdf). Identifikácia, že OCSP odpoveď obsahuje stav aj o expirovanom certifikáte, je na základe *ArchiveCutoff* OID (1.3.6.1.5.5.7.48.1.6) OCSP extension (pozri IETF RFC 6960). OCSP podľa § 7 zákona č. 272/2016 Z. z. musí poskytovať správnu odpoveď aj o čase platnosti certifikátu v položke *thisUpdate*, ak certifikát nie je zrušený, čo deklaruje OCSP vložením rozšírenia - *CertHash* OCSP single extension do OCSP odpovede. Rozšírenie *id-pe-authorityInfoAccess* OID (1.3.6.1.5.5.7.1.1) IETF RFC 5280 sekcia 4.2.2.1 obsahuje v položke *id-ad-ocsp* OID (1.3.6.1.5.5.7.48.1) http adresu na službu Online Certificate Status Protocol (OCSP). Pozri: https://tools.ietf.org/html/rfc5280#section-4.2.2.1 https://tools.ietf.org/html/rfc6960 Rozšírenie CRLDistributionPoints OID (2.5.29.31) je definované v kapitole 8.6.2.1 Rec. ITU-T X.509. Podľa § 4 zákona č. 272/2016 Z. z., ak podpisovateľ (vydavateľ) overovaného certifikátu 1) nie je podpisovateľom (vydavateľom) CRL a 2) nie je podpisovateľom (vydavateľom) certifikátu na validovanie podpisu OCSP

	odpovedi, podpisovateľ (vydavateľ) overovaného certifikátu autorizuje podpisovateľa CRL alebo podpisovateľa OCSP odpovede. Vydavateľ overovaného kvalifikovaného certifikátu požiada uviesť túto autorizáciu do dôveryhodného zoznamu, v rozšírení dôveryhodnej služby. Autorizácia v dôveryhodnom zozname obsahuje identifikátor autorizovanej dôveryhodnej služby (identifikátor pridelený v dôveryhodnom zozname), URL adresu autorizovanej dôveryhodnej služby a dobu autorizácie od, a ak je známa doba ukončenia autorizácie, aj dobu do. Kapitola 7.10 Rec. ITU-T X.509 "The revocation and a notification of the revocation may be done directly by the same authority that issued the certificate, or indirectly by another authority duly authorized by the authority that issued the certificate." (Pozri http://ep.nbusr.sk/kca/tsl/tlX509XMLSchemaDocumentation.pdf). }
T1.I,III(j)	Ak sa údaje na vyhotovenie elektronického podpisu súvisiace s údajmi na validáciu elektronického podpisu nachádzajú v zariadení na vyhotovenie kvalifikovaného elektronického podpisu, primerané uvedenie tejto skutočnosti, prinajmenšom vo forme vhodnej na automatizované spracovanie. { Rozšírenie *QCStatements* OID (1.3.6.1.5.5.7.1.3) musí obsahovať minimálne položku *QcSSCD*/*QcQSCD* OID (0.4.0.1862.1.4). }

5.2.4 SD čl. 28 ods. 2 a čl. 38 ods. 2 nariadenia (EÚ) č. 910/2014

Na základe čl. 28 ods. 2 nariadenia (EÚ) č. 910/2014, sa požiadavky podľa profilov certifikátov zverejnených na webovom sídle úradu uvádzajú ako nepovinné, dodatočné, osobitné atribúty certifikátu.

5.2.5 SD čl. 28 ods. 3, čl. 38 ods. 3 a odôvodnenia 58 nariadenia (EÚ) č. 910/2014

V súlade s odôvodnením 58 nariadenia (EÚ) č. 910/2014, keď sa pri transakcii vyžaduje kvalifikovaná elektronická pečať právnickej osoby, rovnako akceptovateľný by mal byť aj kvalifikovaný elektronický podpis splnomocneného zástupcu právnickej osoby.

{ Spôsob vhodný pre automatizované spracovanie umožňujúci identifikáciu splnomocneného zástupcu právnickej osoby a typu splnomocnenia definuje národná legislatíva v § 8 zákona č. 272/2016 Z. z. pod označením mandátny certifikát a pre typ splnomocnenia zavádza pojem oprávnenie. Mandátnym certifikátom preukazuje mandatár (fyzická osoba) oprávnenie

a) konať za, alebo v mene mandanta (fyzická osoba alebo právnická osoba),
b) vykonávať činnosť podľa osobitného predpisu, alebo
c) vykonávať funkciu podľa osobitného predpisu.

Identifikačné údaje v zmysle bodov § 8 ods. 1 písm. b) zákona č. 272/2016 Z. z. sa uvedú iba v tých prípadoch, pre ktoré je možné na základe príslušného predpisu obsah týchto bodov identifikovať, teda môžu nastať 4 kombinácie:

1. Uvedú sa podľa bodu 1 a aj podľa bodu 2.
2. Uvedú sa podľa bodu 1, ale neuvedú sa podľa bodu 2.
3. Neuvedú sa podľa bodu 1, ale uvedú sa podľa bodu 2.
4. Neuvedú sa podľa bodu 1 a ani podľa bodu 2.

V zmysle § 8 ods. 1 písm. b) bod 1 zákona č. 272/2016 Z. z. sa identifikačné údaje mandanta podľa § 2 zákona č. 272/2016 Z. z. uvádzajú tak, že každá položka obsahujúca identifikačné údaje mandanta v položke subjektu certifikátu musí začínať reťazcom "MANDANT ", aby nedošlo k zámene obsahu položky mandanta a mandatára, pričom minimálne sa uvedú položky *serialNumber* OID (2.5.4.5) alebo *organizationIdentifier* OID(2.5.4.97), podľa kapitoly "SD čl. 28 ods. 3 a čl. 38 ods. 3 nariadenia (EÚ) č. 910/2014" a položky podľa riadkov T1.I(c) a T1.III(c) tabuľky T1. Reťazec "MANDANT " sa uvádza len v položkách podľa § 8 ods. 1 písm. b) bod 1 zákona č. 272/2016 Z. z. Napríklad položka *serialNumber* obsahuje "MANDANT PNOSK-535919999".

V zmysle § 8 ods. 1 písm. b) bod 2 zákona č. 272/2016 Z. z. sa identifikačné údaje orgánu verejnej moci alebo osoby, u ktorej mandatár vykonáva činnosť podľa osobitného predpisu alebo vykonáva funkciu podľa osobitného predpisu, podľa § 2 zákona č. 272/2016 Z. z., uvádzajú minimálne v položkách *organizationName* OID (2.5.4.10) a *serialNumber* OID (2.5.4.5) alebo *organizationIdentifier* OID (2.5.4.97) subjektu certifikátu, kde *serialNumber* alebo *organizationIdentifier* obsahuje údaje podľa typu "NTR" v súlade s kapitolou "SD čl. 28 ods. 3 a čl. 38 ods. 3 nariadenia (EÚ) č. 910/2014" a *organizationName* obsahuje názov registrovaný k údajom podľa typu "NTR" z položky *serialNumber* alebo *organizationIdentifier*.

Na webovom sídle úradu je podľa § 9 zákona č. 272/2016 Z. z. zverejnený zoznam registrovaných typov oprávnení (splnomocnení), ktoré sa musia uvádzať v rozšírení certifikátu *certificatePolicies* OID (2.5.29.32) (kapitoly 8.1.1 a 8.2.2.6 Rec. ITU-T X.509) ako OID oprávnenia. V OID hodnote sa registrované oprávnenie xyz uvádza ako posledná hodnota OID (1.3.158.36061701.1.1.xyz).

Jeden certifikát môže v rozšírení certifikátu *certificatePolicies* OID (2.5.29.32) obsahovať jedno alebo viacero oprávnení (splnomocnení) ako samostatné hodnoty OID (1.3.158.36061701.1.1.xyz).

Názov oprávnenia, zverejnený v zozname registrovaných typov oprávnení, sa odporúča uviesť v rozšírení certifikátu *certificatePolicies* OID (2.5.29.32) k hodnote oprávnenia OID (1.3.158.36061701.1.1.xyz) v jednej alebo viacerých položkách typu *UserNotice* v položke *explicitText* ako *utf8String* o maximálnej veľkosti 200 znakov minimálne v slovenskom jazyku.

Nepovinne je možné uvádzať číslo oprávnenia, pre informáciu na uľahčenie neautomatizovanej manipulácii s mandátnym certifikátom, v položke *commonName* subjektu certifikátu, kde sa odporúča za textový reťazec "OPRÁVNENIE", alebo skrátene "MANDÁT", medzerou oddeliť číslo oprávnenia xyz a následne medzerou oddeliť textový názov oprávnenia zo zoznamu registrovaných typov oprávnení (splnomocnení), pričom položka *commonName* má maximálnu dĺžku 64 znakov a na začiatku môže obsahovať aj iný text, ako je napríklad uvedené v kapitole "SD čl. 28 ods. 3 a čl. 38 ods. 3 nariadenia (EÚ) č. 910/2014". Ak je jeden certifikát vydaný pre viacero oprávnení, postup sa zopakuje v jednej položke *commonName,* ak to maximálna dĺžka umožňuje. Ak text v *commonName* prekračuje povolenú dĺžku, text názvu oprávnenia sa neuvádza a uvedie sa len reťazec "OPRÁVNENIE", alebo skrátene "MANDÁT", medzera a číslo oprávnenia xyz.
}

5.2.6 SD čl. 24 ods. 1 nariadenia (EÚ) č. 910/2014

Podľa čl. 24 ods. 1 nariadenia (EÚ) č. 910/2014, kvalifikovaný poskytovateľ dôveryhodných služieb pri vydávaní kvalifikovaného certifikátu pre dôveryhodnú službu vhodnými prostriedkami a v súlade s vnútroštátnym právom overuje totožnosť a prípadne akékoľvek osobitné atribúty fyzickej alebo právnickej osoby, ktorej vydáva kvalifikovaný certifikát.

{
Ak sa kvalifikovaný certifikát vydáva na kľúčový pár, ktorého súkromný kľúč (údaje na vyhotovenie elektronického podpisu alebo pečate) je uložený na zariadení pre vyhotovovanie kvalifikovaného elektronického podpisu alebo kvalifikovanej elektronickej pečate (ďalej len "QSCD"), vydavateľ kvalifikovaného certifikátu musí, okrem požiadaviek podľa čl. 24 ods. 1 nariadenia (EÚ) č. 910/2014, overiť aj:

- či sú splnené požiadavky podľa čl. 26 písm. c) nariadenia (EÚ) č. 910/2014 vyžadujúce overenie, či môže podpisovateľ s vysokou mierou dôveryhodnosti používať údaje na vyhotovenie elektronického podpisu **pod svojou výlučnou kontrolou**, alebo či sú splnené požiadavky podľa čl. 36 písm. c) nariadenia (EÚ) č. 910/2014 vyžadujúce overenie, či môže pôvodca pečate **s vysokou mierou dôveryhodnosti pod jeho kontrolou** používať údaje na vyhotovenie elektronickej pečate a

- či požiadavky na QSCD podľa prílohy II nariadenia (EÚ) č. 910/2014 sú splnené na základe informácií zverejnených podľa čl. 31 ods. 2 nariadenia (EÚ) č. 910/2014, podľa ktorého Komisia na základe získaných informácií vytvorí, zverejňuje a vedie zoznam certifikovaných zariadení na vyhotovenie kvalifikovaných elektronických podpisov.

}

Informácie uvedené v prvom pododseku overuje kvalifikovaný poskytovateľ dôveryhodných služieb buď priamo, alebo prostredníctvom spoľahnutia sa na tretiu stranu v súlade s vnútroštátnym právom:
a) na základe fyzickej prítomnosti fyzickej osoby alebo splnomocneného zástupcu právnickej osoby, alebo
b) na diaľku prostredníctvom prostriedkov elektronickej identifikácie, pre ktoré sa pred vydaním kvalifikovaného certifikátu zabezpečila fyzická prítomnosť fyzickej osoby alebo splnomocneného zástupcu právnickej osoby, a ktoré spĺňajú požiadavky stanovené v článku 8 nariadenia (EÚ) č. 910/2014, pokiaľ ide o úroveň zabezpečenia „pokročilá“ alebo „vysoká“, alebo
{ Pri overení totožnosti na diaľku prostredníctvom prostriedkov elektronickej identifikácie sa v zásade vyžaduje mechanizmus Extended Access Control (ďalej len "EAC") podľa technickej smernice Federal Office for Information Security (ďalej len "BSI") BSI TR-03110. V takomto prípade sa musí použiť EAC mechanizmus vzájomnej autentifikácie na zabezpečenie nielen identity ale aj integrity zasielaných údajov a ich šifrovania pri procese vydávania kvalifikovaného certifikátu na karte na diaľku (čo zahŕňa najmä generovanie kľúčového páru v čipe, vydanie kvalifikovaného certifikátu na vygenerovaný verejný kľúč a uloženie kvalifikovaného certifikátu na čip s prepojením na vygenerovaný kľúčový pár), čím sa zaručí bezpečnosť komunikácie, identifikácia a autentifikácia komunikujúcich strán (kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov a osoby, pre ktorú je kvalifikovaný certifikát vydaný, ktorá sa identifikovala prostredníctvom údajov pre EAC, z ktorých niektoré sú uložené v čipe a niektoré sú zapamätané len touto osobou)
}
c) prostredníctvom certifikátu pre kvalifikovaný elektronický podpis alebo kvalifikovanú elektronickú pečať vydaného v súlade s písmenom a) alebo b), alebo
{ Ak sa kvalifikovaný certifikát vydáva pre kvalifikovaný elektronický podpis alebo pečať, tak sa jedná len o následné vydanie kvalifikovaného certifikátu na rovnaký kľúčový pár, ako je kľúčový pár uvedený v aktuálnom kvalifikovanom certifikáte a rovnaké údaje, ako sú uvedené v aktuálnom kvalifikovanom certifikáte, ktorý sa použije na validovanie kvalifikovaného elektronického podpisu alebo pečate, pričom sa v novom kvalifikovanom certifikáte zmení len obdobie platnosti a sériové číslo certifikátu uvedené v tabuľke č. 1 v riadkoch T1.I,III(e)T1.IV(f) a T1.I,III(f)T1.IV(g).
}

d) prostredníctvom použitia iných metód identifikácie uznávaných na vnútroštátnej úrovni, ktorými sa poskytuje rovnocenné zabezpečenie, pokiaľ ide o spoľahlivosť, ako pri fyzickej prítomnosti. Rovnocenné zabezpečenie potvrdzuje orgán posudzovania zhody.

{ Orgán posudzovania zhody, ktorý je akreditovaný SNAS, zverejní zoznam iných metód identifikácie uznávaných na vnútroštátnej úrovni, v ktorom potvrdzuje rovnocenné zabezpečenie.
}

5.2.7 SD čl. 24 ods. 2 písm. d) nariadenia (EÚ) č. 910/2014

Podľa čl. 24 ods. 2 písm. d) nariadenia (EÚ) č. 910/2014 kvalifikovaný poskytovateľ dôveryhodných služieb pred uzavretím zmluvného vzťahu jednoznačne a vyčerpávajúco informuje každú osobu, ktorá chce využívať kvalifikovanú dôveryhodnú službu, o presných podmienkach využívania tejto služby vrátane obmedzení jej využívania.
{ Informácia o povinnostiach osoby, pre ktorú sa vydáva kvalifikovaný certifikát, ktorá má pod výhradnou kontrolou súkromný kľúč, ktorého verejný kľúč je obsiahnutý vo vydávanom kvalifikovanom certifikáte pre túto osobu, musí obsahovať minimálne povinnosť používať súkromný kľúč len na účely vyhotovenia kvalifikovaného elektronického podpisu (pečate), aby nedošlo k jeho zneužitiu nesprávnym použitím a bezodkladne požiadať vydavateľa certifikátu o zrušenie certifikátu

1. pri strate výhradnej kontroly nad súkromným kľúčom a

2. pri zmene údajov uvedených v certifikáte.

}

5.2.8 SD čl. 24 ods. 2 písm. k) nariadenia (EÚ) č. 910/2014

Podľa čl. 24 ods. 2 písm. k) nariadenia (EÚ) č. 910/2014 sa požaduje, aby kvalifikovaný poskytovateľ dôveryhodných služieb zriadil a aktualizoval databázu certifikátov.

{ Databáza certifikátov obsahuje minimálne vydaný kvalifikovaný certifikát a

- ak kvalifikovaný certifikát bol zrušený, minimálne jednu OCSP odpoveď alebo CRL v ktorom bol kvalifikovaný certifikát zrušený a identifikáciu CRL alebo OCSP odpovede, v ktorom bol certifikát prvýkrát zrušený (pre overenie dodržania maximálneho 24 hodinového intervalu, požadovaného v článku 24 ods. 3 nariadenia (EÚ) č. 910/2014, na základe položky *thisUpdate*),
- ak počas svojej platnosti kvalifikovaný certifikát nebol zrušený a expiroval, minimálne jedno CRL alebo OCSP odpoveď aktualizovanú (*thisUpdate*) po expirovaní kvalifikovaného certifikátu.

}

5.2.9 SD čl. 24 ods. 3 nariadenia (EÚ) č. 910/2014

Podľa čl. 24 ods. 3 nariadenia (EÚ) č. 910/2014, ak sa kvalifikovaný certifikát zruší, kvalifikovaný poskytovateľ dôveryhodných služieb zaznamená takéto zrušenie vo svojej databáze certifikátov { čas zrušenia je hodnota v prvom CRL, ktoré zrušenie obsahuje, v položkách *thisUpdate* a *revocationDate*; čas zrušenia v OCSP odpovedi je hodnota v položke *revocationTime* } a štatút zrušenia certifikátu uverejní čo najskôr, a v každom prípade do 24 hodín od doručenia žiadosti { databáza certifikátov obsahuje v požadovanom intervale hodnotu v položke *thisUpdate* z CRL alebo OCSP odpovede, v ktorom došlo k prvému zrušeniu a čas zrušenia v CRL *revocationDate* alebo v OCSP odpovedi v *revocationTime* }. Zrušenie je účinné ihneď po jeho uverejnení { najmenšia hodnota *thisUpdate* v OCSP odpovediach alebo vydaných CRL, ktoré obsahujú zrušenie }.

{ Pozri kapitolu 7.10 Rec. ITU-T X.509 https://www.itu.int/rec/T-REC-X.509 a sekciu 2.4 IETF RFC 6960 https://tools.ietf.org/html/rfc6960#section-2.4 .
}

5.2.10 Kvalifikovaná dôveryhodná služba overovania (verification) kvalifikovaných certifikátov ako služba v rámci kvalifikovanej dôveryhodnej služby vyhotovovania kvalifikovaných certifikátov pre elektronický podpis alebo pre elektronickú pečať alebo pre autentifikáciu webových sídiel

{ *ServiceTypeIdentifier* URI Identifikácia v dôveryhodnom zozname:
Ako spoločná služba vyhotovovania kvalifikovaných certifikátov pre elektronický podpis alebo pre elektronickú pečať alebo pre autentifikáciu webových sídiel "http://uri.etsi.org/TrstSvc/Svctype/CA/QC" alebo ako samostatná služba v zodpovednosti služby vyhotovovania kvalifikovaných certifikátov pre elektronický podpis alebo pre elektronickú pečať alebo pre autentifikáciu webových sídiel
"http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC" a
"http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC". }

5.2.11 SD čl. 24 ods. 4 nariadenia (EÚ) č. 910/2014

Podľa čl. 24 ods. 4 nariadenia (EÚ) č. 910/2014, pokiaľ ide o ods. 3, kvalifikovaní poskytovatelia dôveryhodných služieb, ktorí vydávajú kvalifikované certifikáty, každej spoliehajúcej sa strane poskytnú informácie **o štatúte platnosti** { čas platnosti je (ak nie je uvedený čas zrušenia certifikátu): čas v položke *thisUpdate* v OCSP odpovedi povinne obsahujúcej aj *CertHash* OCSP single rozšírenie, pozri http://www.common-pki.org/uploads/media/Common-PKI_v2.0.pdf a čas v položke *thisUpdate* v CRL } **alebo zrušenia** { čas zrušenia je čas v OCSP položke *revocationTime* a čas v CRL položke *revocationDate* } 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.

{ Služba vyhotovovania kvalifikovaných certifikátov autorizuje kvalifikovanú dôveryhodnú službu overovania kvalifikovaných certifikátov (na vydávanie OCSP odpovedí a CRL), uvedením tejto služby v dôveryhodnom zozname v službách kvalifikovaného poskytovateľa dôveryhodných služieb, ktorého služba "vyhotovovania kvalifikovaných certifikátov" vyhotovila kvalifikovaný certifikát alebo autorizuje iného kvalifikovaného poskytovateľa dôveryhodných služieb pomocou rozšírenia dôveryhodného zoznamu v elemente *URLContentTypeAndAuthorizedServiceList* definovaného v XSD schéme http://ep.nbusr.sk/kca/tsl/x509types# v dokumentácii http://ep.nbusr.sk/kca/tsl/tlX509XMLSchemaDocumentation.pdf, pričom zodpovednosť za správnosť údajov je na službe "vyhotovovania kvalifikovaných certifikátov", ktorá kvalifikovaný certifikát vyhotovila.

Táto schéma nepovoľuje, aby právnu zodpovednosť za kvalifikovanú dôveryhodnú službu "vyhotovovania kvalifikovaných certifikátov" prevzala iná služba overovania, teda za službu overovania je zodpovedná vždy "kvalifikovaná dôveryhodná služba vyhotovovania kvalifikovaných certifikátov", ktorá certifikát vyhotovila, pričom informácie o tomto certifikáte na základe autorizácie uvedenej priamo alebo nepriamo v dôveryhodnom zozname, môže poskytovať pod jej zodpovednosťou aj iná ňou autorizovaná služba overenia.

Element *URLContentTypeAndAuthorizedServiceList* definovaný v XSD schéme http://ep.nbusr.sk/kca/tsl/x509types# slúži aj na zverejnenie novej adresy a typu kvalifikovanej dôveryhodnej služby overovania (verification) kvalifikovaných certifikátov a to najmä, ak v čase vyhotovovania kvalifikovaného certifikátu takáto služba ešte nebolo dostupná, a teda odkaz na službu nie je uvedený v URL odkaze vo vydanom kvalifikovanom certifikáte, čím sa prostredníctvom dôveryhodného zoznamu umožní jej používanie automatizovaným spôsobom.

Kvalifikovaná dôveryhodná služba " overovania (verification) kvalifikovaných certifikátov" založená na OCSP protokole definovanom v IETF RFC 6960, ktorého OCSP odpoveď spĺňa požiadavky uvedené v nižšie definovanom profile OCSP, sa posudzuje primerane podľa požiadaviek na službu elektronickej časovej pečiatky podľa ETSI EN 319 421 v1.1.1 "Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps", okrem požiadavky uvedenej v prvej vete v kapitole 7.7.1EN 319 421 v1.1.1, kde profil definovaný v ETSI EN 319 422 je nahradený profilom pre OCSP uvedeným nižšie a písmeno d) kapitoly 7.7.1 ETSI EN 319 421 v1.1.1 sa aplikuje pre kľúčový pár pre podpisovanie OCSP odpovede.

5.2.12 SD - profil OCSP odpovede

a) Vzhľadom na povinnosť zriadenia a aktualizovania databázy certifikátov podľa čl. 24 ods. 2 písm. k) nariadenia (EÚ) č. 910/2014, je databáza certifikátov zdrojom údajov poskytovaných v OCSP odpovedi definovanej v IETF RFC 6960. Z dôvodu povinného použitia databázy certifikátov, voliteľná položka *nextUpdate* objektu *SingleResponse* sa do OCSP odpovede neuvádza.
b) OCSP odpoveď obsahuje odpoveď typu *id-pkix-ocsp-basic*.
c) Dátum a čas uvedený v položke *producedAt* objektu *ResponseData* OCSP odpovede definovanej v IETF RFC 6960 je s presnosťou minimálne na 1 sekundu, čím sa primerane musia splniť požiadavky ETSI EN 319 421 v1.1.1.
d) Objekt *SingleResponse* v položke *singleExtensions* OCSP odpovede musí obsahovať minimálne *CertHash* OID (1.3.36.8.3.13) OCSP single extension (pozri http://www.common-pki.org/uploads/media/Common-PKI_v2.0.pdf). Rozšírenie *CertHash* obsahuje hash hodnotu certifikátu, ktorého stav je v položke *certStatus* objektu *SingleResponse*, pričom použitie rozšírenia *CertHash* identifikuje spresnenie významu OCSP stavu *good,* uvedeného v položke *certStatus* OCSP odpovede. Stav *good* bez rozšírenia *CertHash* nemusí znamenať, že certifikát bol platný, napríklad pred expirovaním bol certifikát neplatný a záznam o zrušení po expirovaní bol vymazaný, alebo certifikát je neznámy. Ak je uvedené OCSP rozšírenie *CertHash,* stav *good* znamená, že certifikát je platný, alebo bol platný v intervale platnosti, keď certifikát expiroval. Ak je uvedené rozšírenie *CertHash* a stav certifikátu

je *good,* položka *thisUpdate* objektu *SingleResponse* OCSP odpovede obsahuje čas a dátum, do ktorého je certifikát evidovaný ako platný a zrušenie môže nastať len s neskoršou hodnotou času zrušenia.

e) Ak je certifikát zrušený, v položke *certStatus* v objekte *SingleResponse* je uvedený objekt *RevokedInfo* obsahujúci položku *revocationTime* s časom zrušenia certifikátu.

f) Algoritmus v objekte *BasicOCSPResponse* v položke *signature* musí byť v zozname algoritmov a veľkostí uvedených v platných podpisových politikách zverejnených na webovom sídle NBÚ pre obdobie, v ktorom bol súkromný kľúč použitý, zverejnených podľa § 11 ods. 1 písm. m) zákona č. 272/2016 Z. z.

g) OCSP odpoveď v objekte *BasicOCSPResponse* v položke *certs* musí obsahovať certifikát na validovanie podpisu OCSP odpovede, ktorý sa uvedie v dôveryhodnom zozname ako identifikátor služby "overovania (verification) kvalifikovaných certifikátov" s kvalifikovaným štatútom.

h) Objekt *SingleResponse* v položke *singleExtensions* OCSP odpovedi môže obsahovať *ServiceLocator*, ktorá v položke *locator* môže obsahovať hodnotu z 'TLServiceIdentifier' elementu pridelenú TLSO v TL (pozri http://ep.nbusr.sk/kca/tsl/tlX509XMLSchemaDocumentation.pdf a 5.5.3 ETSI TS 119 612). Hodnota 'TLServiceIdentifier' položky tejto služby môže byť zahrnutá do položky *locator*, ako odkaz na túto službu v tvare 'TLIxx-y' v rozšírení *AuthorityInformationAccess* v položke *accessMethod*, ktorá obsahuje *id-ad-caIssuers*. Identifikátor dôveryhodného zoznamu služby vydavateľa certifikátu je zahrnutý v položke *accessLocation* typu *GeneralName* ako *directoryName*, komponent typu *X520SerialNumber*. Príklad: *X520SerialNumber* = "TLISK-4". Pozri http://ep.nbusr.sk/kca/tsl/tsl.xml

Plnenie požiadavky podľa čl. 24 ods. 4 nariadenia (EÚ) č. 910/2014 "aj po uplynutí doby platnosti certifikátu" z požiadavky "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" umožní zjednodušiť dôveryhodná infraštruktúra úradu, budovaná ako národné rozšírenia dôveryhodných služieb podľa čl. 17 ods. 5 nariadenia (EÚ) č. 910/2014, pre certifikáty vydané v súlade s vnútroštátnym právom, ak vydavateľom certifikátu je dôveryhodná služba poskytovateľa dôveryhodných služieb, ktorej kvalifikovaný štatút udelil úrad. Služba vydavateľa kvalifikovaných certifikátov podľa § 6 ods. 2 písm. a) a b) zákona č. 272/2016 Z. z. zasiela úradu minimálne raz mesačne vydané kvalifikované certifikáty a ak dôjde k zrušeniu certifikátu, tak aj minimálne s jedným CRL alebo OCSP odpoveďou, v ktorej je uvedené zrušenie kvalifikovaného certifikátu, alebo ak certifikát expiroval, minimálne jedno CRL alebo OCSP odpoveď aktualizovanú (*thisUpdate*) po expirovaní kvalifikovaného certifikátu, čím sa potvrdí, že certifikát nebol počas celej doby platnosti zrušený. Úrad na základe týchto informácií poskytuje podľa štandardu úradu pre CRL a OCSP, na neobmedzenú dobu, informáciu o stave expirovaných kvalifikovaných certifikátov, čím uľahčí splnenie požiadavky podľa čl. 24 ods. 4 nariadenia (EÚ) č. 910/2014 vydavateľom kvalifikovaných certifikátov a chráni spoliehajúce sa strany pred prípadným nedostupným spôsobom dlhodobého overovania platnosti kvalifikovaného certifikátu.

}

5.2.13 SD čl. 28 ods. 5 a čl. 38 ods. 5 nariadenia (EÚ) č. 910/2014

Podľa článku 28 ods. 5 a čl. 38 ods. 5 nariadenia (EÚ) č. 910/2014, členské štáty môžu ustanoviť vnútroštátne predpisy o dočasnom pozastavení kvalifikovaného certifikátu pre elektronický podpis, a to za týchto podmienok:

a) ak sa kvalifikovaný certifikát pre elektronický podpis dočasne pozastaví, certifikát stráca platnosť na obdobie pozastavenia;

b) obdobie pozastavenia sa jasne uvedie v databáze certifikátov a štatút pozastavenia musí byť počas obdobia pozastavenia viditeľný zo služby, ktorou sa poskytujú informácie o štatúte certifikátu.

{

Podľa § 7 ods. 2 zákona č. 272/2016 Z. z. certifikát nesmie byť zrušený s vyplnenou položkou "Reason Code" (Pozri kapitolu 8.5.3.1 Rec. ITU-T X.509 https://www.itu.int/rec/T-REC-X.509 a sekciu 5.3.1 IETF RFC 5280 https://tools.ietf.org/html/rfc5280#section-5.3.1) obsahujúcou hodnotu *certificateHold* typu *CRLReason*, čo sa považuje za pozastavenie platnosti certifikátu podľa čl. 28 ods. 5 a čl. 38 ods. 5 nariadenia (EÚ) č. 910/2014.

}

5.3 Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí

{ URI Identifikácia v dôveryhodnom zozname *ServiceTypeIdentifier*:
"http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q"

Výsledkom kvalifikovanej dôveryhodnej služby validácie kvalifikovaných elektronických podpisov a pečatí je správa z validácie v textovom dokumente v UTF8 kódovaní, ktorá ako posledný riadok obsahuje iba súhrnný výsledok PLATNÝ(VALID) alebo NEPLATNÝ(INVALID) a ak čas podpísania alebo zapečatenia nie je možné dôveryhodne preukázať, uvedie sa čas, do ktorého je kvalifikovaný certifikát evidovaný ako platný (*thisUpdate* CRL alebo OCSP odpovede), alebo ak bol kvalifikovaný certifikát zrušený, uvedie sa čas zrušenia platnosti kvalifikovaného certifikátu a ak bol vydaný ďalší certifikát pre rovnaký kľúčový pár s rovnakým menom subjektu, overuje sa len ten podpisový certifikát, na ktorého referencia (odkaz s hash hodnotou certifikátu) je chránená podpisom alebo pečaťou.

Prvý riadok správy z procesu validácie obsahuje prehlásenie "Správa z validácie kvalifikovaného elektronického podpisu alebo pečate podľa článkov 32 a 40 nariadenia (EÚ) č. 910/2014 - SRId [Base64 kódovaný SRId].".

SRId je DER kódovaný ASN.1 type *MessageImprint*, definovaný v IETF RFC 3161, obsahujúci hash hodnotu z digitálneho podpisu (DER kódovaného výsledku asymetrickej funkcie), pozri poznámku pre SRId v kapitole 4.

Výsledná správa procesu validácie obsahuje len položky, ktorých zobrazenie sa požaduje, alebo položky pri ktorých neboli splnené nasledovné podmienky z procesu validácie spolu s označením podmienky vo formáte:
Prvý je znak "R", oddeľovač je znak "-", nasleduje číslo a prípadne písmeno článku 32 (zhodné s čl. 40) nariadenia (EÚ) č. 910/2014, prípadne nasleduje označenie tabuľky napr. T1 a označenie riadka v tabuľke, ak na ňu položka odkazuje v prípade, ak nesplnenie požiadavky vzniklo napríklad v podmienke na riadku tejto tabuľky.
Napríklad:
"R-1.d)-T1.I(b) subjekt kvalifikovaného certifikátu:
Peter - *givenName* OID (2.5.4.42)
Tesla - *surname* OID (2.5.4.4) "

Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických podpisov a pečatí môže ponúknuť na výber správu okrem TXT dokumentu aj vo viacerých formátoch, ako napríklad v PDF alebo v štruktúrovanom texte formátu JSON, poprípade v inom. Správa je uložená napr. v ZIP podpisovom kontajneri typu ASiC alebo PDF, ktorých formáty sú uvedené 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 čl. 27 ods. 5 a čl. 37 ods. 5 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (Text s významom pre EHP) (ďalej len „vykonávacie rozhodnutie Komisie (EÚ) 2015/1506“).
}

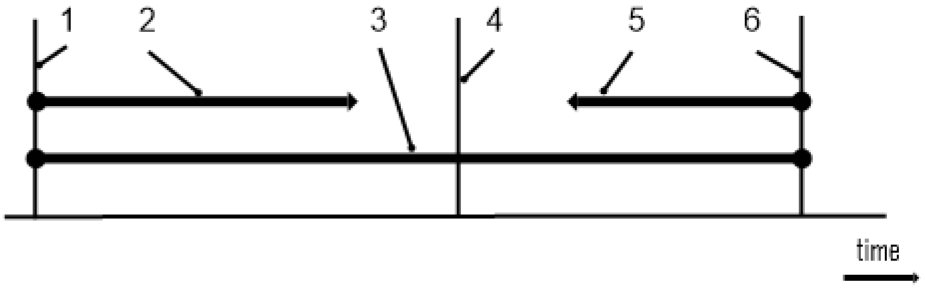
5.3.1 SD čl. 32 a 40 nariadenia (EÚ) č. 910/2014

Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických podpisov a pečatí podľa článkov 32 a 40 nariadenia (EÚ) č. 910/2014 spĺňa tieto požiadavky:

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

a) certifikát, ktorý potvrdzuje podpis alebo pečať, bol v čase podpísania alebo vyhotovenia pečate kvalifikovaným certifikátom pre elektronický podpis alebo elektronickú pečať v súlade s prílohou I alebo III;

{ R-1.a) Čas podpísania alebo vyhotovenia pečate je čas, pre ktorý je dostupný preukázateľný dôveryhodný dôkaz o existencii a čase podpísania alebo vyhotovenia pečate v minulosti, napríklad prostredníctvom kvalifikovanej elektronickej časovej pečiatky zahrňujúcej údaje digitálneho podpisu, v opačnom prípade je to čas, v ktorom sa overovanie vykonáva.
Certifikát a jeho položky sa overia podľa požiadaviek uvedených v tabuľke T1 v riadkoch označených "I" pre podpis a v riadkoch označených "III" pre pečať.
Čas podpísania alebo vyhotovenia pečate kvalifikovaným certifikátom pre elektronický podpis alebo elektronickú pečať je v nasledujúcom texte označený ako *control-time*. Postup jeho určenia je uvedený v obrázku 2 *control-time* in a Proof of Existence (PoE) of the closed interval.



Key

1 (PoE) – the signature was created after the time value stored in:
- the *thisUpdate* field of the CRL or in the *producedAt* field of the OCSP response, when CRL or OCSP response are covered by the *ats-hash-index-v3* signed attribute, where in the context of the present document, the *ats-hash-index-v3* attribute shall be a signed attribute of the CMS signature as an additional usage of the *ats-hash-index-v3* attribute defined in clause 5.5.2 of ETSI EN 319 122-1 V1.1.1 (2016-04),
- the content time-stamp (CTS) attribute defined in ETSI EN 319 122-1, or
- the objects (the time-stamp, in the *thisUpdate* field of the CRL or in the *producedAt* field of the OCSP response) of the previous signature covered with the signature.

2 Interval – the signature covers the objects listed in the Key 1 in the hash value.

3 The closed interval in which the signature was created.

4 The factual time of the signature creation of data (electronic document).

5 Interval – the objects listed in the Key 6 cover the value of the digital signature in the hash value.

6 (PoE) – the signature was created before the time value stored in:
- the signature time-stamp (STS) defined in IETF RFC 3161,
- the *producedAt* field of the OCSP response when the OCSP *nonce* contains SRId - the *MessageImprint* field, defined in IETF RFC 3161, covering the value of the digital signature as the signature time-stamp (STS) implemented over OCSP,
- the time-stamp of the subsequent signature covering the signature value of the digital signature,
- the PDF subsequent document time-stamp, or
- the external objects covering in the hash value the signature value of the digital signature like the Evidence Records defined in IETF RFC 4998 or IETF RFC 6283.

Figure 2 — *control-time* in a PoE of the closed interval

Správa z validácie obsahuje riadok "R-1.a) Interval času vytvorenia podpisu - control-time ([x],[y])", kde hodnota času "x" sa uvedie len vtedy, ak objekt PoE pre hodnotu času "x" je dostupný a je dôveryhodný a hodnota času "y" sa uvedie len vtedy, ak objekt PoE pre hodnotu času "y" je dostupný a je dôveryhodný.
}

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

{ R-1.b) V čase začiatku platnosti kvalifikovaného certifikátu (položka *notBefore* podľa tabuľky T1 riadku T1.I,III (e)), musí byť certifikát vydavateľa, ktorým sa overuje kvalifikovaný certifikát, uvedený priamo v dôveryhodnom zozname podľa čl. 22 nariadenia (EÚ) č. 910/2014 (ďalej len "TL") alebo nepriamo cez zostavenú certifikačnú cestu končiacu v TL a stav v TL musí byť "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted" (5.5.4 ETSI TS 119 612 V2.1.1) pre typ služby "http://uri.etsi.org/TrstSvc/Svctype/CA/QC".
Ak je vydavateľ uvedený priamo v TL, nesmie byť použité URI "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC", ktoré sa vkladá do rozšírenia TL *additionalServiceInformation* (5.5.9.4 ETSI TS 119 612 V2.1.1) v *ServiceInformationExtension* (5.5.9 ETSI TS 119 612 V2.1.1) a musia byť splnené pravidlá na zostavenie, validovanie a overenie certifikačnej cesty podľa "Certification path processing procedure" (Kapitola 10 Recommendation ITU-T X.509 | ISO/IEC 9594-8) zahrňujúce položky TL definované v doplnkovej XSD schéme http://ep.nbusr.sk/kca/tsl/x509types#.
Ak je použité URI "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC", potom sa musí postupovať podľa pravidiel na zostavenie, validovanie a overenie certifikačnej cesty podľa "Certification path processing procedure" (Kapitola 10 Recommendation ITU-T X.509 | ISO/IEC 9594-8), ktoré zahrňujú položky TL definované v doplnkovej XSD schéme http://ep.nbusr.sk/kca/tsl/x509types#, pričom certifikačná cesta musí končiť na certifikáte uvedenom v TL so stavom "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted" (5.5.4 ETSI TS 119 612 V2.1.1).
Ak je vydavateľ uvedený priamo v TL, platnosť kvalifikovaného certifikátu sa overí pomocou CRL alebo OCSP odpovede získanej z adresy uvedenej v kvalifikovanom certifikáte podľa tabuľky T1 riadku T1.I,III (i) alebo z TL položky vydavateľa certifikátu *URLContentTypeAndAuthorizedServiceList* definovanej v doplnkovej XSD schéme. Validovanie CRL alebo OCSP odpovede je buď certifikátom uvedeným v službe TL, ktorej stav je "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted" (5.5.4 ETSI TS 119 612 V2.1.1) v čase vydania a preukázateľnej existencie CRL alebo OCSP odpovede (CRL alebo OCSP odpoveď je vydaná pred expirovaním certifikátu služby a pred koncom platnosti uvedeným v TL položke *PrivateKeyUsagePeriod* služby vydávajúcej CRL alebo OCSP odpoveď).
Ak certifikát na validáciu CRL alebo OCSP odpovede nie je priamo v TL, postupuje sa podľa pravidiel "Certification path processing procedure" (Kapitola 10 Recommendation ITU-T X.509 | ISO/IEC 9594-8), ktoré zahrňujú položky TL definované v doplnkovej XSD schéme, pričom certifikačná cesta musí končiť na certifikáte uvedenom v službe TL so stavom "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted" (5.5.4 ETSI TS 119 612 V2.1.1).
Pri určení platnosti certifikátu sa postupuje podľa tabuliek v obrázkoch 3 a 4, kde čas podpísania alebo vyhotovenia pečate je označený ako *control-time*.

```
1  if ( certificate.notBefore < CRL.thisUpdate ) and
     ( ((CRL.expiredCertsOnCRL  <= certificate.notAfter ) and ( 0 < CRL.expiredCertsOnCRL )) or
      (( CRL.thisUpdate <= certificate.notAfter ) and ( 0 = CRL.expiredCertsOnCRL ))) then
2        if certificate is not revoked in CRL then
3              if control-time <= CRL.thisUpdate then
                     VALID
               else
4                    WAS VALID at [CRL.thisUpdate], the later status is not confirmed.
                     If you need a confirmation of the later status, try to get a newer updated CRL.
                     INDETERMINATE
         else
5              if control-time < CRL[certificate].revocationDate then
                     VALID
               else
6                    INVALID – revoked at [ CRL[certificate].revocationDate ]
   else
7        INDETERMINATE (INCOMPLETE AUTOMATIC VALIDATION: a request to CA for CRL
         that can contain the status of the certificate being verified.)
```

Key

1 CRL was updated in time of certificate validity + a period of time during which the record about the certificate revocation is listed in CRL even after the certificate expiration.

If "expired certificates on CRL" extension is not present in the CRL extension, then CRL.*expiredCertsOnCRL* value shall be 0; otherwise the CRL.*expiredCertsOnCRL* value is according to the extension "Expired certificates on CRL" defined in ITU-T X.509.

CRL.*thisUpdate* is the time when the certificate status was updated, what means the certificate status will not be changed to "*revoked*" with the time value before the *thisUpdate* time in any time later.

Certificate.*notBefore* is the time since when it is possible to use the certificate and its status can be included in CRL.

Certificate.*notAfter* is the time after which the certificate status in CRL is not changed anymore but the status can be included in CRL.

2 The certificate was not revoked; it is not in CRL.

3 The certificate status in CRL is updated after *control time*.

4 The certificate was valid at the time value of CRL.*thisUpdate* field.

CRL is not issued after *control time*. When the status at *control time* is necessary then the validation procedure must wait for a new updated CRL (CRL.*thisUpdate* >= *control time*).

5 The certificate was revoked after control time, thus it is valid.

6 The certificate was revoked before *control time* at CRL[certificate].*revocationDate*.

7 It is necessary to obtain CRL or OCSP response, which is updated in time when the certificate has not been expired yet + a period of time in which the certificate status is still known in OCSP or CRL.

CRL is updated before the certificate usage period, Certificate.*notBefore* time.

Figure 3 — Validation with CRL

```
1  if ( certificate.notBefore < OCSP[certificate].thisUpdate ) and
     ( (( OCSP.ArchiveCutoff <= certificate.notAfter ) and ( 0 < OCSP.ArchiveCutoff )) or
      (( OCSP[certificate].thisUpdate <= certificate.notAfter) and (0 = OCSP.ArchiveCutoff )) or
      (OCSP[certificate].CertHash = certificate.CertHash) ) then
2        if OCSP[certificate].CertStatus = good then
3              if control-time <= OCSP[certificate].thisUpdate then
                     VALID
               else
4                    WAS VALID at [OCSP[certificate].thisUpdate], the later status is not confirmed.
                     If you need a confirmation of the later status, try to get a newer updated
                     OCSP response.     INDETERMINATE
         else
5              if OCSP[certificate].CertStatus = revoked then
                     if control-time < OCSP[certificate].revocationTime then
                           VALID
6                    else
                           INVALID - revoked at [OCSP[certificate].revocationTime ]
               else
7                    INDETERMINATE (INCOMPLETE AUTOMATIC VALIDATION: OCSP does not know
                      the current status of the certificate validity because OCSP[certificate].CertStatus
                     = unknown Validation is possible by other OCSP or CRL.)
   else
8        INDETERMINATE (INCOMPLETE AUTOMATIC VALIDATION: a request to CA for OCSP response or
         CRL that can contain the status of the certificate being verified.)
```

Key

1 OCSP was updated in time of certificate validity + a period of time during which the record about the certificate revocation for OCSP is known even after the certificate expiration.

Certificate.*notBefore* is the time since when it is possible to use the certificate and the certificate status can be included in OCSP (CRL).

Certificate.*notAfter* is the time after which the certificate status in CRL (OCSP) cannot be changed but the certificate status can be included in CRL (OCSP).

OCSP.*ArchiveCutoff* – if OCSP extension *ArchiveCutoff* is not present in the OCSP response, then OCSP.*ArchiveCutoff* value shall be 0; otherwise the *ArchiveCutoff* value is according to "*ArchiveCutoff*" extension defined in IETF RFC 6960.

OCSP[certificate].*CertHash* is the hash value of the certificate whose status is returned by the OCSP response (Common PKI extensions *CertHash* (positive statement), Clause 3.1.2, Common PKI Specification V2.0 www.common-pki.org). If this extension is found in the OCSP response, then the certificate status is known for OCSP and the hash value ensures the integrity by currently secure hash algorithm.

Certificate.*CertHash* is the hash value of the certificate whose status is verified.

OCSP[certificate].*thisUpdate* is the time when the certificate status was updated, what means the certificate status will not be changed to "*revoked*" with the time value before the *thisUpdate* time in any time later. The value must be smaller or equal to OCSP.*producedAt*.

OCSP.producedAt is the time of the OCSP response issuance.

OCSP[certificate].*nextUpdate* is the auxiliary time about the availability of the latest occurrence of the information about the status. The OCSP response must not contain the item *nextUpdate* if the certificate, whose status is returned, is expired.

2 The certificate was not revoked.

OCSP[certificate].*CertStatus* is the status of the certificate being verified with the values: *good*, *revoked* and *unknown*.

3 A certificate status in OCSP is updated after *control time*.

4 The certificate was valid at the time value of OCSP[certificate].*thisUpdate* field.

OCSP response is not issued after *control time*. When the status at *control time* is necessary then the validation procedure must wait for a new updated OCSP response (OCSP[certificate].*thisUpdate* >= *control time*).

5 The certificate was revoked after *control time*, thus it is valid.

6 The certificate is revoked in OCSP response before *control time*.

OCSP[certificate].revocationTime is the time of the certificate revocation.

7 OCSP response is not able to determine a certificate status, it is necessary to try other OCSP responder or CRL.

8 It is necessary to obtain OCSP response or CRL, which is updated in time when the certificate has not been expired yet + a period of time in which the certificate status is still known in OCSP or CRL.

OCSP response was updated before the certificate usage period, Certificate.*notBefore* time.

Figure 4 — Validation with OCSP response

The validation report "R-1.b)" contains at least 2 sentences, where the content described in the square brackets "[ ]" is replaced with the particular value.
The sentences of the report are the following:
"
R-1.b) The qualified certificate issuer is the qualified trust service provider (QTSP) [*TLIxx-y*] *according to TL. The validity status of the qualified certificate at the time of signing provided by this QTSP is* [*valid* | *revoked at* [the revocation date and time] | *expired (the PoE before the qualified certificate expiration is not available)* [the expiration date and time]]
",
where the TL service identifier 'TLIxx-y' consists of "xx" value representing the country code of TL issuer (see 5.1.5 ETSI TS 119 612) and "y" value containing a sequential service number in the respective TL. The value 'TLIxx-y' of digital service identifier in 'TLServiceIdentifier' element is assigned by the TLSO in TL (see http://ep.nbusr.sk/kca/tsl/tlX509XMLSchemaDocumentation.pdf).

If the TL unique and precise service identifier 'TLIxx-y' in "TLServiceIdentifier" element of the digital service identifier "ServiceDigitalIdentity", "DigitalId" elements is not included in the TL, then the validation report contains in the sentence instead of [TLIxx-y] identification the identification of the issuer of the qualified certificate indicated in TL. This case is problematic because the identification of the issuer of the qualified certificate indicated in TL is based on many optional components and it is up to the validation application which component will be used to create the unique representation of the QTSP which is the issuer of the qualified certificate in TL.
Instead of [TLIxx-y] the following is included in the report:
"
1. Hash algorithm [OID of the hash algorithm in a dot notation and the algorithm name]*,*
2. Hash of the issuer certificate [the hash value of the qualified certificate issuer DER X.509 *Certificate* - the certificate included in TL]*,*
3. Hash of the certificate issuer name [the hash value of the subject name (*DistinguishedName*) of the certificate included in TL – as defined for *CertID. issuerNameHash* IETF RFC 6960]*,*
4. Hash of the certificate issuer Public Key [the hash value of *SubjectPublicKeyInfo* of the certificate included in TL – as defined for *CertID. issuerKeyHash* IETF RFC 6960]*,*
5. Certificate issuer serial number [base64 encoded *TBSCertificate*.*serialNumber* of the certificate included in TL http://www.itu.int/itu-t/recommendations/rec.aspx?rec=X.509]*,*
6. Key identifier of the certificate issuer [base64 encoded hash value composed of the SHA-1 hash of the value of the BIT STRING *subjectPublicKey* (excluding the tag, length, and number of unused bits) of the *SubjectPublicKeyInfo* of the certificate included in TL],
7. The certificate issuer name [LDAP name (IETF RFC 4514) of the ITU-T X.501 *DistinguishedName* of the certificate subject name included in TL http://www.itu.int/itu-t/recommendations/rec.aspx?rec=X.501],
8. Service Type Identifier [URI identification in a trusted list *ServiceTypeIdentifier* of the certificate issuer included in TL - QTSP],
9. [Any other TL values of TL elements of the qualified certificate issuer included in TL which must be included in the report to have a unique identification of the QTSP] …
"

Note: The validation report contains identification of at least one of many possible certificates (cross-certificates) included in TL "ServiceDigitalIdentity" element. When the hash value is used, then the OID of the hash algorithm is the same for the hash values in the report "R-1.b)" and any hash values in the report are base64 encoded.

}

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

{ R-1.c) Prekontroluje sa, či spoliehajúcej sa strane sú poskytnuté údaje v jednom z formátov zdokonaleného elektronického podpisu / pečate, ktorý definuje príloha vykonávacieho rozhodnutia Komisie (EÚ) 2015/1506 prostredníctvom zoznamu technických špecifikácií pre zdokonalené elektronické podpisy XML, CMS alebo PDF a pre podpisový kontajner vo formáte ASiC.
Správa obsahuje informácie len v prípade nesúladu s požiadavkami formátov uvedených v prílohe vykonávacieho rozhodnutia Komisie (EÚ) 2015/1506, v tvare: Dôvod nesúladu oddelený pomlčkou "-" v zátvorkách "()" označenie mena objektu/súboru "-" označenie štandardu "-" hierarchické meno komponent (podľa definícií v štandarde) oddelené s "." alebo poľom "[]" s indexom od 0, kde nesúlad nastal.
Príklad: R-1.c) Nedostupný certifikát podpisovateľa (signature.p7s)-IETF-RFC5652-*ContentInfo*.*content*.*SignedData*.*signerInfos*[0].*signerInfo*.*signedAttrs*[3].
IETF-RFC5035-*SigningCertificateV2*.*certs*[0].*ESSCertIDv2*.*certHash* =
9E6A332C1100BD704BDDB15B0306D70942826F86AE3AE5E5A20C5CFCFE532EEE
}

d) sa jedinečný súbor údajov reprezentujúcich podpisovateľa alebo pôvodcu pečate v certifikáte správne poskytol spoliehajúcej sa strane;

{ R-1.d) Zobrazia sa všetky položky z položky *Subject*, z rozšírenia typu alternatívne meno subjektu a rozšírenia *subjectDirectoryAttributes* kvalifikovaného certifikátu, pričom sa jednoznačne uvedie minimálne názov položiek (prípadne OID) a obsah položiek podľa tabuľky T1 riadku T1.I(c) , riadku T1.III(c) a nepovinných dodatočných osobitných atribútov podľa "SD článku 28 ods. 3 a čl. 38 ods. 3 nariadenia (EÚ) č. 910/2014".
}

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

{ R-1.e) Skontrolujú sa podmienky podľa tabuľky T1 riadku T1.I(c)
}

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

{ R-1.f) Na základe podmienky podľa tabuľky T1 riadok T1.I,III(j) sa v správe uvedie výsledok, či sa jedná o kvalifikovaný podpis alebo kvalifikovanú pečať na základe identifikátora QSCD.
}

g) nebola narušená integrita podpísaných alebo zapečatených údajov;

{ R-1.g) Správa obsahuje informácie v prípade neúspešného použitia výsledku hašovacej funkcie zahrňujúcej podpísané alebo zapečatené údaje alebo postupného použitia údajov z viacerých vnorených hašovacích funkcií na postupnosť podpísaných alebo zapečatených údajov, ktorej výsledná hodnota musí zodpovedať hodnote údajov podľa výsledku asymetrickej funkcie, ktorej jedným zo vstupov sú údaje na validáciu podpisu alebo pečate z kvalifikovaného certifikátu podľa tabuľky T1 riadku T1.I, III(d).
}

h) v čase podpísania boli dodržané požiadavky stanovené v článkoch 26 alebo 36 nariadenia (EÚ) č. 910/2014:

5.3.2 SD čl. 26 a 36 nariadenia (EÚ) č. 910/2014

Zdokonalený elektronický podpis alebo zdokonalená elektronická pečať musí spĺňať tieto požiadavky:
a) je jedinečne spojený s podpisovateľom alebo je jedinečne spojená s pôvodcom pečate;

{ R-1.h)-a)
CMS zdokonalený elektronický podpis alebo pečať – je CMS podpis, ktorý musí obsahovať podpísanú položku *SigningCertificateV2* obsahujúcu v prvej položke *certs* typu *ESSCertIDv2* definovanú v IETF RFC 5035 odkaz a hash hodnotu certifikátu podpisovateľa. CMS podpis musí obsahovať kvalifikovaný certifikát podpisovateľa v položke *SignedData.certificates,* pričom algoritmy použité v CMS podpise musia byť v zozname algoritmov a veľkostí uvedených v platných podpisových politikách zverejnených podľa § 11 ods. 1 písm. m) zákona č. 272/2016 Z. z. na webovom sídle NBÚ pre obdobie, v ktorom bol súkromný kľúč použitý.

PDF zdokonalený elektronický podpis alebo pečať – je CMS podpis IETF RFC 5652 spĺňajúci pravidlá pre CMS z predchádzajúceho odseku a je uložený v objekte Signature Dictionary, kde *SubFilter* musí obsahovať hodnotu *ETSI.CAdES.detached*.

XML zdokonalený elektronický podpis alebo pečať – je XML podpis definovaný v https://www.w3.org/TR/xmldsig-core/, ktorý musí obsahovať v *SignedInfo* elemente, v ktorom je *Reference* element obsahujúci odkaz buď na *KeyInfo* obsahujúci v *X509Data* elemente *X509Certificate* element s certifikátom podpisovateľa, alebo obsahujúci odkaz na *SignedProperties* element definovaný v XSD "http://uri.etsi.org/01903/v1.3.2#" obsahujúci vnorené elementy *SignedSignatureProperties, SigningCertificate* a *Cert* element obsahujúci odkaz a hash hodnotu certifikátu podpisovateľa. XML podpis musí obsahovať kvalifikovaný certifikát podpisovateľa v elemente *X509Certificate* v elemente *X509Data,* pričom algoritmy použité v XML podpise musia byť v zozname algoritmov a veľkostí uvedených v platných podpisových politikách zverejnených na webovom sídle NBÚ pre obdobie, v ktorom bol súkromný kľúč použitý.
}

b) umožňuje určenie totožnosti podpisovateľa alebo pôvodcu pečate;

{ R-1.h)-b) V certifikáte jednoznačne identifikovanom v bode R-1.h)-a) sa totožnosť zobrazí podľa bodu R-1.d)
}

c) je vyhotovený pomocou údajov na vyhotovenie elektronického podpisu, ktoré môže podpisovateľ s vysokou mierou dôveryhodnosti používať **pod svojou výlučnou kontrolou** alebo je vyhotovená pomocou údajov na vyhotovenie elektronickej pečate, ktoré môže pôvodca pečate s vysokou mierou dôveryhodnosti **pod jeho kontrolou** používať na vyhotovenie elektronickej pečate, a
{ R-1.h)-c) Informácia o type údajov na vyhotovenie elektronického podpisu je uvedená v kvalifikovanom certifikáte v tabuľke T1 riadku T1.I, III(d). Informácia o úrovni bezpečnosti uloženia a použitia údajov na vyhotovenie elektronického podpisu je uvedená v kvalifikovanom certifikáte v tabuľke T1 riadku T1.I, III(j).
}

d) je prepojený s údajmi, ktoré sa ním podpisujú alebo na ktoré sa pečať vzťahuje, takým spôsobom, že každú dodatočnú zmenu údajov možno zistiť.

{ R-1.h)-d) Integrita je zabezpečená použitým hash algoritmom a validovaná použitím údajov z kvalifikovaného certifikátu v tabuľke T1 riadku T1.I, III(d).

Ochrana pred zmenou údajov, nesprávnou interpretáciou údajov, ktoré sa podpisujú, alebo na ktoré sa vzťahuje pečať, sa zabezpečuje buď kontextom, v ktorom sa podpis použije, napríklad CMS v PDF dokumente, alebo dodatočnými podmienkami, ako sú podmienky na použitie pri podpísaní ZIP kontajnera, ktorý v ZIP adresári obsahuje typ údajov a ich interpretáciu podľa špecifikácie uvedenej napríklad v štandarde pre ASiC, alebo sa použije podpísaný atribút alebo element s dodatočnými informáciami o type.

Pri CMS podpise, ak je nejednoznačné určenie vizualizácie podľa OID *id-aa-contentType*, sa použije aj *id-aa-contentHint* s *contentDescription* obsahujúci MIME *Content-Type.*

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

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

```
Attribute SEQUENCE {
 attrType OBJECT IDENTIFIER 1.2.840.113549.1.9.16.2.4 id-aa-contentHint
 attrValues SET {
  ContentHints SEQUENCE {
   contentDescription UTF8String 'MIME-Version: 1.0
      Content-Type: text/plain; charset=UTF-8; name="Document.txt"
      Content-Disposition: attachment; filename="Document.txt"'
   contentType OBJECT IDENTIFIER 1.2.840.113549.1.7.1 id-data
  }
 }
}
```

Pri XML podpise, ak je nejednoznačné určenie vizualizácie podľa *MimeType* elementu v *DataObjectFormat* elemente, sa použije aj *Description* element obsahujúci MIME *Content-Type.*

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>`

```
<xades:DataObjectFormat ObjectReference="...">
  <xades:Description>
   Content-Type: text/plain; charset=UTF-8; name="Document.txt"
  </xades:Description>
<xades:MimeType>text/plain</xades:MimeType>
```

Pri ASiC jedna z viacerých ochrán formátu podpisovaného dokumentu je pomocou:

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.

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

}

2. Systém použitý na validáciu kvalifikovaného elektronického podpisu poskytuje spoliehajúcej sa strane správny výsledok procesu validácie a umožňuje spoliehajúcej sa strane odhaliť akékoľvek problémy súvisiace s bezpečnosťou.

{ R-2 Spoliehajúcej sa strane je poskytnutá podpísaná alebo zapečatená správa validácie, ktorá primerane identifikuje a popisuje zistené problémy súvisiace s bezpečnosťou.

The end of the validation report "R-2" contains the sentence of the time value to which the validation was performed. It can be the current time or the time value from the PoE. When the PoE is used, the PoE is identified according to SRId value of the PoE digital signature and also the issuer of the PoE is provided according to the QTSP identifier included in TL. The content described in the square brackets "[ ]" is replaced with the particular value.

Two types of sentences of the final line of the report "R-2" can be used:
1. "*R-2 The validation was performed to the current time* [current time].".
2. "*R-2 The validation was performed to the time* [the time value of PoE] *according to* [the type of the PoE] *identified by SRId* [Base64 encoded SRId of PoE] *issued by QTSP* [TLIxx-y] *according to TL*".
The content described in the square brackets "[ ]" identifying QTSP [TLIxx-y] is used (or replaced with another QTSP identifier) according to rules defined in the report "R-1.b)" for the QTSP identification in the report "R-1.b)".
}

5.4 Kvalifikovaná dôveryhodná služba uchovávania kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí

{ URI Identifikácia v dôveryhodnom zozname *ServiceTypeIdentifier*:
"http://uri.etsi.org/TrstSvc/Svctype/PSES/Q" }

5.4.1 SD čl. 34 a 40 nariadenia (EÚ) č. 910/2014

Kvalifikovaná dôveryhodná služba uchovávania kvalifikovaných elektronických podpisov a pečatí podľa článkov 34 a 40 nariadenia (EÚ) č. 910/2014 spĺňa tieto požiadavky:
Kvalifikovanú dôveryhodnú službu uchovávania kvalifikovaných elektronických podpisov a pečatí môže poskytovať iba kvalifikovaný poskytovateľ dôveryhodných služieb, ktorý používa postupy a technológie, ktoré umožňujú predĺžiť dôveryhodnosť kvalifikovaného elektronického podpisu a pečate aj na obdobie po uplynutí technologickej platnosti.
Kvalifikovaný elektronický podpis (pečať) je vzhľadom na definíciu kvalifikovaného elektronického podpisu (pečate) uvedenú v čl. 3 ods. 12 (ods. 27) nariadenia (EÚ) č. 910/2014, zdokonalený elektronický podpis (pečať) vyhotovený s použitím zariadenia na vyhotovenie kvalifikovaného elektronického podpisu (QSCD) a založený na kvalifikovanom certifikáte pre elektronické podpisy (pečate).
Formát zdokonaleného elektronického podpisu / pečate definuje príloha vykonávacieho rozhodnutia Komisie (EÚ) 2015/1506 prostredníctvom zoznamu technických špecifikácií pre zdokonalené elektronické podpisy XML, CMS alebo PDF a pre podpisový kontajner vo formáte ASiC.

{ Službu uchovávania expirovaných a zrušených certifikátov, ktoré súvisia so službami s kvalifikovaným štatútom, ktorým kvalifikovaný štatút udelil úrad, zabezpečuje úrad podľa štandardov NBÚ v dôveryhodnej infraštruktúre podľa čl. 17 ods. 5 nariadenia (EÚ) č. 910/2014 na základe § 11 ods. 1 písm. f) a g) zákona č. 272/2016 Z. z.
Postupy a technológie, ktoré umožňujú predĺžiť dôveryhodnosť kvalifikovaného elektronického podpisu a pečate aj na obdobie po uplynutí technologickej platnosti, sú založené na zabezpečení integrity kvalifikovaného elektronického podpisu a pečate. Zabezpečenie integrity je buď pomocou integritného podpisu (pečate) definovaného v štandardoch NBÚ s kvalifikovanou elektronickou časovou pečiatkou, kedy certifikát na validáciu integritného podpisu (pečate) je uvedený ako identifikátor služby v dôveryhodnom zozname. Ak sa na zabezpečenie integrity použijú ekvivalentné postupy integritného podpisu (pečate) zabezpečujúce požiadavky nariadenia (EÚ) č. 910/2014, certifikát na validáciu ich použitia, napríklad vo forme podpísanej alebo zapečatenej potvrdenky o poskytnutí "Kvalifikovanej služby uchovávania kvalifikovaných elektronických podpisov a pečatí", je uvedený ako identifikátor služby v dôveryhodnom zozname.

V postupoch musí byť dodržané pravidlo dopĺňania kvalifikovanej elektronickej časovej pečiatky do podpisu alebo pečate, alebo ako samostatnej kvalifikovanej elektronickej časovej pečiatky v čase platnosti predchádzajúcej kvalifikovanej elektronickej časovej pečiatky, ktorá zahŕňa položky podpisu, pečate, elektronických časových pečiatok a dokumentov, ktoré boli podpísané alebo zapečatené.
Služba zabezpečuje len podpis a pečať, pričom podpísaný alebo zapečatený dokument nemusí byť pre službu dostupný (môže obsahovať citlivé údaje) a pre službu sa môže poskytnúť len hash hodnota z podpísaného alebo zapečateného dokumentu, prípadne viacero hash hodnôt vytvorených rôznymi hash funkciami, napríklad neskôr, pri dlhodobejšom uchovávaní.
Pre dopĺňanie kvalifikovaných elektronických časových pečiatok môžu byť použité postupy definované v nasledujúcich formátoch podpisov (pečatí):
ETSI EN 319 122-1 v1.1.1 - CAdES digital signatures s využitím *ats-hash-index-v3* atribútu v pridanom atribúte *archive-time-stamp-v3*, ktorý obsahuje kvalifikovanú elektronickú časovú pečiatku.
ETSI EN 319 132-1 v1.1.1 - XAdES digital signatures s využitím elementu *ArchiveTimeStamp*, ktorý obsahuje kvalifikovanú elektronickú časovú pečiatku.
ETSI EN 319 142-1 v1.1.1 - PAdES digital signatures s využitím objektu Document Time-stamp, ktorý obsahuje kvalifikovanú elektronickú časovú pečiatku.
Pre PDF dokumenty podľa ISO 32000-2 PDF verzie 2 sa postupuje podľa ISO 14533-3 Processes, data elements and documents in commerce, industry and administration -- Long term signature profiles -- Part 3: Long term signature profiles for PDF Advanced Electronic Signatures (PAdES) s využitím objektu Document Timestamp, ktorý obsahuje kvalifikovanú elektronickú časovú pečiatku.
}

5.5 Kvalifikovaná dôveryhodná služba vyhotovovania kvalifikovaných elektronických časových pečiatok

{ URI Identifikácia v dôveryhodnom zozname *ServiceTypeIdentifier*:
"http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST" }

5.5.1 SD čl. 42 nariadenia (EÚ) č. 910/2014

Kvalifikovaná elektronická časová pečiatka kvalifikovanej dôveryhodnej služby podľa čl. 42 nariadenia (EÚ) č. 910/2014 spĺňa tieto požiadavky:
a) spája dátum a čas s údajmi spôsobom, ktorý v rozumnej miere zamedzuje možnosť nezistiteľnej zmeny údajov;

{ Realizácia je jedným z dvoch postupov, kde je použitá položka *MessageImprint*, ktorá reprezentuje spájané údaje a je definovaná v IETF RFC 3161 - Time-Stamp Protocol (TSP).

```
MessageImprint ::= SEQUENCE  {
      hashAlgorithm        AlgorithmIdentifier,
      hashedMessage        OCTET STRING  }
```

1. postup (elektronická časová pečiatka **implementovaná interným CMS podpisom** elektronického dokumentu typu *TSTInfo* definovaného v IETF RFC 3161), kde položku *MessageImprint* reprezentujúcu (časovo opečiatkované) údaje spája objekt typu *TSTInfo* definovaný v IETF RFC 3161 s dátumom a časom uvedeným v položke *genTime* objektu *TSTInfo*. Objekt *TSTInfo* je podpísaný CMS zdokonaleným elektronickým podpisom IETF RFC 5652, ktorý spĺňa požiadavky podľa IETF RFC 3161 a IETF RFC 5816, vyžadujúce použitie podpísanej položky *SigningCertificateV2* obsahujúcej *ESSCertIDv2* definovanej v IETF RFC 5035. CMS zdokonalený elektronický podpis časovej pečiatky musí obsahovať certifikát na jeho validovanie, ktorý je uvedený aj v dôveryhodnom zozname v kvalifikovanej službe vyhotovovania kvalifikovaných elektronických časových pečiatok. Služba kvalifikovanej elektronickej časovej pečiatky primerane spĺňa požiadavky ETSI EN 319 421 v1.1.1: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps.

2. postup (elektronická časová pečiatka **implementovaná nad OCSP protokolom** IETF RFC 6960) je definovaný len pre elektronickú časovú pečiatku z digitálneho podpisu (zo zdokonaleného elektronického podpisu alebo zo zdokonalenej elektronickej pečate). Položka *MessageImprint* reprezentuje (časovo opečiatkované) údaje spájané s dátumom a časom, kde položka *hashedMessage* obsahuje hash hodnotu z DER kódovaného digitálneho podpisu. Napríklad pri CMS podpise neobsahuje TAG a LEN z položky *SignerInfo.signature* typu *OCTET STRING*, ale len hodnotu *OCTET STRING* digitálneho podpisu a pri XML podpise sa počíta z obsahu <SignatureValue> elementu bez XML tag, po dekódovaní base64 kódovania. Položka *MessageImprint* je uložená v OCSP rozšírení *Nonce* definovanom v IETF RFC 6960 (Online Certificate Status Protocol) pre OCSP žiadosť a pre OCSP odpoveď. OCSP odpoveď spája *MessageImprint* uložený v OCSP rozšírení *Nonce* s dátumom a časom uvedeným v položke *producedAt* OCSP odpovede definovanej v IETF RFC 6960. OCSP odpoveď v objekte *BasicOCSPResponse,* musí obsahovať certifikát na validáciu podpisu OCSP odpovede, ktorý je uvedený aj v dôveryhodnom zozname v kvalifikovanej dôveryhodnej službe. Certifikát na validáciu podpisu OCSP odpovede môže obsahovať rozšírenie certifikátu *certificatePolicies* OID (2.5.29.32) (kapitoly 8.1.1 a 8.2.2.6 Rec. ITU-T X.509) s OID 1.3.158.36061701.1.3.2 certifikačnou politikou zverejnenou na webovom sídle NBÚ, ktorá uľahčí aplikáciám overujúcim elektronické časové pečiatky identifikovať použitie objektu OCSP odpovede aj ako objektu elektronickej časovej pečiatky. Aplikácie overujúce elektronické časové pečiatky identifikujú použitie elektronickej časovej pečiatky nad OCSP pomocou úspešného dekódovania ASN.1 typu *MessageImprint* z údajov uložených v OCSP rozšírení *Nonce*. Služba kvalifikovanej elektronickej časovej pečiatky primerane spĺňa požiadavky ETSI EN 319 421 v1.1.1 (Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps), okrem požiadavky uvedenej v prvej vete v kapitole 7.7.1EN 319 421 v1.1.1, kde profil definovaný v ETSI EN 319 422 je nahradený profilom uvedeným pre OCSP službu "Kvalifikovaná dôveryhodná služba overovania (verification) kvalifikovaných certifikátov" a písmeno d) kapitoly 7.7.1 EN 319 421 v1.1.1 sa aplikuje pre kľúčový pár pre podpisovanie OCSP odpovede.

}

b) je založená na presnom zdroji času prepojenom s koordinovaným svetovým časom a

{ presnosť času musí byť minimálne na jednu sekundu
}

c) je podpísaná zdokonaleným elektronickým podpisom alebo zapečatená zdokonalenou elektronickou pečaťou kvalifikovaného poskytovateľa dôveryhodných služieb alebo rovnocennou metódou.

{ Aktuálne sú použité len zdokonalené elektronické podpisy založené na ASN.1 jazyku typu CMS zdokonaleného elektronického podpisu IETF RFC 5652 z objektu *TSTInfo* IETF RFC 3161 a zdokonaleného elektronického podpisu objektu *ResponseData* z *BasicOCSPResponse*, ktorého typ v ASN.1 jazyku definuje IETF RFC 6960.
}

5.6 Kvalifikovaná dôveryhodná elektronická doručovacia služba pre registrované zásielky

{ URI Identifikácia v dôveryhodnom zozname *ServiceTypeIdentifier*:
"http://uri.etsi.org/TrstSvc/Svctype/EDS/Q" a "http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q" }

5.6.1 SD čl. 44 nariadenia (EÚ) č. 910/2014

Predpokladá sa, že Komisia pre tento typ služby vydá v blízkej dobe implementačné akty.

Príloha A (informatívna) Zoznam použitej literatúry

Základná legislatíva Slovenskej republiky a EÚ pre dôveryhodné služby:
http://www.nbu.gov.sk/urad/pravne-predpisy/doveryhodne-sluzby/index.html

Štandardy NBÚ:
http://www.nbu.gov.sk/doveryhodne-sluzby/standardy/index.html

Schémy NBÚ:
http://www.nbu.gov.sk/doveryhodne-sluzby/dohlad/index.html

Príloha B História

Verzia	Dátum	Poznámka	Vypracoval
Verzia 1.0	20.9.2016	Prvé vydanie	Ing. Peter Rybár, NBÚ
Verzia 1.1 5767/2016/IBEP/OA-016	30.11.2016	Zjednotenie postupov so SNAS	Ing. Peter Rybár, NBÚ Ing. Lenka Gondová, SNAS
Verzia 1.2 1353/2017/IBEP/OA-001	18.1.2017	Jednotná šablóna dokumentov, spresnenia	Ing. Peter Rybár, NBÚ
Verzia 1.3 1353/2017/IBEP/OA-006	3.3.2017	Spresnenie 5.2.5 a 5.3.1	Ing. Peter Rybár, NBÚ