Version 1.4

Supervision Scheme of Qualified Trust Services defined by the Supervisory Body

This standard shall enter into force on 1 August 2019

This English version of the Slovak document No. 05968/2019/ORD-001 is for reference purposes only. In case of conflict between the English translation and the original Slovak version, the Slovak version shall prevail and supersede the English translation as the original version. Therefore, only the National Security Authority (NSA) Deliverables published by NSA in their original language shall be used for evaluation of products and technical assessment.

Regulation and Supervision Division | National Security Authority
Budatínska 30 | 851 06 Bratislava | Slovak Republic
tel.: +421 2 6869 1111 | fax: +421 2 6869 1700
e-mail: podatelna@nbu.gov.sk | https://www.nbu.gov.sk/

Content

1 Introduction

Supervision scheme of qualified trust services defined by the supervisory body (hereinafter referred to as the SS or scheme) is carried out in accordance with Clause II of Annex I of Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

The SS is used for assuring the common essential supervision requirements to ensure a comparable security level of qualified trust services across the Union. The scheme ensures this objective by mapping of legal requirements into the technical procedures, and thus achieving the goal, to ease the consistent application of those requirements across the Union and it shall allow Member States to adopt comparable procedures based on mutual exchange of information on their supervision activities and best practices in the field.

Notice: Text of the scheme shall be continuously updated. In order to distinguish unambiguously legislative requirements from technical requirements, the legislative requirement is placed in front of a curly bracket {} whilst its obligatory technical fulfilment is placed in the curly bracket.

2 Scope

The SS defines the rules applied by the supervisory body at supervision of the qualified trust services and is the base for the certification scheme of the conformity assessment body.

According to Article 3(18) of the Regulation (EU) No 910/2014 [1], the conformity assessment body means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008 [2], which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service providers and the qualified trust services it provides.

The certification scheme of the conformity assessment body is created by the National Security Authority (hereinafter referred to as "NSA") in cooperation with conformity assessment bodies and the accreditation body according to requirements defined in the SS, ISO/IEC 17065 [3], Act No 272/2016 Coll. on Trust Services for Electronic Transactions in the Internal Market and on the Amendment and Supplementing of certain Acts (Trust Services Act) [4], Regulation (EU) No 910/2014 and in the accreditation scheme of the Slovak National Accreditation Service (hereinafter referred to as "SNAS").

SNAS defines the accreditation scheme MSA-CP/05 for the Slovak Republic mutatis mutandis according to ETSI EN 319 403 v2.2.2. (Requirements for conformity assessment bodies assessing Trust Service Providers) [5] and according to requirements of legislation for trust services from which specific legislative requirements for particular qualified trust services are transferred to technical procedures of the SS.

The SNAS gives official acreditation to the conformity assessment body pursuant to Article 3(18) of the Regulation (EU) No 910/2014. The SNAS when accrediting proceeds according to the accreditation scheme. It shall publish the accreditation granted together with the Annex containing the reference to the certification scheme on the SNAS website.

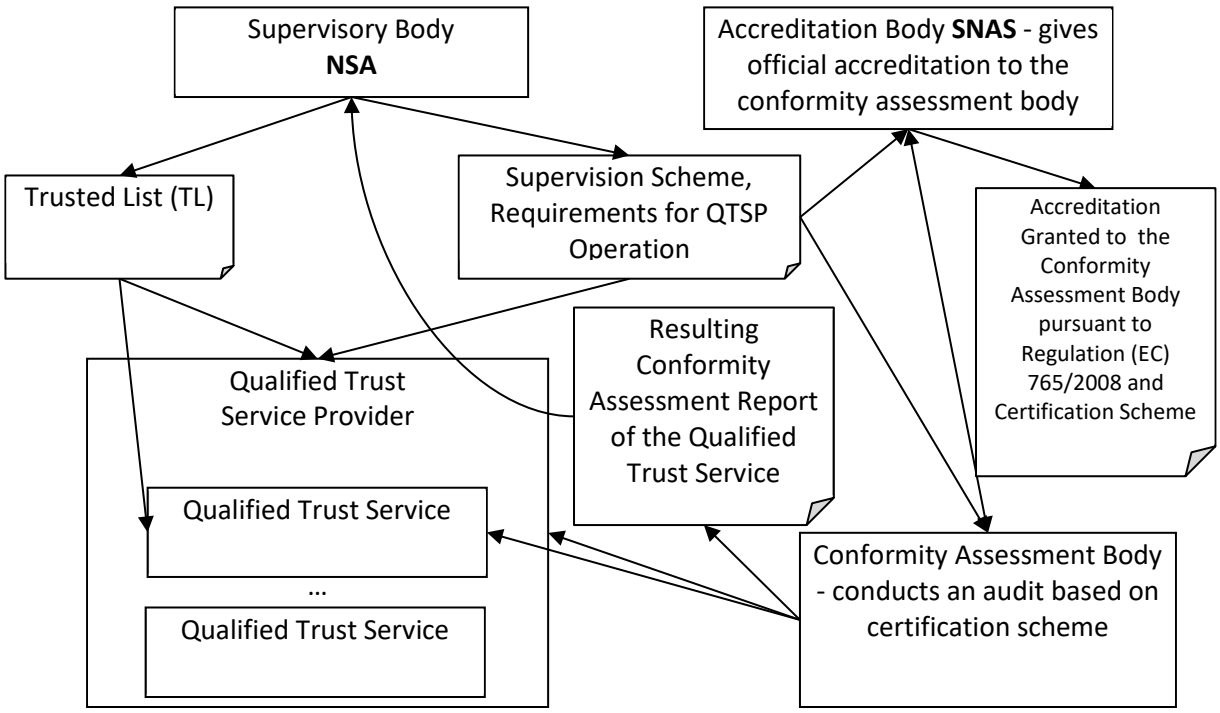


Figure 1 – Supervision Scheme

Pursuant to Regulation (EU) No 910/2014 a qualified status can be granted to 9 trust services:

1. Qualified trust service of qualified certificate creation and verification of electronic signature (see Clause 5.2)
2. Qualified trust service of qualified certificate creation and verification of electronic seal (see Clause 5.2)
3. Qualified trust service of qualified certificate creation and verification of website authentication (see Clause 5.2)
4. Qualified validation service of qualified electronic signatures (see Clause 5.3)
5. Qualified validation service of qualified electronic seals (see Clause 5.3)
6. Qualified preservation service of qualified electronic signatures (see Clause 5.4)
7. Qualified preservation service of qualified electronic seals (see Clause 5.4)
8. Qualified trust service of qualified electronic time stamp creation (see Clause 5.5)
9. Qualified electronic registered delivery service (see Clause 5.6)

3 References

References to documents defining used types and procedures.

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing the Directive 1999/93/EC

[2] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (Text with EEA relevance).

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

[4] Act No 272/2016 Coll. on Trust Services for Electronic Transactions in the Iternal Market and on the Amendment and Supplementing of certain Acts (Trust Services Act)

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

[6] Decree No 55/2014 Coll. of the Ministry of Finance of the Slovak Republic on Standards for Information Systems of Public Administration

[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] NSA Documentation of TL X.509 XML scheme for a trusted list (see http://tl.nbu.gov.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] Supervision Scheme of the NSA (see http://tl.nbu.gov.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] Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[19] Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of the Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

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

[21] ISO 14533-4 Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 4: Attributes pointing to (external) proof of existence objects used in long term signature formats (PoEAttributes) - (Available at https://www.iso.org/standard/72835.html)

4 Abbreviations

ASN.1	Abstract Syntax Notation 1
CA	Certification Authority
CAB	Conformity Assessment Body
CAdES	CMS Advanced Electronic Signature
DId	Document Identifier

Note 1: The structure of the DId is the same as is defined for DSId and contains the hash algorithm identifier with parameters and the hash value of the electronic document. If the Did is used for implementation of signature time-stamp (STS) over OCSP, Did will be inserted into *nonce* of the OCSP item (IETF RFC 6960) as data connected with the time value situated in the *producedAt* item of OCSP response.

DSId	Document Signature Identifier

Note 1: DSId is defined in Clause 3.3 of ISO 14533-4 [21] and contains an identifier of the hash algorithm with parameters and the hash value of the digital signature (DER encoded result of the asymmetric function) in DER encoded object ASN.1 type of the *MessageImprint*, defined in EITF RC 3161.

CMS	Cryptographic Message Syntax
CP	Certificate Policy
NSA RCA CP	Certificate Policy of the NSA Root Certification Authority http://ep.nbusr.sk/kca/cp_kca.html
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules (for ASN.1)
eIDAS	Regulation the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
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
NSA	National Security Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier (in dot notation, e.g. 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

RCA	Root Certification Authority
QC	Qualified Certificate
QCP SK	Qualified Certificate Policy of Slovakia
QSCD	Qualified Electronic Signature/Seal Creation Devices
QTS	Qualified Trust Service
QTSP	Qualified Trust Service Provider
SS	Supervision Scheme of Qualified Trust Services defined by the Supervisory Body
SNAS	Slovak National Accreditation Service
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

5 Mapping of requirements

5.1 Common requirements for qualified trust service providers

5.1.1 SS of Article 27(5) and Article 37(5) of Regulation (EU) No 910/2014

If the Member State requires an electronic signature (seal) also of a lower security level than a qualified electronic signature (seal) to use an online service offered by, or on behalf of, a public sector body, the Regulation (EU) No 910/2014 places a duty on recognition of alternative formats whose methods are defined in implementing acts referred to in Article 27 (5) and Article 37 (5) of the Regulation (EU) No 910/2014.

{ In order to prevent the situation when an unpredictable number of alternative formats shall be recognised, it is required to use the electronic signature (seal) which is not of a lower security level than a qualified electronic signature (seal), if a public sector body for the service offered by, or on behalf of, does not state otherwise (if a public sector body is a qualified trust service provider, it can provide that information in the conditions of the use of that service according to Article 24 (2) point d) of the Regulation (EU) No 910/2014).

Bodies to which applies Act No 95/2019 Coll. on Information Technologies in Public Administration and on Amendments and Supplementing certain Acts (ITPA Act) shall in creating and verifying the signature/seal proceed also in accordance with legislation implementing public administration information systems standards, which will supersede procedures stated in Articles 57a to 57e of Decree No 55/2014 Coll. of the Ministry of Finance of the Slovak Republic on Standards for Information Systems of Public Administration [6]. }

5.1.2 SS of Articles 19 and 24 of Regulation (EU) No 910/2014

Trust services with the qualified status are provided in compliance with Articles 19 and 24 of the Regulation (EU) No 910/2014.

{ European Union Agency for Network and Information Security (hereinafter referred to as "ENISA") has prepared recommendations particularly for Articles 19 and 24(2) of the Regulation (EU) No 910/2014 which are published on the ENISA website (https://www.enisa.europa.eu/publications/tsp-conformity-assessment). Common requirements for operation of qualified trust service providers (hereinafter referred to as QTSP) defined by the supervisory body are provided in the document "Requirements for operation of qualified trust service providers defined by a supervisory body" (hereinafter referred to as "*Requirements for QTSP"*, see http://ep.nbusr.sk/kca/tsl/PoziadavkyPrevadzkyTSP.pdf). The document *Requirements for QTSP* is part of this Supervision scheme and is published in the separate document regarding its scope and definition of joint actions for all trust services. The document *Requirements for QTSP* covers mainly a mapping of legal requirements of Articles 19 and 24(2) of the Regulation (EU) No 910/2014 into technical procedures concerning particularly buildings, personnel, software and technical equipment of qualified trust services of qualified trust service providers and of conformity assessment bodies mutatis mutandis. The document *Requirements for QTSP* also defines the minimal items of forms that shall be included in procedures required by legislation, as for example is a list of form items being sent to the NSA according to Article 21(1) of the Regulation (EU) No 910/2014 and Article 3(1) of the Act No 272/2016 Coll.
Trust services meet mutatis mutandis the requirements laid down in ETSI EN 319 401 (Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [7]. }

5.1.3 SS of Article 46 of Regulation (EU) No 910/2014

5.1.3.1 Electronic document

In accordance with Article 46 of the Regulation (EU) No 910/2014 an electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.

{ To support the legal effect of the electronic document Regulation (EU) No 910/2014 defines rules enabling to secure

- integrity of the electronic document,
- correct interpretation of the content of the electronic document and
- link to the identity of the person, who secured it through qualified electronic signature, qualified electronic seal or qualified electronic time-stamp.

Electronic document may be secured independently or jointly with other electronic documents, namely through several or one qualified electronic signature, qualified electronic seal or qualified electronic time-stamp.

Secured electronic document (documents) is identified based on the identifier of the signature of the signed document (documents) marked DSId, whose binary value (defined also in Clause 3.3 in ISO 14533-4, [21]) contains hash from the digital signature (DER encoded result of the asymmetric function of signing – the result is stored in the field of advanced electronic signature, it is unchangeable in time and unambiguous for every signature).

The relying party may only work with the electronic document that was secured by

- the person indicated in the electronic document as signer / seal creator or
- the person, to whom the securing through signature /seal follows from the context of electronic signature usage of the particular document.

E.g. a pdf file may encompass several PDF document versions and only the version identified based on DSId may be worked with, secured by the person identified in accordance with clause 5.1.3.4. By using DSId the signature of one PDF document version is identified or one signature from ASiC container, or one signature from nested containers in ASiC, while ASiC may encompass a huge number of signatures of one or several various documents or PDF document versions, if PDF is signed by a PDF signature as is stored in ASiC.

With multiple signature it is recommended to sign electronic documents in ASiC container, where it is possible to sign at the same time other documents, add other documents and jointly sign all the documents.

If it is necessary to determine date and time, after which could occur securing of electronic document, e. g. if the electronic document is multiply secured, from the available qualified electronic time stamps covering electronic document shall be selected the one with the least date and time (e.g. see clause 5.6.1 "SS Article 44 of Regulation (EU) No 910/2014" – how to determine the accuracy of the date and time of sending and receipt).

If it is necessary to determine date and time, after which could occur signing / sealing of electronic document, e. g. if the electronic document is multiply secured, from the available qualified electronic time stamps covering electronic document and whose are covered by signature / seal, shall be selected the one with the highest date and time (e.g. see how to determine the date and time when one or several authorizations of one electronic document are used in Article 23a(1) item b) of the Act No. 305/2013 Coll on the Electronic Form of Governance Conducted by Public Authorities and on Amendment of certain Acts (e-Government Act) as amended.)

If it is necessary to determine date and time, before which could occur securing (signing / sealing) of electronic document (the date and time of signing / sealing), e. g. if the electronic document is multiply secured, from the available qualified electronic time stamps covering signature / seal, shall be selected the one with the least date and time, though if electronic document must be multiply signed / sealed with more persons, the date and time of signing / sealing of the electronic document is the date and time of securing of such the person whose signing / sealing is with the highest date and time.

If an electronic document is being signed electronically, the fields where in the written form the handwritten signature is included, this field should include words

- "electronically signed" surname / name and surname and as the case may be authorization[1]/authorization[2] and their number after launching the service in accordance with Article 23a of the Act No. 305/2013 Coll.) or
- "signed electronically", whereas "signed electronically" shall be indicated only if the name of the person or their identification data are already indicated in this component.

Based on the data indicated in the document, like name of the person or their potential other identification data, e.g. number of authorization in accordance with Article 9 of Act No 272/2016 Coll. (Trust Services Act) it is possible in the signature container to search for qualified electronic signature, if the container encompasses several electronic signatures of the same document. After finding the belonging electronic signature the relying party shall jot down the signature identifier for identification of electronic documents signed by this signature. DSId is e.g. used for identification of signed documents in systems working with electronic documents like documents register or in acquiring of the validation report from qualified trust service of validation of qualified electronic signatures / seals.

5.1.3.2 Integrity

Integrity of the electronic document is proved by the comparison of the secured hash value and computed hash value from electronic document through hash function, whereas standard manner of indicating of hash function identification, its potential parameters and hash function value is a binary value of DId (defined also in clause 3.2 in ISO 14533-4 [21]), which if stated in the text, shall be encoded appropriately in Base64 (IETF RFC 4648), "base64url" (IETF RFC 4648) or in hex encoding "base16" / "hex" (IETF RFC 4648).

5.1.3.3 Interpretations

To ensure correct interpretation of the content of the electronic document it is necessary to secure integrity of the electronic document as well as correct manner of interpretation of the respective bits of electronic document, which is done through data marked as DTId.
DTId data, stated also in Annex F in ISO 14533-4 [21], are following:
In CMS signature, if there is an ambiguous specification of visualization according to the attribute identified by *id-aa-contentType* OID, then the *id-aa-contentHint* attribute (IETF RFC 2634) should be used with item *contentDescription* containing the UTF-8 encoded MIME header defined in IETF RFC 2045 containing fields: *MIME-Version*, *Content-Type* and *Content-Disposition* with *attachment* disposition-type and *filename* parameter (see IETF RFC 2183, Section 2.2 and 2.3, IETF RFC 6532, Section 3.1, or IETF RFC 7231, Section 3.1).

[1] "**Authorization No**." shall be indicated in accordance with Article 9 of the Act No 272/2016 Coll. Trust Services for Electronic Transactions in the Internal Market and Amendment of certain Acts (Trust Services Act)

[2] "**Authorization No**." shall be indicated in accordance with Article 23a of the Act No. 305/2013 Coll on the Electronic Form of Governance Conducted by Public Authorities and on Amendment of certain Acts (e-Government Act) as amended

The following is an example of a MIME header:

Content-hints CMS signed attribute values have ASN.1 type *contentHints*.

```
ContentHints ::= SEQUENCE {
   contentDescription UTF8String (SIZE (1..MAX)) OPTIONAL
      'MIME-Version: 1.0
      Content-Type: text/plain; charset=UTF-8; name="Document.txt"
      Content-Disposition: attachment; filename="Document.txt"',
   contentType ContentType "1.2.840.113549.1.7.1" } -- id-data
id-aa-contentHint OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
   rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 4}
```

In XML signature, if there is an ambiguous specification of visualization according to the MimeType element in the DataObjectFormat element, the Description element containing MIME header fields should be used.

The following is an example of a MIME header:

```
<xades:DataObjectFormat ObjectReference="...">
   <xades:Description>
      MIME-Version: 1.0
      Content-Type: text/plain; charset=UTF-8; name="Document.txt"
      Content-Disposition: attachment; filename="Document.txt"
   </xades:Description>
   <xades:MimeType>text/plain</xades:MimeType>
```

In ASiC, the protection of the type of the document being signed should be assured by including the document being signed in a signed ZIP file within an ASiC container (see the inner ZIP container in ETSI EN 319 162-1, 4.3.2 and B.1.3), where the file name extension is also protected and MIME type with parameters of the MIME *Content-Type* should be included in the component "file comment" of "4.3.12 Central directory structure" in signed ZIP file (see ZIP specification) or it should be included in ASiC elements "URI" and "MimeType" in "META-INF\ASiCManifest*.xml".

The following is an example of the content of the ZIP "file comment": `mimetype=text/plain; charset=UTF-8`

5.1.3.4 Linking the document with the identity of the person indicated in the signatory's certificate

Identity of the natural or a legal person is included in the signatory's certificate, reference to whom is protected by the signature of the signatory / by the seal of the seal creator. Reference with the hash value is included in the following singed components in the signature formats, whereas unprecise value of the name of the issuer and serial number of the certificate in signed component is reason for warning but not for invalidation of the signature / seal:

- **CMS** AdES: id-aa-signingCertificate (IETF RFC 2634) | id-aa-signingCertificateV2 (IETF RFC 5035)
- **PDF** AdES: id-aa-signingCertificate (IETF RFC 2634) | id-aa-signingCertificateV2 (IETF RFC 5035)
- **ASiC CMS** AdES: id-aa-signingCertificate (IETF RFC 2634) | id-aa-signingCertificateV2 (IETF RFC 5035)
- AdES **timestamp**: id-aa-signingCertificate (IETF RFC 2634) | id-aa-signingCertificateV2 (IETF RFC 5035)
- AdES **ASiC timestamp**: id-aa-signingCertificate (IETF RFC 2634) | id-aa-signingCertificateV2 (IETF RFC 5035)
- **XML** AdES: SigningCertificate (http://uri.etsi.org/01903/v1.3.2/XAdES.xsd) | Annex of Commission Implementing Decision No. 2015/1506 does not require SigningCertificateV2 (http://uri.etsi.org/01903/v1.3.2/XAdES01903v132-201601.xsd)
- **ASiC XML** AdES: SigningCertificate (http://uri.etsi.org/01903/v1.3.2/XAdES.xsd) | Annex of Commission Implementing Decision No. 2015/1506 does not require SigningCertificateV2 (http://uri.etsi.org/01903/v1.3.2/XAdES01903v132-201601.xsd)

}

5.2 Qualified trust service of qualified certificate creation and verification of electronic signature, electronic seal and website authentication

5.2.1 Identification

{ URI identification in trusted list *ServiceTypeIdentifier*:
"http://uri.etsi.org/TrstSvc/Svctype/CA/QC"
URI identification in trusted list in elements *ServiceInformationExtensions – Extension – AdditionalServiceInformation* if the service creates the certificate for:

- electronic signature: "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures"
- electronic seal: "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals"
- website authentication: "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication"

}

5.2.2 SS of Articles 17(5), 24, 28, 38 and Article 45 of Regulation (EU) No 910/2014

The service is provided particularly in compliance with Articles 24 and 28 of the Regulation (EU) No 910/2014 and with the requirements of the national legislation pursuant to Article 17(5) of the Regulation (EU) No 910/2014.

{ A procedure to perform the requirements of the national legislation is provided particularly in Clause 10 of the certificate policy of the NSA Root Certification Authority (hereinafter referred to as "NSA RCA CP") Object Identifier (OID) (1.3.158.36061701.0.0.0.1.2.2), profiling ETSI EN 319 411-2 V2.1.1 (2016-02) certificate policies for issuing the qualified certificates. Performance of the NSA RCA CP when issuing and verifying the qualified certificates shall be indicated for each qualified trust service in the document *Certification Practice Statement* (CPS).
Information in the trusted list according to Article 22 of the Regulation (EU) No 910/2014 is updated by the NSA on the basis of the sent conformity assessment report according to Articles 20 and 21 of the Regulation (EU) No 910/2014 which is built, in particular, on practices defined in CPS. The NSA proceeds according to the abovementioned statement when requiring a change in data (sent in the forms https://www.nbu.gov.sk/en/trust-services/e-forms/) in the trusted list, for example when requiring the authorization or the authorization change for issuing OCSP responses (partial qualified trust service of verification of qualified certificates of qualified trust service of qualified certificate creation) being specified in the trusted list in the element *AuthorizedService* which is a part of *URLContentTypeAndAuthorizedServiceList* element defined in additional XSD scheme according to documentation http://tl.nbu.gov.sk/kca/tsl/tlX509XMLSchemaDocumentation.pdf. }

5.2.3 SS of Articles 28(3) and 38(3) of Regulation (EU) No 910/2014

In accordance with Articles 28(3) and 38(3) of the Regulation (EU) No 910/2014, qualified certificates for electronic signatures (seals) may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures (seals).
In accordance with recital 54 of the Regulation (EU) No 910/2014 cross-border interoperability and recognition of qualified certificates is a precondition for cross-border recognition of qualified electronic signatures. Therefore, qualified certificates should not be subject to any mandatory requirements exceeding the requirements laid down in this Regulation. However, at national level, the inclusion of specific attributes, such as unique identifiers, in qualified certificates should be allowed, provided that such specific attributes do not interfere with cross-border interoperability and recognition of qualified certificates and electronic signatures.

{ Non-mandatory additional specific attributes are in particular data for unambiguous identification enabling to prepare in advance especially information systems for automated processing of at least a minimal set of identifier types that are defined in the field *Subject* of the certificate in one or more

components *serialNumber* being identified by an object identifier (OID) (2.5.4.5). One component *serialNumber* contains only one value consisting of the following characters:

3 characters

1. "PAS" for identification based on passport number
2. "IDC" for identification based on identity card number
3. "PNO" for identification based on personal number (a personal identification number for Slovak citizens and foreigners who were assigned a personal identification number pursuant to Act No 301/1995 Coll. on Personal Identification Number
4. "NTR" for identification based on the registration number of the organisation.
5. "PSD" for PSD2 Authorization Number defined in ETSI TS 119 495.

2 characters containing the country code according to ISO 3166 (for Slovakia "SK")
1 character "-" (ASCII 0x2D)
Non-mandatory 4 characters giving precision, the type of which is specified by first three initial characters and the country code, for example:

3 characters:

1. "JUS" giving precision to "PNO" or "IDC" for identification based on identity card number of judges and on other cards in administration and in the format according to procedure at http://www.justice.gov.sk/, for example "IDCSK-JUS-123123",
2. "NSA" giving precision to "PNO" or "IDC" for identification based on identity card number of the NSA officers and on other cards in administration and in the format according to procedure at http://www.nbu.gov.sk/,
3. "POL" giving precision to "PNO" or "IDC" for identification based on identity card number of the police and on other cards in administration and in the format according to procedure at http://www.minv.sk/,
4. "MIL" giving precision to "PNO" or "IDC" for identification based on identity card number of the armed forces of the Slovak Republic and on other cards in administration and in the format according to procedure at http://www.mod.gov.sk/.

1 character "-" (ASCII 0x2D)
Characters of data the type of which is specified by first three initial characters and the country code (and by optional 4 characters).

Identification based on "NTR" can be included also in *organizationIdentifier* OID (2.5.4.97) in accordance with the procedure defined for the component *serialNumber*. Identification based on "PSD" should be included in *organizationIdentifier* OID (2.5.4.97)
If the component *serialNumber* contains other types of data than those defined above, they must not be used if the first three characters were to be identical with the characters defined above in points 1 to 4.
If the qualified certificate is issued to a person younger than 18 years and the component *serialNumber* OID (2.5.4.5) does not contain a personal identification number, the date of birth shall be indicated in the certificate extension *subjectDirectoryAttributes* OID (2.5.29.9) in the component *DateOfBirth* OID (1.3.6.1.5.5.7.9.1).

Non-mandatory additional specific attributes comprise also information included in the field *Subject* of the certificate, in the component *commonName* (the maximum length 64 characters as an example stated in the Annex C Rec. ITU-T X.520|ISO/IEC 9594-6 does not have to be maintained, look up

the restrictions in Clause 6 of C Rec. ITU-T X.520|ISO/IEC 9594-6), containing for example a text with the heplful information in order to facilitate a non-automated handling of a certificate such as a shortened subject name or a string "QES xy" to distinguish certificates for signature (or for seal) issued to the same subject with the additional sequential number xy if for example QSCD device (smart card) contains more certificates. }

5.2.4 SS of Annexes I, III and IV of Regulation (EU) No 910/2014

Table T1 – SS of Annexes I, III and IV of Regulation (EU) No 910/2014

Line identification	Qualified certificates contain: { implementation of the Regulation requirement }

T1.I, III, IV (a)	An indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified one:
	{
	1) extension *QCStatements* OID (1.3.6.1.5.5.7.1.3) contains the field *QcCompliance* OID (0.4.0.1862.1.1), and
	2) certificates issued on the basis of a qualified status being granted to a qualified trust service by the NSA, shall contain the certificate extension *certificatePolicies* OID (2.5.29.32) (Clauses 8.1.1 and 8.2.2.6 Rec. ITU-T X.509) that shall contain as a minimum OID of the NSA certificate policy OID (1.3.158.36061701.0.0.0.1.2.2).
	}
	
	An indication, at least in a form suitable for automated processing, that the certificate has been issued for electronic signature.
	{
	The field *Subject* of the certificate contains as a minimum one component identified through OID components: *pseudonym* OID (2.5.4.65), *surname* OID (2.5.4.4), *givenName* OID (2.5.4.42).
	}
	
	An indication, at least in a form suitable for automated processing, that the certificate has been issued for electronic seal.
	{
	The field *Subject* of the certificate contains as a minimum the component *organizationName* OID (2.5.4.10) and must not contain any component identified through OID components: *pseudonym* OID (2.5.4.65), *surname* OID (2.5.4.4), *givenName* OID (2.5.4.42).
	}
	
	An indication, at least in a form suitable for automated processing, that the certificate has been issued for website authentication.
	{
	The certificate extension *extendedKeyUsage* OID (2.5.29.37) contains as a minimum the field *serverAuthentication* OID (1.3.6.1.5.5.7.3.1).
	}

T1.I, III, IV (b)	A set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and: — for a legal person: the name and, where applicable, registration number as stated in the official records, — for a natural person: the person’s name.

	{ A certificate component *Issuer* contains: a set of data unambiguously representing the qualified trust service provider that issues the qualified certificates, including at least the Member State in which that provider is established in X.520 component *countryName* OID (2.5.4.6), and — for a legal person: at least the name in the component *organizationName* OID (2.5.4.10) and, where applicable, the registration number in the component *serialNumber* OID (2.5.4.5) or in the component *organizationIdentifier* OID (2.5.4.97) as stated in the official records in the format defined in "SS of Articles 28(3) and 38(3) of Regulation (EU) No 910/2014", —for a natural person: at least the person's name in components *surname* OID (2.5.4.4) and *givenName* OID (2.5.4.42). }
T1.I (c)	At least a name of a signatory or a pseudonym; if a pseudonym is used, it shall be clearly indicated. { The field *subject* of the certificate contains as a minimum in X.520 components at least a name of the signatory in components *surname* OID (2.5.4.4) and *givenName* OID (2.5.4.42) or a pseudonym in the component *pseudonym* OID (2.5.4.65); if a *pseudonym* is used in the component *commonName* OID (2.5.4.3), it shall be clearly indicated (at least the text "PSEUDONYM" shall be included in the component *commonName*). }
T1.III (c)	At least the name of the creator of the seal and, where applicable, registration number as stated in the official records. { The field *subject* of the certificate contains as a minimum in X.520 components at least the name of the creator of the seal in the component *organizationName* OID (2.5.4.10) and, where applicable, the registration number in the component *serialNumber* OID (2.5.4.5) or in the component *organizationIdentifier* OID (2.5.4.97) as stated in the official records in the format defined in "SS of Articles 28(3) and 38(3) of Regulation (EU) No 910/2014". }
T1.IV (c)	For natural persons: at least the name of the person to whom the certificate has been issued or a pseudonym. If a pseudonym is used, it shall be clearly indicated. For legal persons: at least the name of the legal person to whom the certificate is issued and, where applicable, registration number as stated in the official records. { The field *subject* of the certificate contains as a minimum in X.520 components: — for natural persons: at least the name of the person to whom the certificate has been issued - in *surname* OID (2.5.4.4) and *givenName* OID (2.5.4.42), or a pseudonym in the component *pseudonym* OID (2.5.4.65). If a *pseudonym* is used in *commonName* OID (2.5.4.3), it shall be clearly indicated (at least the text "PSEUDONYM" shall be included in the component *commonName*); — for legal persons: at least the name of the legal person to whom the certificate is issued in the component *organizationName* OID (2.5.4.10) and, where applicable, the registration number in the component *serialNumber* OID (2.5.4.5) or in the component *organizationIdentifier* OID (2.5.4.97) as stated in the official records in the format defined in "SS of Articles 28(3) and 38(3) of Regulation (EU) No 910/2014". }
T1.I, III (d)	Electronic signature /electronic seal validation data that correspond to electronic signature /electronic seal creation data { According to Clause 7.2 of Rec. ITU-T X.509.

	SubjectPublicKeyInfo ::= SEQUENCE { *algorithm AlgorithmIdentifier,* *subjectPublicKey BIT STRING }* An algorithm shall be in the list of algorithms and lengths included in valid signature policies published on the NSA website for the period during which the private key was used. Note: Taking into account the definition according to the Regulation (EU) No 910/2014 the qualified certificate for website authentication may not contain data for validation. The format also meets the definition of Rec. ITU-T X.509 for the attribute certificate. }
T1.IV (d)	Elements of the address, including at least city and State, of the natural or legal person to whom the certificate is issued and, where applicable, as stated in the official records.
T1.IV (e)	The domain name(s) operated by the natural or legal person to whom the certificate is issued.
T1.I, III (e) T1.IV (f)	Details of the beginning and end of the certificate's period of validity. { They are defined in the field *Validity* - according to Clause 7.2 of Rec. ITU-T X.509. *Validity ::= SEQUENCE {* *notBefore Time,* *notAfter Time }* Electronic signature (seal) creation data shall be used in time interval indicated in the field *Validity*. }
T1.I, III (f) T1.IV (g)	The certificate identity code which shall be unique for the qualified trust service provider. { A positive number of a maximum size 20 bytes according to Clause 7.2 of Rec. ITU-T X.509. *CertificateSerialNumber ::= INTEGER* }
T1.I, III (g) T1.IV (h)	The advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider. { A digital signature that shall be validated according to Clause 6.2 of Rec. ITU-T X.509. *SIGNATURE{ToBeSigned} ::= SEQUENCE {* *algorithmIdentifier AlgorithmIdentifier{{SupportedAlgorithms}},* *encrypted ENCRYPTED-HASH{ToBeSigned},* *... }* An algorithm of a key pair and hash function shall be in the list of algorithms and lengths included in valid signature policies published according to Article 11, point m) of the Act No 272/2016 Coll. on the NSA website for the period during which the private key was used. }
T1.I, III (h) T1.IV (i)	The location where the certificate for the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge. { An extension *id-pe-authorityInfoAccess* OID (1.3.6.1.5.5.7.1.1) defined in IETF RFC 5280 section 4.2.2.1 containing in the field *id-ad-caIssuers* OID (1.3.6.1.5.5.7.48.2) 1) http address of CA certificate of the issuer ".cer" or of cross certificates of the issuer ".p7c" in the CMS envelope of IETF RFC 2797 section 7.1. 2) It may contain an unambiguous identifier of the qualified trust service indicated in the national trusted list in the element 'TLServiceIdentifier'. The format of the TL service identifier 'TLIxx-y' consists of xx value that represents 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 y value may be also indicated in the "Name" fielf of the element "serviceName" in the form "(y)z", where "z" is the name of the service in the TL. The value of digital service identifier in 'TLServiceIdentifier' element is assigned by the TLSO in the TL (see http://ep.nbusr.sk/kca/tsl/tlX509XMLSchemaDocumentation.pdf and 5.5.3 ETSI TS 119 612). The value of 'TLServiceIdentifier' field of this service may be included in references to this service in the form 'TLIxx-y' in the qualified certificate extension *AuthorityInformationAccess* in the *accessMethod* field which contains *id-ad-caIssuers*. The trusted list identifier of the issuer service is included in the *accessLocation* field of *GeneralName* type as *directoryName* as a component of *X520SerialNumber* type. Example: *X520SerialNumber* = "TLISK-4" See: http://ep.nbusr.sk/kca/tsl/tsl.xml See: https://tools.ietf.org/html/rfc5280#section-4.2.2.1 https://tools.ietf.org/html/rfc2797 }
T1.I, III (i) T1.IV (j)	The location of the services that can be used to enquire about the validity status of the qualified certificate. { Certificate Revocation List (CRL defined in Rec. ITU-T X.509) is optional and Online Certificate Status Protocol (OSCP defined in IETF RFC 6960) is mandatory after post-termination transition period according to Article 18(5) of the Act No 272/2016 Coll. CRL shall be complete. OCSP and CRL shall also contain information about expired certificate, which is not necessary, if such information is provided on the basis of authorization indicated in the trusted list by a qualified trust service provider who was auhtorized to issue e.g. OSCP response: 1. by the qualified certificate issuer, or 2. by law, e.g. the NSA according to Article 11, point g) of the Act No 272/2016 Coll. Identification that CRL also contains expired certificates: *expiredCertsOnCRL* OID (2.5.29.60) CRL extension (see https://www.itu.int/rec/T-REC-X.509). OCSP response shall contain according to Article 18(5) of the Act No 272/2016 Coll. also *CertHash* OID (1.3.36.8.3.13) OCSP single extension (see https://www.common-pki.org/uploads/media/Common-PKI_v2.0.pdf or Annex B to ISO 14533-4 [21]). Identification that OCSP response contains also a status of an expired certificate is based on *ArchiveCutoff* OID (1.3.6.1.5.5.7.48.1.6) OCSP extension (see IETF RFC 6960). OCSP according to Article 7 of the Act No 272/2016 Coll. shall also provide the correct time value in which the certificate was valid (not revoked) in the component *thisUpdate*. If the certificate is not revoked, the existence of the certificate shall be declared by inserting OCSP extension - *CertHash* OCSP single extension to OCSP response. An extension *id-pe-authorityInfoAccess* OID (1.3.6.1.5.5.7.1.1) defined in IETF RFC 5280 section 4.2.2.1 contains the http address on the Online

	Certificate Status Protocol (OCSP) service in the field *id-ad-ocsp* OID (1.3.6.1.5.5.7.48.1). See: https://tools.ietf.org/html/rfc5280#section-4.2.2.1 https://tools.ietf.org/html/rfc6960 An extension CRLDistributionPoints OID (2.5.29.31) is defined in Clause 8.6.2.1 of Rec. ITU-T X.509. According to Article 4 of the Act No 272/2016 Coll., if a signatory (issuer) of a certificate being verified 1) is not a signatory (issuer) of CRL, and 2) is not a signatory (issuer) of a certificate for a signature verification of OCSP response, the signatory (issuer) of a certificate being verified will authorize the CRL signatory or the OCSP response signatory. The issuer of the qualified certificate that is being verified shall request an inclusion of this authorization in the trusted list, in the trust service extension. The authorization in the trusted list contains the identifier of the authorized trust service (the identifier assigned in the trusted list), the URL address of the authorized trust service and the *date from* of the authorization and if known the *date to* of the authorization termination. Clause 7.10 of 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." (See http://ep.nbusr.sk/kca/tsl/tlX509XMLSchemaDocumentation.pdf) }
T1.I, III (j)	Where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing, is: { An extension *QCStatements* OID (1.3.6.1.5.5.7.1.3) shall contain as a minimum the field QcSSCD/QcQSCD OID (0.4.0.1862.1.4). }

5.2.5 SS of Articles 28(2) and 38(2) of Regulation (EU) No 910/2014

Pursuant to Article 28 (2) of the Regulation (EU) No. 910/2014 the requirements according to 5.2.6 and profiles of certificates published on the NSA website are stipulated as non-mandatory additional specific attributeshttps://www.nbusr.sk/en/electronic-signature/approved-formats.1.html.

5.2.6 SS of Articles 28(3) and 38(3) and of recital 58 of Regulation (EU) No 910/2014

In accordance with recital 58 of the Regulation (EU) No 910/2014 when a transaction requires a qualified electronic seal from a legal person, a qualified electronic signature from the authorised representative of the legal person should be equally acceptable.

{ The way suitable for automated processing enabling identification of the authorised representative of the legal person and of the type of authorization is defined by national legislation under a mandate certificate and the type of authorization in Article 8 of the Act No 272/2016 Coll. The mandatary (a natural person) using the mandate certificate proves the authorization:

a) to act for, or on behalf of the mandator (a natural or a legal person),
b) to perform the activities according to special legislation, or
c) to carry out a function according to special legislation.

Identification data pursuant to points of Article 8(1) letter b) of the Act No 272/2016 Coll. shall be included only in cases when it is possible, under respective regulation, to identify the content of these points; thus 4 combinations may occur:

i) Identification data shall be included according to point 1 and also according to point 2.
ii) Identification data shall be included according to point 1 but not according to point 2.
iii) Identification data shall not be included according to point 1 but shall be indicated according to point 2.
iv) Identification data shall be incuded neither according to point 1 nor according to point 2.

In accordance with Article 8(1) letter b) item 1 of the Act No 272/2016 Coll. the identification data of the mandator in accordance with Article 2 of Act No 272/2016 Coll. are stated in such a way, that every filed containing identification data of the mandator in the field of the certificate subject has to begin with the string "MANDANT", so that an exchange in the fields for mandantor and mandator is unambiguously excluded, stating it at minimum in the fields *serialNumber* OID (2.5.4.5) or *organizationIdentifier* OID(2.5.4.97), in accordance with Clause "SS of 28(3) and 38(3) of the Regulation (EU) No 910/2014" and fields according to the lines T1.I(c) and T1.III(c) of the T1 Table. The string „MANDANT" is only stated in the fields according to Article 8 (1) item b) point 1 of Act No 272/2016 Coll. For example field *serialNumber* contains „MANDANT PNOSK-535919999".

In accordance with Article 8(1) point b) of point 2 of the Act No 272/2016 Coll. the identification data of a public authority or a person for whom a mandatar conducts activities under special legislation or performs a function under a special regulation pursuant to Article 2 of the Act No 272/2016 Coll. shall be indicated as a minimum in components *organizationName* OID (2.5.4.10) and *serialNumber* OID (2.5.4.5) or *organizationIdentifier* OID (2.5.4.97) of the certificate subject where *serialNumber* or *organizationIdentifier* contains data according to "NTR" type in compliance with the clause "The Supervision Scheme of Articles 28(3) and 38(3) of the Regulation (EU) No 910/2014" and *organizationName* contains a name registered for the data according to "NTR" type from the components *serialNumber* or *organizationIdentifier*. In ambiguous instances when stating name of the organization in *organizationName*, it is possible to specify in more detail the structural unit by using the component *organizationUnitName* OID (2.5.4.11). It is recommended that the respective components are stated in hierarchical order from component *countryName* OID (2.5.4.11) and component containing the chain „MANDANT" state before the last component *commonName* OID (2.5.4.3).

On the NSA website according to Article 9 of the Act No 272/2016 Coll. there is published a list of registered types of authorizations which shall be included in the certificate extension *certificatePolicies* OID (2.5.29.32) (clauses 8.1.1 and 8.2.2.6 of Rec. ITU-T X.509) as OID mandates. A registered authorization xyz is included as the last OID value (1.3.158.36061701.1.1.xyz) in OID value.

A name (identification) of authorization, published in a list of registered types of authorizations, is recommended to be included in the certificate extension *certificatePolicies* OID (2.5.29.32) along with the authorization value OID (1.3.158.36061701.1.1.xyz) in one or more components of *UserNotice* type in the component *explicitText* as *utf8String* with the maximum length 200 characters at least in the Slovak language.

Optionally, it is possible to indicate number of authorization, to facilitate a non-automated handling of the mandate certificate in the component *commonName* of the certificate subject where it is recommended to separate the textual string "OPRÁVNENIE" or abbreviated "MANDÁT" by a blank space after number of authorization xyz and subsequently by another blank space to separate a textual name of authorization from the list of registered types of authorizations whereas the component *commonName* does not have to be limited to the maximum length 64 characters (example stated in

Annex C Rec. ITU-T X.520|ISO/IEC 9594-6 it is not necessary to maintain, look up the restrictions in Clause 6 Rec. ITU-T X.520|ISO/IEC 9594-6) and at the beginning it can also contain some other text, such as stated e.g. in "SS of Articles 28(3) and 38(3) of Regulation (EU) No 910/2014". }

5.2.7 SS of Article 24(1) of Regulation (EU) No 910/2014

According to Article 24(1) of the Regulation (EU) No 910/2014 when issuing a qualified certificate for a trust service, a qualified trust service provider shall verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued.

{ If a qualified certificate is issued for a key pair whose private key (electronic signature creation data or electronic seal creation data) is stored in a qualified electronic signature/qualified electronic seal creation device (hereinafter referred to as QSCD), the issuer of the qualified certificate shall verify, apart from the requirements according to Article 24(1) of the Regulation (EU) No 910/2014, also the following:

- if the requirements are met according to Article 26 (c) of the Regulation (EU) No 910/2014, requiring verification whether the signatory can, with a high level of confidence, use **under his sole control** the electronic signature creation data; or if the requirements are met according to Article 36(c) of the Regulation (EU) No 910/2014 requiring verification whether the creator of the seal can, **with a high level of confidence under its control** use the data for the electronic seal creation; and
- if the requirements for QSCD according to Annex II of the Regulation (EU) No 910/2014 are met on the basis of the information published according to Article 31(2) of the Regulation (EU) No 910/2014 according to which the Commission, on the basis of the information received, shall establish, publish and maintain a list of certified qualified electronic signature creation devices.

}

The qualified trust service provider shall verify the information referred to in the first subparagraph either directly or relying on a third party in accordance with national law:
a) by the physical presence of the natural person or of an authorised representative of the legal person; or
b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meet the requirements set out in Article 8 of the Regulation (EU) No 910/2014 with regard to the assurance levels ‘substantial’ or ‘high’; or

{ When verifying the identity remotely using electronic identification means, in fact, it is required to use the Extended Access Control mechanism (hereinafter referred to as EAC) according to technical directive of Federal Office for Information Security (hereinafter referred to as BSI) BSI TR-03110. In that case EAC mechanism of mutual authentication shall be used to ensure not only the identity but also the integrity of the data being sent and their encryption in the process of issuing the remote qualified certificate on a card (it includes in particular generating a key pair in the chip, issuing the qualified certificate for the generated public key and storing the qualified certificate on the chip being interconnected with the generated key pair), to ensure communication security, identification and authentication of communicating parties (qualified trust service of qualified certificate creation and verification and a person to whom the qualified certificate is issued and who was identified through the data for EAC where some of them are stored in the chip and some of them are remembered solely by that person)
}
c) by means of a certificate for a qualified electronic signature or qualified electronic seal which is issued in compliance with points (a) or (b); or

{ If a qualified certificate is issued for a qualified electronic signature or seal, it only means a subsequent issuance of a qualified certificate on the same key pair as is defined in the current qualified certificate and the same data as are defined in the current qualified certificate which shall be used to verify the qualified electronic signature or seal, whereas only the validity period and the certificate serial number indicated in Table 1 in lines T1.I, III(e) T1.IV(f) and T1.III(f) T1.IV(g) shall be modified in a new qualified certificate.
}

d) by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.

{ The conformity assessment body, accredited by SNAS, shall publish a list of other identification methods recognised at national level in which the equivalent assurance is confirmed in accordance with Article 8 of the Regulation (EU) No 910/2014 .
}

5.2.8 SS of Article 24(2) point d) of Regulation (EU) No 910/2014

According to Article 24(2) point d) of the Regulation (EU) No 910/2014 a qualified trust service provider before entering into a contractual relationship, shall inform, in a clear and comprehensive manner, any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use.
{ Information on a person's obligations to whom a qualified certificate is issued and who has the sole control over a private key whose public key is included in the qualified certificate being issued to that person, shall contain as a minimum an obligation to use a private key solely for the purposes of the qualified electronic signature/seal creation to avoid the risk of misuse and without delay to ask the certificate issuer for the certificate revocation

1) in case of a loss of the sole control over a private key, and
2) in case of a change of the data indicated in the certificate.

}

5.2.9 SS of Article 24(2) point k) of Regulation (EU) No 910/2014

According to Article 24(2) point k) of the Regulation (EU) No 910/2014 it is required that a qualified trust service provider shall establish and keep updated a certificate database.

{ The certificate database contains as a minimum an issued qualified certificate, and

- if a qualified certificate has been revoked, it contains as a minimum one OCSP response or CRL in which a qualified certificate was revoked and it contains an identification of CRL or OCSP response in which a certificate had been revoked for the first time (for verification of meeting the time interval within 24 hours which is required in Article 24(3) of the Regulation (EU) No 910/2014 by the component *thisUpdate*),
- if a qualified certificate during its validity period has not been revoked but has expired, it contains as a minimum one CRL or OCSP response updated (*thisUpdate*) after the expiration of the qualified certificate.

}

5.2.10 SS of Article 24(3) of Regulation (EU) No 910/2014

According to Article 24(3) of the Regulation (EU) No 910/2014, if a qualified certificate is revoked, a qualified trust service provider shall register such revocation in its certificate database {the revocation time is a value in the first CRL which contains the revocation in components *thisUpdate* and *revocationDate*; the revocation time in OCSP response is the value included in the component *revocationTime*} and publish the revocation status of the certificate in a timely manner,

and in any event within 24 hours after the receipt of the request {the certificate database contains, in the requested interval, a value in the component *thisUpdate* from CRL or OCSP response within which was the first revocation and the revocation time in CRL *revocationDate* or in OCSP response *revocationTime*}. The revocation shall become effective immediately upon its publication {the smallest value of *thisUpdate* in OCSP responses or issued CRLs that contain the revocation}.

{ See Annex E ISO 14533-4 [21],Clause 7.10 of Rec. ITU-T X.509 https://www.itu.int/rec/T-REC-X.509 and section 2.4 IETF RFC 6960 https://tools.ietf.org/html/rfc6960#section-2.4 .
}

5.2.11 Qualified trust service for qualified certificate verification as service within framework of qualified trust service of qualified certificate creation for electronic signature, or for electronic seal, or for website authentication

{ *ServiceTypeIdentifier* URI identification in a trusted list:
As a common service of qualified certificate creation for electronic signature, or for electronic seal, or for website authentication "http://uri.etsi.org/TrstSvc/Svctype/CA/QC" or as a separate service provided under responsibility of qualified certificate creation service for electronic signature, or for electronic seal, or for website authentication
"http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC" and
"http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC". }

5.2.12 SS of Article 24(4) of Regulation (EU) No 910/2014

According to Article 24(4) of the Regulation (EU) No 910/2014 with regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on **the validity status** {the validity time is (if the certificate validity has not been revoked): the time in the component *thisUpdate* in OCSP response obligatorily containing also *CertHash* OCSP single extension, see Annex B ISO 14533-4 [21], http://www.common-pki.org/uploads/media/Common-PKI_v2.0.pdf and the time in the component *thisUpdate* in CRL} or **revocation status** {the revocation time is the time in OCSP component *revocationTime* and the time in CRL component *revocationDate*, see Annex E ISO 14533-4 [21]} of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and also beyond the validity period of the certificate in an automated manner which is reliable, free of charge and efficient.

{ The qualified certificate creation service authorizes the qualified trust service of qualified certificate verification (for issuing OCSP responses and CRL) by including this service in a trusted list within the qualified trust service provider services whose service of "the qualified certificate creation" has created a qualified certificate or authorizes other qualified trust service provider by an extension of a trusted list in the element *URLContentTypeAndAuthorizedServiceList* defined in XSD scheme http://ep.nbusr.sk/kca/tsl/x509types# in the documentation http://ep.nbusr.sk/kca/tsl/tlX509XMLSchemaDocumentation.pdf, whereas the liability for the data correctness bears "the qualified certificate creation" service that has created the qualified certificate.

This scheme does not allow taking over the legal liability for the qualified trust service of "the qualified certificate creation" by other verification service, thus "the qualified trust service of the qualified certificate creation" that has created the certificate is always responsible for the verification service whereas the information on that certificate based on authorization indicated directly or indirectly in the trusted list can be provided under its responsibility by other verification service authorized by that qualified trust service of the qualified certificate creation.

The element *URLContentTypeAndAuthorizedServiceList* defined in XSD scheme http://ep.nbusr.sk/kca/tsl/x509types# is also used for publication of a new address and a type of the qualified trust service of the qualified certificate verification, particularly, when during the qualified

certificate creation such service has not been yet accessible; thus a reference to the service is not included in URL reference in issued qualified certificate what enables its usage in an automated manner using the trusted list.

The qualified trust service of "the qualified certificate verification" based on OCSP protocol being defined in IETF RFC 6960 whose OCSP response meets the requirements stipulated in OCSP profile stated below shall be assessed mutatis mutandis according to requirements for the electronic time stamp service pursuant to ETSI EN 319 421 v1.1.1 "Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps" except the requirement referred to in the first sentence in Clause 7.7.1 of EN 319 421 v1.1.1, where the profile defined in ETSI EN 319 422 is substituted with a profile for OCSP stated below and the point d) of Clause 7.7.1 of EN 319 421 v1.1.1 is applied for a key pair for the OCSP response signing.

5.2.13 SS – Profile of OCSP response

a) Regarding the obligation to establish and keep updated a certificate database according to Article 24(2) point k) of the Regulation (EU) No 910/2014, the certificate database is the source of data provided in OCSP response being defined in IETF RFC 6960. Due to mandatory use of the certificate database, an optional component *nextUpdate* of an object *SingleResponse* is not provided in OCSP response.
b) OCSP response contains a response of *id-pkix-ocsp-basic* type.
c) Date and time specified in the component *producedAt* of an object *ResponseData* of OCSP response being defined in IETF RFC 6960 is with accuracy of 1 second as a minimum to meet mutatis mutandis the requirements of ETSI EN 319 421 v1.1.1.
d) The object *SingleResponse* in the component *singleExtensions* of OCSP response shall contain as a minimum *CertHash* OID (1.3.36.8.3.13) OCSP single extension (see Annex B ISO 14533-4 and http://www.common-pki.org/uploads/media/Common-PKI_v2.0.pdf). The extension *CertHash* contains certificate hash value whose status is in the component *certStatus* of the object *SingleResponse*, whereas the extension *CertHash* is used to convey additional information on assertions made by the responder regarding the status of the certificate, such as a positive statement about the issuance and validity of a certificate of OCSP status *good* provided in the component *certStatus* of OCSP response. The status *good* without the extension *CertHash* does not have to mean that the certificate was valid, for example the certificate before expiration was invalid and a record on revocation after expiration was deleted or a certificate is unknown. If the OCSP extension *CertHash* is provided, the status *good* means that the certificate is valid or was valid in the validity period when the certificate has expired. If the extension *CertHash* is provided and the status of the certificate is *good*, the component *thisUpdate* of an object *SingleResponse* of OCSP response contains the date and time until which the certificate is recorded as valid and the revocation can happen with the later value of the revocation time.
e) If the certificate has been revoked, the object *RevokedInfo* containing a component *revocationTime* with the certificate revocation time is included in the component *certStatus* in the object *SingleResponse*.
f) The algorithm in the object *BasicOCSPResponse* in the component *signature* shall be in the list of algorithms and lengths provided in the valid signature policies published according to Article 11 point m) of the Act No 272/2016 Coll. on the NSA website for the period during which a private key was used.
g) OCSP response in the object *BasicOCSPResponse* in the component *certs* shall contain a certificate for verification of OCSP response signature that shall be included in the trusted list as a service identifier of "verification of qualified certificates" with the qualified status, thus it is verified exclusively according to the trusted list.
h) The object *SingleResponse* in the component *singleExtensions* of OCSP response may contain *ServiceLocator* which in the component *locator* may contain a value from the element 'TLServiceIdentifier' being assigned by the TLSO in the TL (see

http://ep.nbusr.sk/kca/tsl/tlX509XMLSchemaDocumentation.pdf and 5.5.3 ETSI TS 119 612). The value of the component 'TLServiceIdentifier' of that service may be included in the component *locator* as a reference to that service in the form 'TLIxx-y' in the extension *AuthorityInformationAccess* in the component *accessMethod* which contains *id-ad-caIssuers*. The identifier of the trusted list of the certificate issuer service is included in the component *accessLocation* of *GeneralName* type as *direcoryName*, a component of *X520SerialNumber* type. An example: *X520SerialNumber* = "TLISK-4". See http://ep.nbusr.sk/kca/tsl/tsl.xml

Meeting the requirement according to Article 24(4) of the Regulation (EU) No 910/2014 "beyond the validity period of the certificate" from the requirement "This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient" shall be facilitated by a trust infrastructure of the NSA, built as national extensions of trust services according to Article 17(5) of the Regulation (EU) No 910/2014, for certificates issued in accordance with the conditions under national law if the certificate issuer is a trust service of a trust service provider which was granted with the qualified status by the NSA. The service of a qualified certificate issuer, according to Article 6(2) points a) and b) of the Act No 272/2016 Coll. submits to the NSA, at least once a month, issued qualified certificates and in case of the certificate revocation it submits also at least one CRL or OCSP response in which there is indicated the qualified certificate revocation or if the certificate was expired, it submits at least one CRL or OCSP response being updated (*thisUpdate*) after expiration of the qualified certificate, which shall confirm that the certificate has not been revoked during its validity period. The NSA shall provide, based on such information, according to the NSA standard for CRL and OCSP, for unlimited period, information on status of expired qualified certificates to facilitate meeting the requirements according to Article 24(4) of the Regulation (EU) No 910/2014 for the issuers of qualified certificates and shall protect relying parties from potential unavailable manner for long-term verification of the qualified certificate validity.
}

5.2.14 SS of Article 28(5) and Article 38(5) of Regulation (EU) No 910/2014

According to Article 28(5) and Article 38(5) of the Regulation (EU) No 910/2014, subject to the following conditions, Member States may lay down national rules on temporary suspension of a qualified certificate for electronic signature:
(a) if a qualified certificate for electronic signature has been temporarily suspended that certificate shall lose its validity for the period of suspension;
(b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.

{
According to Article 7(2) of the Act No 272/2016 Coll. the certificate must not be revoked with the filled-in component "Reason Code" (see Clause 8.5.3.1 of Rec. ITU-T X.509 https://www.itu.int/rec/T-REC-X.509 and section 5.3.1 of IETF RFC 5280 https://tools.ietf.org/html/rfc5280#section-5.3.1) containing the value *certificateHold* of *CRLReason* type what is considered as the certificate validity suspension according to Article 28(5) and Article 38(5) of the Regulation (EU) No 910/2014.
}

5.3 Qualified validation service for qualified electronic signatures and qualified electronic seals

5.3.1 Identification

{ URI identification in a trusted list *ServiceTypeIdentifier*:

"http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q"

The result of qualified validation service for qualified electronic signatures and seals is a report from the validation process in a textual document in UTF8 coding whose last line contains only a summary result VALID or INVALID and if the time of signing or sealing cannot be proved trustworthily, there shall be indicated the time until which the qualified certificate is recorded as valid (*thisUpdate* of CRL or OCSP response) or if the qualified certificate has been revoked, the revocation time of the qualified certificate validity shall be indicated and if another certificate for the same key pair with the same subject name has been issued, only the signing certificate, to which the reference is protected by signature or seal, shall be verified. See 5.1.3.4.

The first line of the report from the validation process contains the statement "The validation report of the qualified electronic signature or seal according to Articles 32 and 40 of the Regulation (EU) No 910/2014 - SRId [Base64 encoded SRId].".

The SDId is defined in Clause 3.3 in ISO 14533-4 [21] as DER encoded ASN.1 type *MessageImprint*, defined in IETF RFC 3161, containing the hash value of the digital signature (of the DER encoded result of asymmetric function), see note of SDId in Clause 4 in ISO 14533-4.

The resulting report of the validation process contains only the components whose display is required or the components where the following conditions from the validation process were not met together with the indication of the condition in the format:

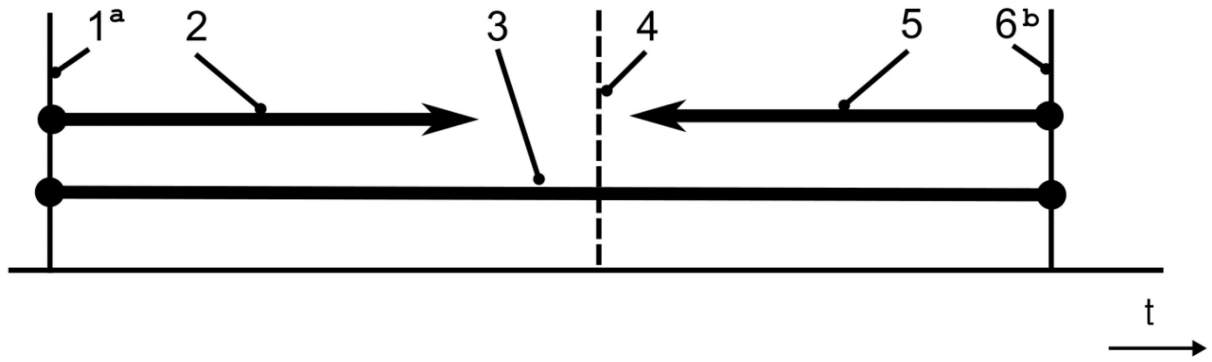
The first one is the character "R", a separator is the character "-", followed by a number and possibly by a point of Article 32 (identical with Article 40) of the Regulation (EU) No 910/2014, possibly followed by Table identification, e.g. T1 and the line identification in the Table if the component refers to it in case of failure to fulfil the requirement in the line of that Table.
For example:
"R-1.d)-T1.I(b) a qualified certificate subject:
Peter - *givenName* OID (2.5.4.42)
Tesla - *surname* OID (2.5.4.4)"

The qualified trust service of validation of qualified electronic signatures and seals can offer a message apart from TXT document in more formats as well, such as in PDF or in structured text of JSON format or in another one. The message is stored e.g. in ZIP signing container of ASiC or PDF type, whose formats are provided in the Annex of the Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced electronic seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance) (hereinafter referred to as Commission Implementing Decision (EU) 2015/1506)
}

5.3.2 SS of Article 32 and Article 40 of Regulation (EU) No 910/2014

The qualified validation service for qualified electronic signatures and seals according to Articles 32 and 40 of the Regulation (EU) No 910/2014 meets the following requirements:
1. The process for the validation of a qualified electronic signature or seal shall confirm the validity of a qualified electronic signature or seal provided that:
   a) the certificate that supports the signature or seal was, at the time of signing or creating the seal, a qualified certificate for electronic signature or electronic seal complying with Annex I or Annex III;

{ R-1.a) The time of signing or creating the seal is the time for which a provable trustworthy evidence on existence and on the time of signing or creating the seal in the past is accessible, for example by using a qualified electronic time stamp (PoE object in accordance with clause 3.12. in ISO 14533-4 [21]) covering the data of the digital signature, otherwise it is the time during which the verification is carried out. See public-key certificate validation 3.5.58 of Rec. ITU-T X.509 | ISO/IEC 9594-8.
The certificate and its components shall be verified according to requirements indicated in the Table T1 in lines marked with "I" for the signature and in lines marked with "III" for the seal.
The time of signing with the qualified electronic signature or creating the qualified electronic seal is indicated as *given-time* in the following text. A procedure of its determination is shown in Figure 2 *given-time* in a Proof of Existence (PoE) of the closed interval in accordance with Annex E in ISO 14533-4 [21].



Key

t time
1 PoE
2 interval in which the signature covers the objects listed in Key 1 covered by the hash value
3 the closed interval in which the signature was created (given-time)
4 the factual time of the signature creation of data (electronic document)
5 interval – the objects listed in Key 6 cover the value of the digital signature covered by the hash value
6 PoE
a The signature was created after the time value stored in
- *thisUpdate* field of the CRL or in the *producedAt* field of the OCSP response covered by the *PoEHashIndex* signed attribute or covered by the PoEAttribute signed attribute,
- the content timestamp (CTS) attribute, or
- the objects (the timestamp, in *thisUpdate* field of the CRL or in *producedAt* field of the OCSP response) of the previous signature covered by the signature or covered by the preservation-integrity-list signed attribute.

b The signature was created before the time value stored in
- the signature timestamp (STS) defined in IETF RFC 3161,
- *producedAt* field of the OCSP response when the OCSP *Nonce* extension contains *MessageImprint* field, defined in IETF RFC 3161, covering the value of the digital signature as the signature timestamp (STS) implemented through OCSP,
- the timestamp of the subsequent signature covering the signature value of the digital signature,
- the PDF subsequent document timestamp, or
- the hash value included in the external objects covering the signature value of the digital signature, e.g. timestamp of preservation service record or the Evidence Record defined in IETF RFC 4998 or IETF RFC 6283 or the attribute PoEAttribute with the *poEObjectRef.type* field with *id-TStOCSP* OID, *id-poe-lti-rfcts* OID, *id-poe-lti-ers* OID or *id-poe-ers* OID.

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

The validation report contains the line "R-1.a) interval of the signature creation time - given-time ([x],[y])", where the time value "x" shall be included only when PoE object of the "x" time value
- is available and
- is trusted,

- has got the highest date and time out of all PoE objects and

the time value "y" shall be included only when PoE object of the "y" time value

- is available and
- PoE is trusted and
- has got the least date and time out of all PoE objects,

otherwise the validation report contains the line "R-1.a) Externally stated time of signing ([z])", where the time value "z" is the time value stated by the relying party, e.g. from other trusted records which cover the signature value (delivery services and others which include qualified electronic time stamp), or time value which is accepted by the relying party).

Given-time with "y" or "z" value shall be used in validation.

}

b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;

{ R-1.b) At the time of beginning of the qualified certificate's period of validity (the component *notBefore* according to Table T1 of line T1.I, III (e)), the issuer certificate, which is used to verify the qualified certificate, shall be included directly in the trusted list according to Article 22 of the Regulation (EU) No 910/2014 (hereinafter referred to as TL) or indirectly via the built certification path ending in TL; the status in TL shall be "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted" (5.5.4 of ETSI TS 119 612 V2.1.1) for the service type "http://uri.etsi.org/TrstSvc/Svctype/CA/QC".

If the issuer is included directly in TL, URI "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC" must not be used, being inserted in TL extension *additionalServiceInformation* (5.5.9.4 of ETSI TS 119 612 V2.1.1) in *ServiceInformationExtension* (5.5.9 of ETSI TS 119 612 V2.1.1) and the rules for the certification path creation and verification according to "Certification path processing procedure" (Clause 10 of Recommendation ITU-T X.509 | ISO/IEC 9594-8) including the TL components defined in the additional XSD scheme http://ep.nbusr.sk/kca/tsl/x509types# shall be met.

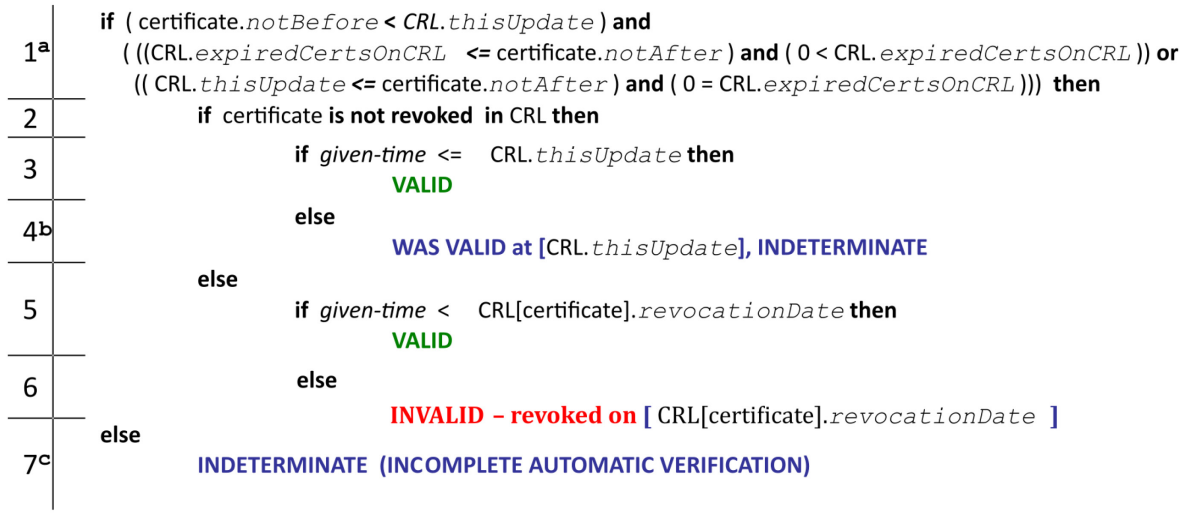
If URI "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC" is used, then it is necessary to follow the rules for the certification path creation and verification according to "Certification path processing procedure" (Clause 10 of Recommendation ITU-T X.509 | ISO/IEC 9594-8), which include the TL components defined in the additional XSD scheme http://ep.nbusr.sk/kca/tsl/x509types#, whereas the certification path shall finish on the certificate of the service included in TL with the status "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted" (5.5.4 of ETSI TS 119 612 V2.1.1).

If TL record in the service regarding the time of signing defines the rules for determining the certificate type (qualifications Extension v ETSI TS 119 612), the certificate type shall be checked (whether it is indeed qualified, made on QSCD and others) and shall regulate the validation process of the field of the found adjusted certificate type.

If the issuer is included directly in TL, the qualified certificate validity shall be verified by CRL or OCSP response obtained from the address indicated in the qualified certificate according to Table 1, line T1.I, III (i) or from the TL component of the certificate issuer *URLContentTypeAndAuthorizedServiceList* defined in the additional XSD scheme. The validation of CRL or OCSP response is either by a certificate included in TL service whose status is "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted" (5.5.4 of ETSI TS 119 612 V2.1.1) at the time of issuance and provable existence of CRL or OCSP response (CRL or OCSP response is issued before the expiration of the service certificate and before the end of the validity period indicated in the TL component *PrivateKeyUsagePeriod* of the service issuing CRL or OCSP response).

If the certificate for the verification of CRL or OCSP response is not directly in TL, it shall be proceeded according to the rules of "Certification path processing procedure" (Clause 10 of Recommendation ITU-T X.509 | ISO/IEC 9594-8) which include the TL components defined in the additional XSD scheme whereas the certification path shall finish on the certificate of the service included in the TL with the status "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted" (5.5.4 ETSI TS 119 612 V2.1.1).

Tables in Figures 3 and 4, where the time of signing or creating the seal is marked as *given-time*, are followed, to determine the certificate validity, in accordance with Annex E in ISO 14533-4 [21].



Key

1 the test of the time interval in which the CRL contains verification data

2 the certificate was not revoked; it is not in CRL

3 the certificate status in CRL is updated after *given-time*

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

5 the certificate was revoked after *given-time*, thus the certificate was valid at the *given-time*

6 the certificate was revoked before *given-time* on CRL[certificate].*revocationDate*

7 the time interval in which the CRL does not contain verification data

a 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. The value of CRL.*expiredCertsOnCRL* is the number representing the content of the extension "Expired certificates on CRL" defined in ITU-T X.509. If "expired certificates on CRL" extension is not present in CRL the value of CRL.*expiredCertsOnCRL* shall be set to 0. The result TRUE of the test "0= CRL.*expiredCertsOnCRL*" allows testing the conditions connected by using "and".

CRL.*thisUpdate* is the time when the certificate status was updated, which means that the certificate status will not be changed to "*revoked*" before the time value *thisUpdate*. The certificate status can be changed only after the time value *thisUpdate*.

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 shall not be changed anymore but the status may be included in CRL.

b The later status is not confirmed.

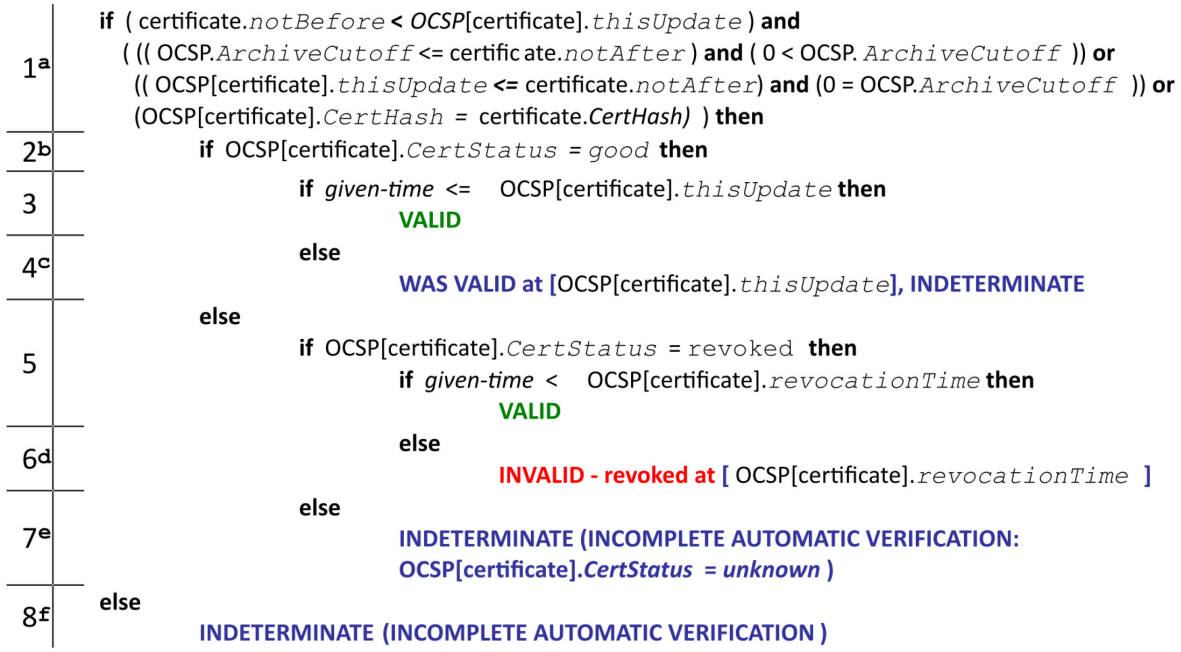
If you need a confirmation of the later status, try to get a newer updated CRL.

CRL is not issued after *given-time*. When the status at *given-time* is necessary, the validation procedure shall wait for a new updated CRL (CRL.*thisUpdate* >= *given-time*).

c It is necessary to obtain CRL or OCSP response, which is updated at a 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. Request CA for CRL that may contain the status of the certificate being verified.

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

Figure 3 — Validation with CRL



Key

1 the test of the time interval in which the OCSP response contains verification data

2 the certificate was not revoked

3 certificate status in OCSP is updated after *given-time*

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

5 the certificate was revoked after *given-time*, thus the certificate was valid at the *given-time*

6 the certificate is revoked in OCSP response before *given-time*

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

8 the time interval in which the OCSP response does not contain verification data

a 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) shall not be changed but the certificate status can be included in CRL (OCSP).

The value of OCSP.*ArchiveCutoff* is the number representing the content of the extension *ArchiveCutoff* defined in IETF RFC 6960. If the extension *ArchiveCutoff* is not present in OCSP response the value of OCSP.*ArchiveCutoff* shall be set to 0. The result TRUE of the test "0=OCSP.*ArchiveCutoff* " allows testing the conditions connected by using "and".

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

OCSP[certificate].*CertHash* is the hash value of the certificate whose status is confirmed by the OCSP response. See Annex B ISO 14533-4 [21]. If this extension is found in the OCSP response, the certificate status is known to 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, which means the certificate status will not be changed to "*revoked*" with the time value before the time value *thisUpdate.* The certificate status may be changed only after the time value *thisUpdate*. The value shall be smaller or equal to OCSP.*producedAt*. OCSP.*producedAt* is the time of the OCSP response issuance.

OCSP[certificate].*nextUpdate* is the auxiliary time when the latest occurrence of the information about the status will be available.

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

c The later status is not confirmed. If you need a confirmation of the later status, try to get a newer updated OCSP response.

OCSP response is not updated (*thisUpdate*) after *given-time*. When the status at *given-time* is necessary, the validation procedure shall wait for a new updated OCSP response (OCSP[certificate].*thisUpdate* >= *given-time*).

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

e OCSP does not know the current status of the certificate validity because OCSP[certificate].*CertStatus* = *unknown*. Verification is possible by other OCSP or CRL.

f 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. Request CA for OCSP response or CRL that can contain the status of the certificate being verified.

OCSP response was updated before the certificate validity interval - the time value Certificate.*notBefore.*

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 (QTS) [*TLIxx-y*] *according to TL. The validity status of the qualified certificate at the time of signing provided by this QTS 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 QTS 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 - QTS],

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 QTS] …
"

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) the signature or seal validation data correspond to the data provided to the relying party;

{ R-1.c) It shall be checked if the data provided to the relying party are in one of the formats of advanced electronic signature/seal defined by Annex of the Commission Implementing Decision (EU) 2015/1506 by means of a list of technical specifications for advanced electronic signatures XML, CMS or PDF and for a signing container in the ASiC format.
The report contains information only in case of discrepancy with the requirements of formats provided in Annex of the Commission Implementing Decision (EU) 2015/1506, e.g. in the form: A reason for discrepancy detached with a dash "-" in brackets "()" marking of object/file name "-" marking of standard "-" hierarchical component name (according to definitions in the standard) detached with "." or with the field "[]" with the index number from 0 where the discrepancy has occured.

Example: R-1.c) Inaccessible certificate of the signatory (signature.p7s)-IETF-RFC5652-*ContentInfo*.*content*.*SignedData*.*signerInfos*[0].*signerInfo*.*signedAttrs*[3].
IETF-RFC5035-*SigningCertificateV2*.*certs*[0].*ESSCertIDv2*.*certHash* =
9E6A332C1100BD704BDDB15B0306D70942826F86AE3AE5E5A20C5CFCFE532EEE
}

d) the unique set of data representing the signatory or the seal creator in the certificate is correctly provided to the relying party;

{ R-1.d) All components from the field *Subject*, from the extension of subject alternative name type and from the extension *subjectDirectoryAttributes* of the qualified certificate shall be displayed, whereas, as a minimum, a name of components (where applicable OID) and the content of components according to Table T1 line T1.I(c), line T1.III(c) and non-mandatory additional specific attributes according to "SD of Articles 28(3) and 38(3) of Regulation (EU) No 910/2014" shall be unambiguously indicated.
}

e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;

{ R-1.e) Conditions according to Table T1 line T1.I(c) shall be checked.
}

f) the electronic signature was created by a qualified electronic signature creation device;

{ R-1.f) Under the condition set out in Table T1 line T1.I, III(j), the report shall contain the result if it is a qualified signature or qualified seal according to QSCD identifier.
}

g) the integrity of the signed data or sealed data has not been compromised;

{ R-1.g) The report contains information in case of failed use of the hash function result including signed or sealed data or in case of gradual use of data from more nested hash functions for the sequence of signed or sealed data whose resulting value shall correspond to the data value according to the result of an asymmetric function whose one of the inputs is the data for signature or seal validation from the qualified certificate according to Table T1 line T1.I, III(d).
}

h) the requirements in Articles 26 or 36 of the Regulation (EU) No 910/2014 were met at the time of signing:

5.3.3 SS of Articles 26 and 36 of Regulation (EU) No 910/2014

Advanced electronic signature or advanced electronic seal shall meet the following requirements:

a) it is uniquely linked to the signatory or it is uniquely linked to the creator of the seal;

{ R-1.h)-a)
CMS advanced electronic signature or seal – is CMS signature that shall contain a signed component *SigningCertificateV2* including in the first component *certs* of *ESSCertIDv2* type defined in IETF RFC 5035 the reference and the hash value of the signatory's certificate. CMS signature shall contain the qualified certificate of the signatory in the component *SignedData.certificates* whereas the algorithms used in CMS signature shall be in the list of algorithms and lengths included in the valid signature policies being published according to Article 11 point m) of the Act No 272/2016 Coll. on the NSA website for the period during which the private key was used.

PDF advanced electronic siganture or seal – is CMS signature of IETF RFC 5652 meeting the rules for CMS from the previous paragraph and is stored in the object Signatory Dictionary where *SubFilter* shall contain the value *ETSI.CAdES.detached*.

XML advanced electronic signature or seal - is XML signature defined in https://www.w3.org/TR/xmldsig-core/ that shall contain in the *SignedInfo* element where is included the *Reference* element containing the reference either to *KeyInfo* including in the *X509Data* element the *X509Certificate* element with the certificate of the signatory or containing the reference to the *SignedProperties* element defined in XSD "http://uri.etsi.org/01903/v1.3.2#" including the nested elements *SignedSignatureProperties, SigningCertificate* and *Cert* element containing the reference and the hash value of the signatory's certificate. XML signature shall contain the qualified certificate of the signatory in the *X509Certificate* element in the *X509Data* element whereas the algorithms used in XML signature shall be in the list of algorithms and lengths included in the valid signature policies being published on the NSA website for the period during which the private key was used.
}

b) it is capable of identifying the signatory or the creator of the seal;

{ R-1.h)-b) The identity shall be displayed according to point R-1.d) in the certificate identified unambiguously in the point R-1.h)-a).
}

c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use **under his sole control** or it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence **under its control**, use for electronic seal creation; and

{ R-1.h)-c) Information on a type of the electronic signature creation data is provided in the qualified certificate in Table T1 line T1.I, III(d). Information on security level of storing and using the electronic signature creation data is provided in the qualified certificate in Table T1 line T1.I, III(j).
}

d) it is linked to the data signed therewith or to which the seal relates in such a way that any subsequent change in the data is detectable.

{ R-1.h)-d) The integrity is secured by used hash algorithm and validated by using the data from the qualified certificate in T1 line T1.I, III(d).
Protection from the data change, incorrect interpretation of the data that is signed or sealed, is ensured either by context wherein the signature is used, for example CMS in PDF document or by additional conditions as are the conditions used for signing a ZIP container that in a ZIP directory contains the data type and its interpretation according to the specification defined for example in the standard for ASiC or the signed attribute or the element with additional information on type shall be used.

Data for the relying party are provided in accordance with clause 5.1.3.

}

2. The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.

{ R-2 A signed or sealed validation report which identifies and describes mutatis mutandis detected security relevant issues is provided to the relying party.
The certificate of signature or seal of the validation report is stored in the TL and its validity is determined by the status of the validation service in TL.

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 QTS 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 SDId of PoE] *issued by QTS* [TLIxx-y] *according to TL*".
The content described in the square brackets "[ ]" identifying QTS [TLIxx-y] is used (or replaced with another QTS identifier) according to rules defined in the report "R-1.b)" for the QTS identification in the report "R-1.b)".
}

5.4 Qualified preservation service for qualified electronic signatures and qualified electronic seals

5.4.1 Identification

{ URI identification in a trusted list *ServiceTypeIdentifier*:
"http://uri.etsi.org/TrstSvc/Svctype/PSES/Q"

5.4.2 SS of Articles 34 and 40 of Regulation (EU) No 910/2014

A qualified preservation service for qualified electronic signatures and seals according to Articles 34 and 40 of the Regulation (EU) No 910/2014 meets the following requirements:
A qualified preservation service for qualified electronic signatures and seals may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature and seal beyond the technological validity period.
A qualified electronic signature (seal) regarding the definition of the qualified electronic signature (seal) referred to in Article 3(12) and (27) of the Regulation (EU) No 910/2014 is an advanced electronic signature (seal) that is created by a qualified electronic signature creation device (QSCD), and which is based on a qualified certificate for electronic signatures (seals).
The format of an advanced electronic signature/seal is defined in the Annex of the Commission Implementing Decision (EU) 2015/1506 by means of a list of technical specifications for advanced electronic signatures CMS, PDF or XML and for a signing container in the ASiC format.

{ The preservation service for expired and revoked certificates related to services with the qualified status that is granted by the NSA, is ensured by the NSA in accordance with the NSA standards in a trust infrastructure pursuant to Article 17(5) of the Regulation (EU) No 910/2014 based on Article 11 items f) and g) of the Act No 272/2016 Coll.
Procedures and technologies capable of extending the trustworthiness of the qualified electronic signature and seal also beyond the technological validity period are based on ensuring the qualified electronic signature and seal integrity.
Qualified trsut service provider in defining its policy proceeds from models indicated in ETSI TS 119 511 - Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques.
The integrity is ensured by the "integrity" signature (seal) defined in the NSA standards (where textual document is replaceable by textual document defined in clause 4.7 in ISO 14533-4 [21] defining the attribute *preservation-integrity-list*) with a qualified electronic time stamp where the certificate for the "integrity" signature (seal) validation is stored as the service identifier in the trusted list. If the integrity is ensured by using equivalent procedures of the integrity signature (seal) which meet the requirements of the Regulation (EU) No 910/2014, the certificate for validation of their usage, for example in the form of signed or sealed receipt on providing "Qualified preservation service of qualified electronic signatures and seals", is stored as the service identifier in the trusted list.
A rule of attaching the qualified electronic time stamp to signature or seal, or using a separate qualified electronic time stamp at the time of validity of the previous qualified electronic time stamp which includes the components of the signature, seal, electronic time stamps and documents that were signed or sealed, shall be met in procedures.
The service ensures only a signature and seal, whereas a signed or sealed document does not have to be accessible for the service (may contain sensitive data) and only a hash value of the signed or sealed document can be provided to the service, and if applicable, more hash values created by different hash functions, for example used later in the long-term preservation.
Procedures defined in the following signature (seal) formats can be used for attaching the qualified electronic time stamps:
ETSI EN 319 122-1 v1.1.1 - CAdES digital signatures with the use of *ats-hash-index-v3* attribute in added attribute *archive-time-stamp-v3* containing the qualified electronic time stamp.
ETSI EN 319 132-1 v1.1.1 - XAdES digital signatures with the use of *ArchiveTimeStamp* element containing the qualified electronic time stamp.
ETSI EN 319 142-1 v1.1.1 - PAdES digital signatures with the use of the object Document Time-stamp containing the qualified electronic time stamp.
PDF documents can according to ISO 32000-2 PDF version 2 proceed pursuant to 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) with the use of the object Document Timestamp which contains qualified electronic time stamp.
}

5.5 Qualified trust service of qualified electronic time stamp creation

5.5.1 Identification

{ URI identification in a trusted list *ServiceTypeIdentifier*:
"http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST" }

5.5.2 SS of Article 42 of Regulation (EU) No 910/2014

A qualified electronic time stamp of the qualified trust service according to Article 42 of the Regulation (EU) No 910/2014 shall meet the following requirements:

a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;

{ Implementation is one of two procedures where the component *MessageImprint* represents the data bound to the time value. The *MessageImprint* type is defined in IETF RFC 3161 - Time-Stamp Protocol (TSP).

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

1. procedure (an electronic time stamp **implemented by internal CMS signature** of the electronic document of *TSTInfo* type defined in IETF RFC 3161), where the component *MessageImprint* represents the data (time-stamped) bound in the object of *TSTInfo* type defined in IETF RFC 3161 to the date and time included in the component *genTime* of an object *TSTInfo*. The object *TSTInfo* is signed by CMS advanced electronic signature defined in IETF RFC 5652 that meets the requirements according to IETF RFC 3161 and IETF RFC 5816, requiring the use of the signed component *SigningCertificateV2* containing *ESSCertIDv2* which is defined in IETF RFC 5035. CMS advanced electronic signature of the time stamp shall contain the certificate for its verification which is included also in the trusted list of the qualified service for the qualified electronic time stamp creation. The service of the qualified electronic time stamp meets mutatis mutandis the requirements of ETSI EN 319 421 v1.1.1: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps.
2. procedure (an electronic time stamp **implemented over OCSP protocol** defined in IETF RFC 6960) is defined only for the electronic time stamp from the digital signature in accordance with Annex C in ISO 14533-4 [21] (from an advanced electronic signature or from an advanced electronic seal). The component *MessageImprint* represents the data (time-stamped) bound to the date and time where the component *hashedMessage* contains the hash value from DER encoded digital signature. For example in CMS signature the hash value stored in the component *MessageImprint* is computed from the component *SignerInfo.signature* of *OCTET STRING* type (excluding the tag and length of *OCTET STRING*) and in XML signature the component *MessageImprint* contains the hash value computed from the content of <SignatureValue> element without XML tag after decoding of Base64 encoding. The component *MessageImprint* is stored in OCSP extension *Nonce* defined in IETF RFC 6960 (Online Certificate Status Protocol) for OCSP request and for OCSP response. OCSP response binds *MessageImprint* stored in OCSP extension *Nonce* to the date and time indicated in the component *producedAt* of OCSP response defined in IETF RFC 6960. OCSP response in the object *BasicOCSPResponse* shall contain the certificate for validation of OCSP response signature, that certificate is also included under the qualified trust service in the trusted list. Certificate for signature validation of OCSP response may contain the certificate extension *certificatePolicies* OID (2.5.29.32) (Clauses 8.1.1 and 8.2.2.6 of Rec. ITU-T X.509) with the certificate policy OID 1.3.158.36061701.1.3.2 published

on the NSA website that shall facilitate the applications verifying the electronic time stamps to identify the use of OCSP response object also as an object of the electronic time stamp. The applications verifying the electronic time stamps identify the use of the electronic time stamp over OCSP by successful decoding of ASN.1 of *MessageImprint* type from the data stored in OCSP extension *Nonce*. The qualified electronic time stamp service meets mutatis mutandis the requirements of ETSI EN 319 421 v1.1.1 (Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps), except the requirement provided in the first sentence of Clause 7.7.1 of EN 319 421 v.1.1.1 where the profile defined in ETSI EN 319 422 is replaced by a profile defined for OCSP service "Qualified trust service for qualified certificate verification" and the point d) of Clause 7.7.1 of EN 319 421 v1.1.1 is applied for a key pair for signing the OCSP response.

}

b) it is based on an accurate time source linked to Coordinated Universal Time; and

{ time accuracy of 1 second shall be the minimum
}

c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.

{ Currently are used only advanced electronic signatures based on ASN.1 language of CMS advanced electronic signature type defined in IETF RFC 5652 from the *TSTInfo* object defined in IETF RFC 3161 and an advanced electronic signature of the *ResponseData* object from *BasicOCSPResponse* whose type in ASN.1 language is defined in IETF RFC 6960.
}

5.6 Qualified electronic registered delivery services

5.6.1 Identification

{ URI identification in a trusted list *ServiceTypeIdentifier*:
"http://uri.etsi.org/TrstSvc/Svctype/EDS/Q" and "http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q" }

5.6.2 SS of Article 44 of Regulation (EU) No 910/2014

Qualified provider of qualified electronic registered delivery services shall have documentation elaborated, stemming from ETSI EN 319521 - Policy and security requirements for Electronic Registered Delivery Service Providers.
Available technical solution, besides others, like Electronic Registered Electronic Mail Service, is implementation based on ASiC container. ASiC container is, for sending and receiving data, possible to transfer on various memory media or through any protocols, supported and stated by the provider in accordance with Article 24(2) point d) of Regulation (EU) No 910/2014.
ASiC container enables to save into files the data for the purpose of sending and receiving and to add files containing identification of the sender and identification of the adressee, while ASiC enables ensuring that the sending and receiving of the data is provided by several advanced electronic signatures or advanced electronic seals of the qualified trust service provider in such a way, that:

- the data files for the purpose of sending and files containing identification of the sender are before signing / sealing by the service provider secured by the qualified electronic time stamp of the content, which is subsequently signed or sealed together with the abovementioned files and
- the data files for the purpose of receiving (which are also data for sending) and files containing identification of the sender and files containing identification of the addressee are

before signing / sealing by the service provider secured by the qualified electronic time stamp of the content, which is subsequently signed or sealed together with the abovementioned files.

Requirements for qualified electronic registered delivery services
1. Qualified electronic registered delivery services shall meet the following requirements:
(a) they are provided by one or more qualified trust service provider(s);
{ Each further provider shall add into ASiC his two signatures/seals (for all files in the main ASiC directory) in such a way, as if the data had been sent by the previous provider or as if they had been delivered to the subsequent provider, thus ensuring a uniform procedure even in several providers delivering the data one after another. }

b) they ensure with a high level of credibility the identification of the sender;

{ Provider of delivery services administers documentation about the procedures and identification results and about mechanism of sender authentication, through which the natural or legal person uses the electronic identification means to confirm their identity as is stated in section 2.3 of the Annex to Commission Implementing Decision No 2015/1502, in accordance with Article 8(3)(c) of Regulation (EU) No 910/2014. If the data for sending are on a physical carrier, in identification it is necessary to proceed in accordance with Article 24(1) point a) of Regulation (EU) No 910/2014.
Provider of delivery services shall store the data identifying the sender into a JSON file with file name beginning with word chain "sending-", followed by characters permitted in file name from component *commonName* OID (2.5.4.3) of the delivery services certificate subject, word chain "-SKID-" followed by "base64url" (IETF RFC 4648) encoded value from the extension Subject Key Identifier according to IETF RFC 5280, section 4.2.1.2, character "-" followed by a growing number from 0, ensuring unambiguity of the file name and extension of the file name ".json".
Identification data of the sender, stored in the file, contain at least attributes in accordance with the Annex of the Commission Implementing Decision No 2015/1501 - "currentFamilyName", "currentFirstName", "dateOfBirth", "uniqueIdentifier", the identifier is constructed by the sending Member State - 2 characters containing the country code according to ISO 3166 "idCountryCode", "firstNameAndFamilyNameAtBirth", "placeOfBirth", "currentAddress", "gender", "currentLegalName", "VATRegistrationNumber", "taxReferenceNumber", "idArticle3(1)OfDirective2009-101-EC", "LegalEntityIdentifierCIR(EU)No1247-2012", "EORI-CIR(EU)No1352-2013", "exciseNumberArticle2(12)CR(EC)No389-2012". If the means of electronic identification issued in the framework of reported scheme of electronic identification of national scheme does not fulfil the requirement stated for the assurance level "High", the document shall include assurance level "assuranceLevelAuthenticationMechanism" with the value "Low" or "Substantial" in accordance with Article 8 (1) of Regulation (EU) No. 910/2014. }

c) they ensure the identification of the addressee before the delivery of the data;
{ Provider of the delivery services administers documentation on procedures and identification results and about mechanism of sender authentication, through which the natural or legal person uses the electronic identification means to confirm their identity as is stated in section 2.3 of the Annex to Commission Implementing Decision No 2015/1502, in accordance with Article 8(3)(c) of Regulation (EU) No 910/2014.
Provider of delivery services shall store the data identifying the addressee into a JSON file with file name beginning with word chain "receiving-", followed by characters permitted in file name from component *commonName* OID (2.5.4.3) of the delivery services certificate subject, word chain "-SKID-" followed by "base64url" (IETF RFC 4648) encoded value from the extension Subject Key Identifier according to IETF RFC 5280, section 4.2.1.2, character "-" followed by a growing number from 0, ensuring unambiguity of the file name and extension of the file name ".json".
Identification data of the addressee, stored in the file, contain at least attributes as are used in the preceding point b).}

d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider so as to prevent the possibility of the data being changed undetectably;
{ From all the data in the root directory of ASiC shall be made an AdES, while AdES shall contain qualified electronic time stamp of the content.}

e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;
{The data is stored in files in ASiC, which ensures its standard handling and identification of their type and interpretation. The file, in the ASiC root directory, in the process of being signed or sealed must not be altered – neither transformation nor canonicalization function must be applied to the ASiC file. }
f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.
{ The requirement is fulfilled because AdES in ASiC shall contain qualified electronic time stamp of the content of all the files in the root directory of ASiC, subsequently secured by AdES of the provider of the delivery services.}
In the event of the data being transferred between two or more qualified trust service providers, the requirements in points (a) to (f) shall apply to all the qualified trust service providers.
{ The requirement is fulfilled as every qualified trust service provider is stated in ASiC in such a way, as if the previous or subsequent trust service provider was from the point of view of the actual provider actually the sender or the addressee. }

Annex A **(informative) Bibliography**

Basic legislation of the Slovak Republic and EU on trust services:
http://www.nbu.gov.sk/en/authority/legislation/index.html

NSA standards:
http://www.nbu.gov.sk/en/trust-services/standards/index.html

NSA schemes:
http://www.nbu.gov.sk/en/trust-services/supervision-schemes/index.html

Annex B **History**

Version	**Date of issuing**	**Note**	**Editor**
Version 1.0	20.9.2016	First issue	Peter Rybár, NSA
Version 1.1 5767/2016/IBEP/OA-016	30.11.2016	Unification of procedures with SNAS	Peter Rybár, NSA Lenka Gondová, SNAS
Version 1.2 1353/2017/IBEP/OA-001	18.1.2017	Unified pattern of documents, specifications	Peter Rybár, NSA
Version 1.3 1353/2017/IBEP/OA-006	3.3.2017	Clarification of 5.2.5 and 5.3.1	Peter Rybár, NSA
Version 1.4 05968/2019/ORD-001	1.7.2019 (enter into force on 1.8.2019)	Moving of the requirements from 5.3 to 5.1.3. Clarification of 5.2.3, 5.2.6, 5.3, 5.4, 5.6 and supplementing of ISO and ETSI standards.	Peter Rybár, NSA