Version 1.3

Supervision Scheme of Qualified Trust Services defined by Supervisory Body

3 March 2017

This English version of the Slovak document No. 1353/2017/IBEP/OA-006 is for reference purposes only. In case of conflict between the English translation and the original Slovak version, the Slovak version shall prevail and supersedes 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 judgement.

Methodology Division | Cyber Security Department
Budatínska 30 | 851 06 Bratislava | Slovak Republic
tel.: +421 2 6869 1111 | fax: +421 2 6869 1700
e-mail: podatelna@nbu.gov.sk | http://www.nbu.gov.sk/

Content

1 Introduction **4**

2 Scope **4**

3 References **6**

4 Abbreviations **8**

5 Mapping of requirements **10**

5.1 Common requirements for qualified trust service provider 10
5.1.1 SS of Article 27(5) and Article 37(5) of Regulation (EU) No 910/2014 10
5.1.2 SS of Articles 19 and 24 of Regulation (EU) No 910/2014 10
5.2 Qualified trust service of qualified certificate creation and verification for electronic signature, electronic seal and website authentication 11
5.2.1 SS of Articles 17(5), 24, 28, 38 and Article 45 of Regulation (EU) No 910/2014 11
5.2.2 SS of Articles 28(3) and 38(3) of Regulation (EU) No 910/2014 11
5.2.3 SS of Annexes I, III and IV of Regulation (EU) No 910/2014 13
Table T1 – SS of Annexes I, III and IV of Regulation (EU) No 910/2014 13
5.2.4 SS of Articles 28(2) and 38(2) of Regulation (EU) No 910/2014 17
5.2.5 SS of Articles 28(3) and 38(3) and of recital 58 of Regulation (EU) No 910/2014 17
5.2.6 SS of Article 24(1) of Regulation (EU) No 910/2014 18
5.2.7 SS of Article 24(2) point d) of Regulation (EU) No 910/2014 19
5.2.8 SS of Article 24(2) point k) of Regulation (EU) No 910/2014 19
5.2.9 SS of Article 24(3) of Regulation (EU) No 910/2014 20
5.2.10 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 20
5.2.11 SS of Article 24(4) of Regulation (EU) No 910/2014 20
5.2.12 SS – Profile of OCSP response 21
5.2.13 SS of Article 28(5) and Article 38(5) of Regulation (EU) No 910/2014 22
5.3 Qualified validation service for qualified electronic signatures and qualified electronic seals 23
5.3.1 SS of Article 32 and Article 40 of Regulation (EU) No 910/2014 23
5.3.2 SS of Articles 26 and 36 of Regulation (EU) No 910/2014 30
5.4 Qualified preservation service for qualified electronic signatures and qualified electronic seals 32
5.4.1 SS of Articles 34 and 40 of Regulation (EU) No 910/2014 32
5.5 Qualified trust service for qualified electronic time stamp creation 33
5.5.1 SS of Article 42 of Regulation (EU) No 910/2014 33
5.6 Qualified electronic registered delivery services 34
5.6.1 SS of Article 44 of Regulation (EU) No 910/2014 34

Annex A (informative) Bibliography **35**

Annex B History **36**

1 Introduction

A supervision scheme of qualified trust services defined by a 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 that 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: A text of the scheme shall be kept 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 provider 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 (act on trust services) [4], Regulation (EU) No 910/2014 and in the accreditation scheme of the Slovak National Accreditation Service (hereinafter referred to as the 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 on the certification scheme on the SNAS website.

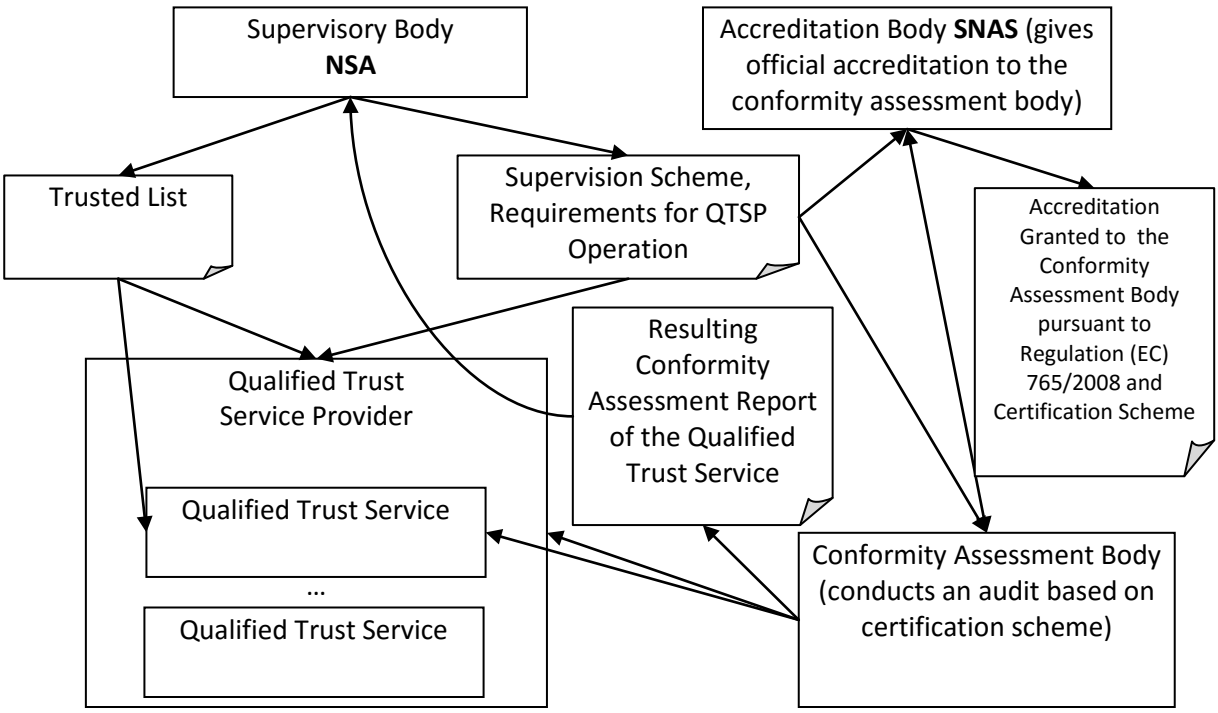


Figure 1 – Supervision Scheme

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 for electronic signature (see Clause 5.2)
2. Qualified trust service of qualified certificate creation and verification for electronic seal (see Clause 5.2)
3. Qualified trust service of qualified certificate creation and verification for website authentication (see Clause 5.2)
4. Qualified validation service for qalified electronic signatures (see Clause 5.3)
5. Qualified validation service for qalified electronic seals (see Clause 5.3)
6. Qualified preservation service for qalified electronic signatures (see Clause 5.4)
7. Qualified preservation service for qalified 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 internal market and on the amendment and supplementing of certain acts (act on trust services)

[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://ep.nbusr.sk/kca/tsl/tlX509XMLSchemaDocumentation.pdf)

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

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

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

[13] Supervision Scheme – of the supervisory body – the NSA
(see http://ep.nbusr.sk/kca/tsl/SchemaDohladu.pdf)

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

[15] ETSI TS 119 612 Trusted Lists

[16] RFC 5652 Cryptographic Message Syntax 9-2009

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

[18] 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

4 Abbreviations

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

Note 1: The structure of the DRId it the same as is defined for SRId and contains the hash algorithm identifier with parameters and the hash value of the electronic document.

CMS	Cryptographic Message Syntax
CP	Certificate Policy
NSA RCA CP	Certificate Policy of the NSA Root Certification Authority See 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 see 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 Supervisory Body

SNAS	Slovak National Accreditation Service
SRId	Signature Relative Identifier

Note 2: The content of the SRId is DER encoded ASN.1 type *MessageImprint*, defined in IETF RFC 3161, containing the hash value covering the value of the digital signature (of the DER encoded result of the asymmetric function). If the SRId is used for the signature time-stamp (STS) over OCSP implementation, the SRId shall be included in the *nonce* OCSP field (IETF RFC 6960) as the data bound to the time value included in the *producedAt* field of the OCSP response.

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 provider

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) 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 apply Act No 275/2006 Coll. on information systems in public administration and on the amendment and supplementing of certain acts as amended shall proceed also in accordance with 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], when creating and verifying the signature/seal.
}

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 http://www.enisa.europa.eu/topics/trust-srevices/guidelines. Common requirements for operation of qualified trust service providers (hereinafter referred to as QTSP) defined by a 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 a 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 objects, personnel, software and technical equipment of qualified trust services of qualified trust service providers and mutatis mutandis of conformity assessment bodies. 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].
}

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

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

}

5.2.1 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 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 above mentioned statement when requiring the data change in the trusted list, for example when requiring the authorization or the authorization change for issuing OCSP responses (partial qualified certificate verification qualified trust service of qualified certificate creation qualified trust service) 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://ep.nbusr.sk/kca/tsl/tlX509XMLSchemaDocumentation.pdf.
}

5.2.2 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 hamper 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 number for Slovak citizens and foreigners who were assigned a personal number pursuant to Act No 301/1995 Coll. on a personal number
4. "NTR" for identification based on the main registration number of the organisation

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

3 characters:

1. "JUS" giving precision for "IDC" for identification based on identity card number of judges and on other cards in administration and in the format according to rules at http://www.justice.gov.sk/, for example "IDCSK-JUS-123123",

2. "NSA" giving precision for "IDC" for identification based on identity card number of the NSA officers and on other cards in administration and in the format according to rules at http://www.nbu.gov.sk/,

3. "POL" giving precision for "IDC" for identification based on identity card number of the police and on other cards in administration and in the format according to rules at http://www.minv.sk/,

4. "MIL" giving precision for "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 rules at http://www.mod.gov.sk/.

1 character "-" (ASCII 0x2D)
Characters of data whose type 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*.
If the component *serialNumber* contains other types of data than those defined above, they must not be used if the first three characters were 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 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* with the maximum length 64 characters, 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.

}

5.2.3 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 certificate:
	{
	1) an 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 who issues 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 who 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 a 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 a 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 a 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 byte 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(1), 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 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 on an expired certificate, what 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(1), 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). Identification that OCSP response contains also a status on 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 a 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. This authorization is required to be included in the trusted list, in the trust service extension, *by an issuer of a qualified certificate being verified*. 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). }

5.2.4 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 profiles of certificates published on the NSA website are stipulated as non-mandatory additional specific attributes.

5.2.5 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 specific rules, or
c) to carry out a function according to specific rules.

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) point 2 of the Act No 272/2016 Coll. the identification data of a public authority or a person for whom a mandatory conducts activities under a special regulation 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*.

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.
One certificate may contain one or more authorizations as separate OID values (1.3.158.36061701.1.1.xyz) in the certificate extension *certificatePolicies* OID (2.5.29.32).
A name 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 Slovak language.

Optionally, it is possible to indicate a 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 a number of authorization xyz by a blank space after a textual string "OPRÁVNENIE" or "MANDÁT" and subsequently to separate a textual name of authorization from the list of registered types of authorizations by a blank space whereas the component *commonName* has got the maximum length 64 characters and at the beginning it can also contain the other text, such as stated in Supervision Scheme Clause "SS of Articles 28(3) and 38(3) of Regulation (EU) No 910/2014". If one certificate is issued for more authorizations, the procedure shall be repeated, if the maximum length allows it. If the text in *commonName* exceeds the length limit, a text of the name of authorization shall not be included, only a string "OPRÁVNENIE" or "MANDÁT", a blank space and a number of authorization xyz shall be provided.
}

5.2.6 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 according to Article 26 point 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, are met; or if the requirements 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 a communication security, identification and authentication of communicating parties (a qualified trust service of a 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.
}

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

}

5.2.8 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

1. 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 was 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*),
2. 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.

}

5.2.9 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 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 .
}

5.2.10 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". }

5.2.11 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** { the validity time is (if the revocation time of the certificate is not stated): the time in the component *thisUpdate* in OCSP response obligatorily containing also *CertHash* OCSP single extension, see 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* } 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.

An 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 was not accessible yet; 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.

5.2.12 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) An 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 http://www.common-pki.org/uploads/media/Common-PKI_v2.0.pdf). An extension *CertHash* contains a hash value of a certificate whose status is in the component *certStatus* of an 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 is revoked, an object *RevokedInfo* containing a component *revocationTime* with the certificate revocation time is included in the component *certStatus* in the object *SingleResponse*.
f) An algorithm in the object *BasicOCSPResponse* in the component *signature* shall be in the list of algorithms and lengths provided in valid signature policies being published on the NSA website for the period during which a private key was used, published according to Article 11(1) point m) of the Act No 272/2016 Coll.

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.
h) An 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, what 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.
}

5.2.13 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

{ 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 was revoked, the revocation time of the qualified certificate validity shall be indicated. If the other certificate for the same key pair with the same subject name has been issued, only the signing certificate, to which the reference (the reference with the hash value of the certificate) is protected by signature or seal, shall be verified.

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 SRId is the DER encoded ASN.1 type *MessageImprint*, defined in IETF RFC 3161, containing the hash value which covers the value of the digital signature (of the DER encoded result of the asymmetric function), see note of SRId in Clause 4.

The resulting report of the validation process contains only the components whose display is required or the components at which 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)"

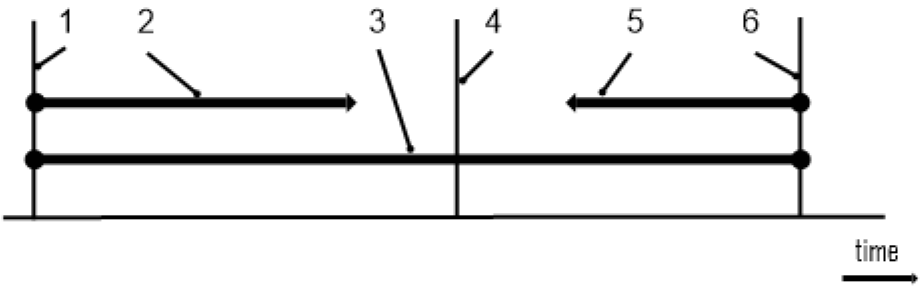
The qualified validation service for qualified electronic signatures and seals can offer a message apart from TXT document in more formats as well, such as in PDF or in structured text of JSON format or in another one. The message is stored e.g. in ZIP signing container of ASiC or PDF type, whose formats 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 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)
}

5.3.1 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 covering the data of the digital signature, otherwise it is the time during which the verification is carried out.
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 or creating the seal with the qualified certificate for electronic signature or electronic seal is indicated as *control-time* in the following text. A procedure of its determination is shown in Figure 2 *control-time* in a Proof of Existence (PoE) of the closed interval.



Key

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

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

3 The closed interval in which the signature was created.

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

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

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

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

The validation report contains the line "R-1.a) interval of the signature creation time - control-time ([x],[y])", where the time value "x" sahll by included only when PoE of the "x" time valu is available and is trusted and the time value "y" sahll by included only when PoE of the "y" time valu is available and is trusted.
}

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

{ R-1.b) In 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, there must not be used URI "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC", that is 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 is used "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC", then it is required 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 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 verification 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) in 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 *control-time*, are followed, to determine the certificate validity.

alebo vyhotovenia pečate je označený ako *control-time*.

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

Key

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

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

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

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

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

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

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

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

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

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

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

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

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

Figure 3 — Validation with CRL

1 **if** (certificate.*notBefore* **<** *OCSP*[certificate].*thisUpdate*) **and**
(((OCSP.*ArchiveCutoff* <= certificate.*notAfter*) **and** (0 < OCSP.*ArchiveCutoff*)) **or**
((OCSP[certificate].*thisUpdate* **<=** certificate.*notAfter*) **and** (0 = OCSP.*ArchiveCutoff*)) **or**
(OCSP[certificate].*CertHash* = certificate.*CertHash)*) **then**

2 **if** OCSP[certificate].*CertStatus* = *good* **then**

3 **if** *control-time* <= OCSP[certificate].*thisUpdate* **then**

VALID

4 **else**

WAS VALID at [OCSP[certificate].*thisUpdate*]**, the later status is not confirmed. If you need a confirmation of the later status, try to get a newer updated OCSP response. INDETERMINATE**

5 **else**

if OCSP[certificate].*CertStatus* = revoked **then**

if *control-time* < OCSP[certificate].*revocationTime* **then**

VALID

6 **else**

INVALID - revoked at [OCSP[certificate].*revocationTime*]

7 **else**

INDETERMINATE (INCOMPLETE AUTOMATIC VALIDATION: OCSP does not know the current status of the certificate validity because OCSP[certificate].*CertStatus* = *unknown* Validation is possible by other OCSP or CRL.)

8 **else**

INDETERMINATE (INCOMPLETE AUTOMATIC VALIDATION: a request to CA for OCSP response or CRL that can contain the status of the certificate being verified.)

Key

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

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

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

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

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

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

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

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

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

2 The certificate was not revoked.

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

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

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

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

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

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

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

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

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

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

Figure 4 — Validation with OCSP response

The validation report "R-1.b)" contains at least 2 sentences, where the content described in the square brackets "[ ]" is replaced with the particular value.
The sentences of the report are the following:
"

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

If the TL unique and precise service identifier 'TLIxx-y' in "TLServiceIdentifier" element of the digital service identifier "ServiceDigitalIdentity", "DigitalId" elements is not included in the TL, then the validation report contains in the sentence instead of [TLIxx-y] identification the identification of the issuer of the qualified certificate indicated in TL. This case is problematic because the identification of the issuer of the qualified certificate indicated in TL is based on many optional components and it is up to the validation application which component will be used to create the unique representation of the QTSP which is the issuer of the qualified certificate in TL.
Instead of [TLIxx-y] the following is included in the report:
"

1. Hash algorithm [OID of the hash algorithm in a dot notation and the algorithm name],
2. Hash of the issuer certificate [the hash value of the qualified certificate issuer DER X.509 *Certificate* - the certificate included in TL],
3. Hash of the certificate issuer name [the hash value of the subject name (*DistinguishedName*) of the certificate included in TL – as defined for *CertID. issuerNameHash* IETF RFC 6960],
4. Hash of the certificate issuer Public Key [the hash value of *SubjectPublicKeyInfo* of the certificate included in TL – as defined for *CertID. issuerKeyHash* IETF RFC 6960],
5. Certificate issuer serial number [base64 encoded *TBSCertificate*.*serialNumber* of the certificate included in TL http://www.itu.int/itu-t/recommendations/rec.aspx?rec=X.509],
6. Key identifier of the certificate issuer [base64 encoded hash value composed of the SHA-1 hash of the value of the BIT STRING *subjectPublicKey* (excluding the tag, length, and number of unused bits) of the *SubjectPublicKeyInfo* of the certificate included in TL],
7. The certificate issuer name [LDAP name (IETF RFC 4514) of the ITU-T X.501 *DistinguishedName* of the certificate subject name included in TL http://www.itu.int/itu-t/recommendations/rec.aspx?rec=X.501],
8. Service Type Identifier [URI identification in a trusted list *ServiceTypeIdentifier* of the certificate issuer included in TL - QTSP],
9. [Any other TL values of TL elements of the qualified certificate issuer included in TL which must be included in the report to have a unique identification of the QTSP] …
"

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

}

c) 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 dispalyed, 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 encapsulated hash functions for the sequence of signed or sealed data whose resulting value shall corespond 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 provided for in Articles 26 or 36 of the Regulation (EU) No 910/2014 were met at the time of signing:

5.3.2 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 to 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(1) 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 encapsulated 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 verified 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 a 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.

In CMS signature, if there is an ambiguous specification of visualization according to OID *id-aa-contentType*, also *id-aa-contentHint* with *contentDescription* containing MIME *Content-Type* shall be used.

MIME ***Content-Type*** field in one line in CAdES *contentDescription* field in *contentHint* attribute.

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

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

In XML signature, if there is an ambiguous specification of visualization according to *MimeType* element in the *DataObjectFormat* element, the *Description* element containing MIME *Content-Type* shall be used.

MIME ***Content-Type*** field in one line in XAdES *Description* element in *DataObjectFormat* element.

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

MIME ***MimeType*** in XAdES *MimeType* element in *DataObjectFormat* element.

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

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

In ASiC protection of the format of the document being signed is assured by:

MIME ***Content-Type*** field containing only MIME type and parameters in the component "file comment" of "4.3.12 Central directory structure" in signed ZIP file.

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

}

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 end of the validation report "R-2" contains the sentence of the time value to which the validation was performed. It can be the current time or the time value from the PoE. When the PoE is used, the PoE is identified according to SRId value of the PoE digital signature and also the issuer of the PoE is provided

according to the QTSP identifier included in TL. The content described in the square brackets "[ ]" is replaced with the particular value.

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

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

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

5.4.1 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).
A 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 XML, CMS or PDF 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 under Article 11(1) points 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. The integrity is ensured by the "integrity" signature (seal) defined in the NSA standards with the qualified electronic time stamp where the certificate for the "integrity" signature (seal) verification is included as the service identifier in the digital service identifier "ServiceDigitalIdentity", "DigitalId" elements in a 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 verification of their usage, for example in the form of signed or sealed receipt on providing "Qualified preservation service for qualified electronic signatures and seals", is included as the service identifier in the trusted list.
A rule of attaching the qualified electronic time stamp to signature or seal, or using as a separate qualified electronic time stamp in 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 for 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 the qualified electronic time stamp.
}

5.5 Qualified trust service for qualified electronic time stamp creation

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

5.5.1 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 (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 calculated 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 verification of OCSP response signature, that certificate is also included in the trusted list of the qualified trust service. The certificate for validation of OCSP response signature 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), in addition to 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 as a 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 there 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

{ 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" }

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

It is foreseeable that the Commission shall release implementing acts for that service type in the near future.

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 issuing	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