MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Document specifying requirements for qualified trust service providers and for qualified services provided by them [DKP]

The history of the document:

Version	*Created on*	*Author*	*Note*	*Status*
1	25.07.2016	FB	The first draft	Draft
2	1.8.2016	FB, EG team	Responses to comments	For publication
2	12.3.2018	FB	Only a formal modification – correction of typing error in the title of Chapter 4	For publication
3	22.01.2020	FB	Changes reflecting new versions of norms and standards, specifications of applicable requirements of ČSN EN ISO/IEC 17021-1 and ČSN ISO/IEC 27006, addition of a part focused on risk management and other parts related to received comments.	For publication

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Content

1. Purpose of the document

The aim of the document is to specify the requirements for accreditation of conformity assessment bodies, (later only „CAB“) by national accreditation body (later only „NAB“). The document contains the list of applicable requirements of eIDAS (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 Directive 1999/93/EC) for qualified trust service providers and for qualified trust services provided by them, references to relevant parts of technical norms, standards and specifications. By meeting these requirements, it is possible to demonstrate conformity with requirements of eIDAS regulation. This document contain also a list of technical norms, standards and specifications related to a particular area. It ought to be mentioned, that some of the requirements of the regulation are not covered by existing technical norms, standards and specifications. Taking into consideration that the regulation targets at technological neutrality, it is not possible to set out the mandatory list of norms, by their fulfilling (only of them) the trust service provider could demonstrate meeting of requirements laid down by eIDAS Regulation.

The requirements are based on **ČSN EN ISO/IEC 17065** standard **(CONFORMITY ASSESSMENT -- REQUIREMENTS FOR BODIES CERTIFYING PRODUCTS, PROCESSES AND SERVICES)** as a general framework laying down requirements for for bodies certifying products, processes and services. General standard ČSN EN **ISO/IEC 17065** requires CAB to fulfil:

- applicable requirements of **ČSN EN ISO/IEC 17021-1 (CONFORMITY ASSESSMENT -- REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF MANAGEMENT SYSTEMS)**
- applicable requirements of **ČSN ISO/IEC 27006 (INFORMATION TECHNOLOGY - SECURITY TECHNIQUES - REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF INFORMATION SECURITY MANAGEMENT SYSTEMS)**

Due to general applicability of **ČSN EN ISO/IEC 17065,** it is necessary to determine special sector requirements for CABs, which are to perform conformity assessment at qualified trust service providers (later only „QTSP“). These sector requirements are defined by **ČSN EN 319 403 (ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); TRUST SERVICE PROVIDER CONFORMITY ASSESSMENT - REQUIREMENTS FOR CONFORMITY ASSESSMENT BODIES ASSESSING TRUST SERVICE PROVIDERS)** and specify both general requirements on CABs and general rules for performing of relevant audits. Above mentioned applicable requirements of ČSN EN ISO/IEC 17021-1 and ČSN ISO/IEC 27006 are also a part of ČSN EN 319 403[1].

[1] See provisions of ČSN EN 319 403: „The present document also incorporates many requirements relating to the audit of a TSP's management system, as defined in ISO/IEC 17021 [i.12] and in ISO/IEC 27006 [i.11]. These

To make the course of conformity assessment really effective, it is necessary to define so called „TSP audit criteria“, according to which the competence of CABs should be accredited by NAB and also according to which the conformity assessment itself should be done by CABs at QTSP. According to **ČSN EN 319 403,** the audit criteria should be based on following:

a) take into account specificities of the type of trust service to be assessed;

b) ensure that all aspects of the TSP activity are fully covered; and

c) be based on standards, publicly available specifications and/or regulatory requirements.

EXAMPLE: The standards, these criteria could be based on, include ETSI EN 319 401 [i.6], ETSI EN 319 411-1 [i.2], or ETSI EN 319 411-2 [i.3] or ETSI EN 319 421 [i.9]. Regulatory requirements, these criteria could be based on, include those defined in Regulation (EU) No 910/2014 [i.1].

In this manner, the accredited CABs would be able to carry out not only regular audits according to Article 20.1 of eIDAS Regulation, but also the initial conformity assessment according to Article 21 of eIDAS Regulation and ad-hoc conformity assessment according to Article 20.2 of eIDAS Regulation, - the same audit criteria for all three types of conformity assessment.

It is required that CAB is a certification body and not “only” inspection body or laboratory, because CAB has to certify providers according to defined audit criteria. Certification requires regular monitoring of services with the aim to find out, whether the requirements relevant for the product – service, as well as requirements of permanent effort to improve provided services, are continually met.

The aim of **ČSN EN 319 403** standard is also to enable conformity assessment both according to best practices and experience and according to technical requirements of eIDAS Regulation.

---

requirements are incorporated by including text to derived from these documents in the present document, as well indirectly through references to requirements of ISO/IEC 17021 [i.12].“

2. Requirements for trust service providers, later only („TSP“)

2.1. Common requirements for all TSP

Data processing and protection:

eIDAS - Article 5.1: Personal data processing shall be carried out in accordance with Regulation (EU) 2016/679 (known as GDPR)[2].

eIDAS - Article 5.2: Without prejudice to the legal effects given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited.

eIDAS Article 5(1)	General Policy Requirements for Trust Service Providers (ETSI EN 319 401)	Chapter 7.13, REQ[3]-7.13-05. TSP operating services in EU shall be governed by the GDPR. Note: Conformity with EN 319 411-2 (QTSP issuing QCs) and conformity with EN 319 421 (QTSP issuing qualified time stamps) also requires compliance with chapter 7.13, REQ-7.13-05 EN 319 401.

Liability for damage and burden of proof:

eIDAS - Article 13.1: Trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under eIDAS Regulation.

- The burden of proving intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damages.
- In the case of QTSP, intention or negligence shall be presumed unless QTSP proves that the damage occurred without intention or negligence of that QTSP.

[2] eIDAS Regulation contains reference to original Directive 95/46/ES which, with effect from 25 May 2018 was repealed. References to repealed Directive are deemed as references to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27. April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ES (General Data Protection Regulation). For this reason, the text of the requirement of Article 5 already contains directly reference to GDPR even though the normative text eIDAS Regulation refers to the original Directive.

[3] The abbreviation REQ means specific requirement set out in given standard (REQ - requirement).

eIDAS - Article 13.2: Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where these limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.

eIDAS - Article 13.3: Liability and damages are governed by national rules.

eIDAS Article 13(2)	General Policy Requirements for Trust Service Providers (ETSI EN 319 401)	Chapter 6.2 Note: Conformity with EN 319 411-2 (QTSP issuing QCs) and conformity with EN 319 421 (QTSP issuing qualified electronic time stamps) also requires compliance with chapter 6.2 in EN 319 401.
	Certificate Profiles (ETSI EN 319 412-5)	Chapter. 4.3.2, if limitation of the maximum value of transactions is given in the form of QCStatement in a certificate.
eIDAS Article 13(3)	General Policy Requirements for Trust Service Providers (ETSI EN 319 401)	Chapter. REQ-7.1.1-04 and REQ-7.1.1-05.

Accessibility for persons with disabilities:

eIDAS - Article 15: Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities.

eIDAS Article 15	General Policy Requirements for Trust Service Providers (ETSI EN 319 401)	Chapter REQ-7.13-03 requires provided services and end-user products used in the provision of these services to be accessible for persons with disabilities (applicable standards should be taken into consideration (chapter. REQ-7.13-04), such as EN 301 549). Note: Conformity with EN 319 411-2 (QTSP issuing QCs) and conformity with EN 319 421 (QTSP issuing qualified electronic time stamps) requires also conformity with Chapter REQ-7.13-03 and Chapter REQ-7.13-04 EN 319 401.
	Accessibility requirements suitable for public procurement of ICT products and services in Europe (ETSI EN 301 549) Design for All - Accessibility following a Design for All approach in products, goods and services - Extending the range of users (EN 17161)	

Security requirements related to trust service providers:

eIDAS - Article 19.1: Trust service providers shall

- take appropriate technical and organisational measures to management of risks posed to security of trust services they provide,
- having regard to the latest technological development, these measures shall ensure that the level of security is commensurate to the degree of risk,
- take measures to prevent security incidents, to minimise their impacts and inform stakeholders of the adverse effects of any such incidents

eIDAS Article 19(1)	General Policy Requirements for Trust Service Providers (ETSI EN 319 401)	However, Chapter 5 (risk assessment) does not contain strict requirements for the implementation of selected measures ("select" to become "implement"). Chapter 6.3 related to information security policy. Chapter 7 (except 7.1.1 & 7.13). Other requirements laid down in Chapter 6.4 (Facility, management and operational controls) and in Chapter 6.5 (Technical security controls) of EN 319 411-1 standard are deemed necessary (generally for all TSP covered by eIDAS Regulation) in view of the obligation to meet requirements laid down in Article 19.1 of eIDAS Regulation. For this reason it is required: - For TSP issuing certificates, conformity with EN 319 411-1 standard, chapters 6.4 and 6.5. - Pro TSP issuing time stamps, conformity with applicable Chapters of EN 319 421.
	Pro TSP issuing certificates: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (EN 319 411-1)	For TSP issuing certificates, ability to demonstrate compliance with requirements of Article 19(1) is compliance with requirements of Chapters 6.4 and 6.5 ETSI EN 319 411-1.

	For TSP issuing electronic time stamps: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (ETSI EN 319 421)	For TSP issuing electronic time stamps, ability to demonstrate compliance with requirements of Article 19(1) is compliance with requirements of chapters 7.8, 7.9, 7.10, 7.12, and 7.13 ETSI EN 319 421.

Reporting on security breaches and breaches of protection of personal data:

eIDAS - Article 19.2: TSP shall:

- notify the supervisory authority and any other competent bodies, such as competent national authority for information security or data protection authority, of every breach of security or loss of integrity, which has a significant impact on trust service provided or on personal data maintained, without undue delay, in any event within 24 hours of the time they found the breach,
- notify without undue delay also the related natural or legal person of security breach or loss of integrity, if the security breach or loss of integrity can have an adverse effect on the person,
- inform the public, where the disclosure of the breach of security or loss of integrity is in the public interest and the TSP has been requested by the supervisory authority to do so.

eIDAS Article 19(2)	General Policy Requirements for Trust Service Providers (ETSI EN 319 401)	Chapter 7.9 (especially REQ-7.9-07 and REQ-7.9-08) Note: Conformity with EN 319 411-2 (QTSP issuing qualified certificates) and conformity with EN 391 421 (QTSP issuing electronic time stamps) requires conformity with EN 319 401 Chapter 7.9.

There are no specific ETSI standards, designed specially to address risk management and technical and organisational measures that TSP must implement to guarantee the safety of provided services. However, it is possible to follow, for example, ČSN ISO 31000 standard containing directives for management of risks, organisations are exposed to. Application of these directives may be adopted to any organisation and its context. The standard provides a common approach to management of any type of risk and it is not specific to industry or sectors. The standard can be used throughout the life of the organisation and can be applied to any activity, including decision-making at all levels. ČSN ISO/IEC 27005 standard, containing information security risk management directives with support for general concepts specified in ISO/IEC 27001 and in ISO/IEC 27002, is another

example of the general standard that can be followed. ČSN ISO/IEC 27005 standard is designed to support the successful implementation of information security based on access control.

There are also no standards containing requirements for formats and procedures, including time limits, applicable for the purposes of notification of security breaches and notifications of personal data breach. However, the ENISA document [6] elaborates this area - contains useful information describing the different flows of information in the event of reporting of security incidents, proposes the factual content of the reports, the list of assets and the assessment of the impact with regard to the integrity, availability and confidentiality.

However, both areas (risk management and the adoption of technical and organisational measures) are addressed in the context of the provision of specific trust services. Standards for issuance of qualified certificates and issuance of qualified electronic time stamps are currently available

2.2. Common requirements for all QTSP

Common requirements for all QTSP consist, on the one hand, of the requirements for all trust service providers (see Chapter 2.1) and the requirements laid down in Article 24.2 of the eIDAS Regulation:

- inform the supervisory authority of any change in the provision of its qualified trust services and an intention to cease those activities (a new requirement compared to Directive 1999/93/EC),
- employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience and qualifications and who have received appropriate training regarding security and personal data protection rules, and shall apply administrative and management procedures which correspond to European or international standards (similar to those of Annex II(e) to Directive 1999/93/EC),
- maintain sufficient financial resources and/or take out appropriate liability insurance in accordance with national law with regard to the risk of liability for damage (similar to requirements of Annex II(h) to Directive 1999/93/EC),
- before entering into a contractual relationship, inform, in a clear and comprehensible 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 (similar to those of Annex II(k) to Directive1999/93/EC),
- use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of processes supported by them, (similar to requirements of Annex II(f) to Directive 1999/93/EC),
- use trustworthy systems to store data provided to them, in a verifiable form (a new requirement compared to Directive 1999/93/EC)
- take appropriate measures against forgery and theft of data (generalisation of Annex II(g) to Directive 1999/93/EC)

- record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular for the purpose of providing evidence in legal proceedings and for purpose of ensuring continuity of the service. Such recording may be done electronically (generalisation of Annex II(i) to Directive 1999/93/EC, a new requirement for keeping records and making information accessible also after the end of the activity)
- have an up-to-date termination plan to ensure continuity of the service (a new requirement compared to Directive 1999/93/EC)
- ensure lawful processing of personal data in accordance with Directive 95/46/ES (similar to requirements of Article 8 of Directive 1999/93/EC)

Note: eIDAS Regulation also defines in Article 20 the audit regime for QTSP and defines in Article 21 the procedure for initiation of provision of qualified trust services.

- Regular audit: qualified trust service providers shall be audited at their own expense at least once in every 24 months by a conformity assessment body. The purpose of the audit is to confirm that qualified trust service providers and qualified trust services provided by them comply with the requirements laid down in this Regulation. Providers shall submit the resulting conformity assessment report to the supervisory authority (e.g. Ministry of the Interior).
- Ad-hoc audit: The supervisory authority may, at expense of QTSP, perform an audit at any time or request a conformity assessment body to carry out a conformity assessment in order to confirm that QTSP themselves and the qualified trust services provided by QTSP comply with the requirements laid down in this Regulation.
- If QTSP does not remedy the failure to comply with the requirements of eIDAS Regulation within (where applicable) the specified time limit set out by supervisory authority, the supervisory authority may, in particular taking into account the extent, duration and consequence of the non-compliance, withdraw the qualified status of the provider or of the affected service it provides. The supervisory authority shall inform the qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned.

Procedure for initiation of provision of a qualified trust service:

- If trust service providers without status of qualified provider intend to start providing qualified trust services, they shall submit a notification of their intention to the supervisory authority together with the conformity assessment report issued by the conformity assessment body.

- The supervisory authority shall verify that the trust service provider and the trust service provided by it meet the requirements laid down in eIDAS Regulation.
- If the supervisory authority concludes that the trust service provider and the trust service provided by it meet the requirements, the supervisory authority shall grant the trust service provider and trust services provided by it the status of a qualified provider and a qualified service within three months of receipt of the notification. If the verification is not completed within three months of notification, the supervisory authority shall inform the provider and indicate the reasons for the delay and the period during which the verification will be completed.
- Qualified trust service providers can start providing a qualified trust service after the status of qualified provider and qualified service has been published in the trusted lists.

eIDAS Article 20(1)	EN 319 411-2 (QTSP issuing qualified certificates)	Not addressed in EN 319 411-2, referred to the requirements EN 319 411-1 - Chapter 6.7. contains only the note referring to ČSN EN 319 403. However, ČSN EN 319 403 applies to (accredited) conformity assessment bodies. Ensuring of remedies when non-compliance was found during an audit is not addressed by these standards. Not addressed in EN 319 401.
	EN 319 421 (issuing qualified el. time stamps)	See comment above.
eIDAS Article 21(1)	No ETSI/CEN standards are available or covering formats and procedures for the purpose of Article 21(1).	
eIDAS Article 21(2)	No ETSI/CEN standards are available or covering formats and procedures for the purpose of Article 21(2).	

eIDAS Article 24(2). a	EN 319 411-2 (QTSP issuing qualified certificates)	Addressed in EN 319 411-2 through Chapter 5.2 with reference to applicable requirements of EN 319 411-1. Chapter 5.2 EN 319 411-1 refers to the applicable requirements laid down in chapter 6.1 EN 319 401.
	EN 319 421 (QTSP issuing qualified el. time stamps)	Addressed in EN 319 421 through Chapter 6.2, with reference to applicable requirements laid down in Chapter 6.1 of EN 319 401 standard.
eIDAS Article 24(2). b	EN 319 401 (QTSP providing qualified trust services)	Chapter REQ-7.1.2-01 and chapter. 7.2 EN 319 401.
	EN 319 411-2 (QTSP issuing qualified certificates)	Chapter 6.4.4 with reference to 6.4.4 EN 319 411-1 on the basis of Chapter 7.2 EN 319 401. Chapter 6.9.1 with reference to 6.9.1 EN 319 411-1 on the basis of Chapter 7.1. EN 319 401.
	EN 319 421 (QTSP issuing qualified el. time stamps)	Chapter 7.2 & 7.3 with reference to applicable requirements of EN 319 401 (Chapters 7.1 and 7.2).

eIDAS Article 24(2).c	EN 319 411-2 (QTSP issuing qualified certificates)	Chapter 6.8.2 with reference to Chapter 6.8.2 EN 319 411-1 on the basis of REQ-7.1.1-04 EN 319 401.
	EN 319 421 (QTSP issuing qualified el. time stamps)	Chapter 7.2 with reference to applicable requirements of Chapter 7.1. EN 319 401 (including Chapter REQ-7.1.1-04).
eIDAS Article 24(2). d	EN 319 411-2 (QTSP issuing qualified certificates)	Chapter 6.1, 6.3.4, 6.3.5 and 6.9.4 with reference to Chapters 6.1, 6.3.4, 6.3.5 and 6.9.4 EN 319 411-1 (Chapter 6.9.4 follows Chapter 6.2. EN 319 401)
	EN 319 421 (QTSP issuing qualified el. time stamps)	Chapter 6.3 with reference to applicable requirements of EN 319 401 (Chapter 6.2).

eIDAS Article 24(2). e & 24(2).f	It depends on what type of process within a particular type of service shall be supported by a trusted system as well as in case of different ways of providing remote signature service (creation or managing data for creation of electronic signatures), e.g. support of remote signing with advanced or qualified el. signature. Candidate standards: - EN 419 221 (Security requirements for trustworthy systems managing certificates for electronic signatures) - protection profiles for cryptographic modules used by providers, especially part 5 –protection profile for cryptographic modules used by providers. - EN 419 231 protection profile for trustworthy systems supporting process of time stamps issuance. - EN 419 241-1 safety requirements and EN 419 241-2 f protection profile for QSCD devices for server signature. - CEN/TS 419 261 (originally prTS 419 221-1, originally prTS 14167-1) – security requirements for trustworthy systems managing certificates and time stamps. EN 319 411-2 and EN 319 421 contain requirements for QTSP for use of trustworthy systems referred to in Article 24(2).e and 24(2).f. Meeting the requirements of Article 24(2)(e) can be proved by assessment of the information security management system according to ČSN ISO/IEC 27002 or other similar standard. If the system is not evaluated, meeting requirements of Article 24(2)(e) can be proved also by meeting the requirements of REQ-7.7-02 to REQ-7.7-09 EN 319 401. Conformity with the requirements of Article 24(2)(f) implies also meeting requirement of REQ-7.3.2-01 EN 319 401 (the principle of safe treatment of the media with regard to their content and possible disposal, if they are not needed).	
eIDAS Article 24(2). g	EN 319 411-2 (QTSP issuing qualified certificates)	Chapters 6.4 and 6.5 with reference to EN 319 411-1 Chapters 6.4 and 6.5, following EN 319 401.
	EN 319 421 (QTSP issuing qualified el. time stamps)	Chapters 6.1, 6.4 & 7 following EN 319 401.

eIDAS Article 24(2). h	EN 319 411-2 (QTSP issuing qualified certificates)	Chapters 6.2.2, 6.3.4, 6.3.8, 6.4.5, 6.4.6, and 6.4.9 with reference to EN 319 411-1 following EN 319 401.
	EN 319 421 (QTSP issuing qualified el. time stamps)	Chapters 7.6.5, 7.7.2, 7.8 and 7.12 following EN 319 401.
eIDAS Article 24(2).i	EN 319 411-2 (QTSP issuing qualified certificates)	Chapter 6.4.9 with reference to Chapter 6.4.9 EN 319 411-1 following EN 319 401 Chapter 7.12.
	EN 319 421 (QTSP issuing qualified el. time stamps)	Chapter 7.14 following EN 319 401 Chapter 7.12.
eIDAS Article 24(2).j	EN 319 411-2 (QTSP issuing qualified certificates)	Chapters 6.8.4 and 6.8.15 with reference to Chapters 6.8.4 and 6.8.15 EN 319 411-1 following EN 319 401 Chapter 7.13.
	EN 319 421 (QTSP issuing qualified el. time stamps)	Chapter 7.15 following Chapter 7.13 EN 319 401.

2.3. Requirements for QTSP issuing qualified certificates

Requirements for QTSP issuing qualified certificates consist both of requirements for all trust service providers (see Chapter 2.1), and requirements set for all QTSP (see Chapter 2.2) and following requirements:

eIDAS - Article 24.1:

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.

The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by 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 meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high'; or
(c) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or
(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.

eIDAS - Article 24.2 (k): QTSP issuing qualified certificates establishes and keeps updated a certificate database.

eIDAS - Article 24.3: If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database 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 revocation shall become effective immediately upon its publication.

eIDAS - Article 24.4: With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide any relying party with information on the validity or revocation of qualified certificates issued by them. 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.

Requirements for qualified certificates:

- Annex I to eIDAS Regulation: Requirements for qualified certificates for electronic signatures pursuant to Article 28.1
- Annex III to eIDAS Regulation: Requirements for qualified certificates for electronic seals pursuant to Article 38.1
- Annex IV to eIDAS Regulation: Requirements for qualified certificates for website authentication pursuant to Article 45.1

Article 28.3, 38.3, recital č. 65: Qualified certificates may include non-mandatory attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures/seals.

Article 28.4, 38.4, recital č. 65: If a qualified certificate for electronic signatures/seals has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.

If QTSP issues together with qualified certificates for el. signatures or el. seals also qualified signature/seal creation device, then it must be secured that these means comply with requirements of Annex II to eIDAS Regulation and also that these means are certified in conformity with Article 30 of eIDAS Regulation by relevant private or public sector bodies designated by Member States. Or it must be a means considered as a qualified signature creation device on the basis of transitional measure laid down in Article 51(1) of eIDAS Regulation.

Implementing Decision of the Commission (EU) 2016/650

On 26. April 2016 Implementing Decision of the Commission (EU) 2016/650 of 25. April 2016 was published in Official Journal of the EU. The Decision states standards for security assessment of qualified signature and seal creation devices pursuant to Article 30(3) and 39(2) of Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1438256835547&uri=CELEX:32016D0650. Annex to the Implementing Decision sets out standards for security assessment of information technology products. These standards should be used for certification of qualified signature and seal creation devices, if data for electronic signature creation or data for electronic seal creation are stored in the environment, which is entirely, but not necessarily exclusively, managed by the user. Related standards shall be used for certification of devices, which are in physical possession of signing or sealing person (e.g. chip card, USB token). In this case the standards are laid down which shall be compulsorily used for certification of the devices in physical possession of signing or sealing person. The Commission will shortly publish a list of certified qualified electronic signature creation devices and qualified electronic seal creation devices pursuant to Article 31, respectively Article 39 of eIDAS Regulation. On this list, the devices, considered as qualified electronic signature creation devices on the basis of transitional measure laid down in Article 51(1) eIDAS Regulation, will be published as well. (*Secure signature creation devices of which the conformity has been determined in accordance with Article 3(4) of Directive 1999/93/EC shall be considered as qualified electronic signature creation devices under this Regulation.*). The list of certified devices is only informative, not constitutional in nature.

Pending the establishment of the list of standards for security assessment of information technology products which should be used for certification of qualified electronic signature creation devices or qualified electronic seal creation devices, if QTSP manages data for electronic signature creation or data for electronic seal creation, the certification of such devices is based on alternative procedure, which uses a comparable level of security with standards referred to in Annex to the Decision and which was notified to the Commission by the relevant public or private sector body.

Except for issuing "own" qualified devices, QTSP can also certify cryptographic keys with corresponding information about storage in the qualified device, which were generated in the qualified device the user has in their disposal. In this case, it must be ensured that QTSP has implemented appropriate processes and procedures to ensure that cryptographic keys were really generated in the qualified device (i.e. ensuring the origin of the key).

eIDAS Article 24(1)	EN 319 411-2 (QTSP issuing qualified certificates)	Chapters 6.2.2 and 6.2.with reference to corresponding Chapters 6.2.2 and 6.2.3 EN 319 411-1. Note.*: With regard to requirements laid down in Article 24.1(b) of eIDAS Regulation, it is necessary to use the electronic identification means for which the physical presence of a natural person or authorised representative of a legal person has been ensured prior to the issuance of the QC, whether it is a means with a substantial or high level of assurance.*
eIDAS Article 24(2).k	EN 319 411-2 (QTSP issuing qualified certificates)	Chapter 6.1 with reference to corresponding Chapter 6.1. EN 319 411-1.
eIDAS Article 24.3	EN 319 411-2 (QTSP issuing qualified certificates)	Chapter 6.2.4 with reference to corresponding Chapter 6.2.4. EN 319 411-1.
eIDAS Article 24.4	EN 319 411-2 (QTSP issuing qualified certificates)	Chapter 6.3.10 with reference to corresponding Chapter 6.3.10 EN 319 411-1. Note.: the requirement of free of charge provision of QC validity information is not addressed in EN 319 411-2 standard – outside the standard scope.

Note: With regard to compliance with Articles 24.3 and 24.4 of eIDAS Regulation, EN 319 411-2 standard is considered not to contain sufficient measures as regards to CRL and OCSP profiles and the process of their creation and compliance with the requirements laid down in those Articles of eIDAS Regulation. The table A.1 in Annex A (informative) of EN 319 411-2 contains the checklist related to requirements for QTSP issuing QC pursuant to the QCP policy from eIDAS Regulation in relation to requirements of this technical standard. The table does not contain mapping of all requirements of eIDAS Regulation set on QTSP issuing QC pursuant to QCP policy, since some of the requirements of eIDAS Regulation are not technical and do not fall within the scope of EN 319 411-2.		
eIDAS Article 28(1) & Annex I eIDAS Article 38(1) & Annex III	EN 319 411-2 (QTSP issuing qualified certificates)	Chapter 6.6.1 with reference to corresponding Chapter 6.6.1 EN 319 411-1 requiring conformity with relevant EN 319 412 series standard (profile of a certificate) depending on the type of QC.
eIDAS Articles 28(3) & 38(3)		Chapter 6.3.9 with reference to corresponding Chapter 6.3.9. EN 319 411-1.
eIDAS Articles 28(4) & 38(4) eIDAS Article 45(1) & Annex IV		*Note: Instead of issuing a new qualified signature/seal creation device, QTSP may want to certify public keys generated in qualified device that is already in the hands of a user or operated remotely in conformity with Annex II (3). In this case the QTSP has to verify by appropriate means before issuing a qualified certificate, that corresponding private key to public key was generated in qualified device (see article 3(12) of eIDAS Regulation). EN 319 411-2* Chapters *SDP-6.5.1-02, SDP-6.5.1-03, SDP-6.5.1-07, 6.5.2, 6.3.5, and 6.3.12.*

eIDAS Article 28(5) eIDAS Article 38(5)	Temporary suspension of qualified certificates for electronic signature and for electronic seal may be specified at national level.

ETSI EN 319 412 should contain sufficient requirements to ensure that QTSPs issuing qualified certificates meet the applicable eIDAS requirements for the content of certificates.

ETSI EN 319 412 series of standards consists of five parts:

ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

ETSI EN 319 412-4 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates

ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

In the case of QTSP statement of compliance with ETSI EN 319 412 series of standards, CAB verifies on a sample of issued certificates that the format of these certificates complies with ETSI EN 319 412-2, ETSI EN 319 412-3 and ETSI EN 319 412-5.

2.3.1 Requirements for QTSP issuing qualified certificates for website authentication

eIDAS Article 45(2)	Baseline requirements for the issuance and management of publicly-trusted certificates (CAB Forum CAB BR)	Partially covered, see below.
	EV SSL certificate guidelines (CAB Forum CAB EVSSL)	Partially covered, see below

Guidance for Auditors and CSPs on ETSI TS 102 042 for Issuing Publicly-Trusted TLS/SSL Certificates (ETSI TR 103 123)	Guidance document for auditors (smaller scope of requirements than foreseen in eIDAS Regulation)
Technical report TR 101 564 on guidance on ETSI TS 102 042 for issuing EV certificates for auditors and CSPs Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 4: Certificate profile for web site certificates ETSI EN 319 412-4	Intended for use by auditors as methodological guidelines for assessing compliance of CA with TS 102 042 and used also for CA to clarify requirements.

Partially covered: Documents from CAB Forum represent industry standards used by the most important web browser makers. However, the requirements set out in these standards are primarily aimed at ensuring the identity of the website and its owner and do not fully meet the requirements for qualified website authentication certificates pursuant to eIDAS Regulation. ETSI standards refer to these standards and complements them with other specific requirements.

A possible implementing act under Article 45(2) of eIDAS Regulation would most likely refer to **ETSI EN 319 412-4** standard ("Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates").

In the case of QTSP statement of compliance with ETSI EN 319 412 series standard, CAB shall verify on a sample of issued certificates that the format of these certificates complies with ETSI EN 319 412-4 and ETSI EN 319 412-5.

2.4. Requirements for QTSP providing qualified validation service for qualified electronic signatures and/or qualified electronic seals

Requirements for QTSP providing qualified validation service for qualified electronic signature and/or qualified electronic seal (with reference to Articles 33 and 40 of eIDAS Regulation) consists of requirements for all trust service providers (see Chapter 2.1), and requirements for all QTSP (see Chapter 2.2) and following:

eIDAS - Article 33.1 (a) : QTSP provides validation in compliance with Article 32(1)

eIDAS – Article 33.1 (b) : QTSP allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service. In conformity with Article 32 (2), the service has to allow the relying party to detect any security relevant issues.

eIDAS Article 32(1)	Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation EN 319 102-1, ETSI TS 119 102-1
eIDAS Article 32(2)	Policy and security requirements for applications for signature creation and signature validation (ETSI TS 119 101)
eIDAS Article 33(1)	General requirements on testing compliance and interoperability of signature creation and validation (ETSI TS 119 144)
	EN 319 102-1, ETSI TS 119 102-1
	Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report (ETSI TS 119 102-2)

In February 2019, ETSI published updated technical specifications of **TS 119 312 (ELECTRONIC SIGNATURES AND INFRASTRUCTURES ; CRYPTOGRAPHIC SUITES)** – These are updates to the original specifications **TS 102 176-1**, known as "Algo paper". The document contains recommendations for selections of appropriate algorithms to ensure security and interoperability of electronic signatures depending on required level of security.

The issue of validation of qualified electronic signatures and seals is also related to the issue of formats of advanced electronic signatures and seals, see **COMMISSION IMPLEMENTING DECISION OF THE (EU) 2015/1506 OF 8. AUGUST 2015, LAYING DOWN SPECIFICATIONS RELATING TO FORMATS OF ADVANCED ELECTRONIC SIGNATURES AND ADVANCED SEALS TO BE RECOGNISED BY PUBLIC SECTOR BODIES PURSUANT ARTICLE 27 (5) AND ARTICLE 37(5) OF REGULATION (EU) NO 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON ELECTRONIC IDENTIFICATION AND TRUST SERVICES IN THE INTERNAL MARKET.**

Implementing decision specifies formats of advanced electronic signatures and of advanced electronic seals to be recognised by Member States, if they require, in order to use a particular online service offered by a public sector body, electronically signed documents or electronic documents bearing electronic seals:

ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); XADES BASELINE PROFILE ETSI TS 103 171 V.2.1.1.

ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI);CADES BASELINE PROFILE ETSI TS 103 173 V.2.2.1.

ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI);PADES BASELINE PROFILE ETSI TS 103 172 V.2.2.2.

ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); ASIC BASELINE ETSI TS 103 174 V.2.2.1.

In 2016, EN standards have been adopted to replace the above-mentioned technical specifications (however, Commission Implementing Decision (EU) 2015/1506 refers to technical specifications pending possible amendment of the Decision).

ETSI EN 319 132-1 ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); XADES DIGITAL SIGNATURES; PART 1: BUILDING BLOCKS AND XADES BASELINE SIGNATURES

ETSI EN 319 132-2 ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); XADES DIGITAL SIGNATURES; PART 2: EXTENDED XADES SIGNATURES

ETSI EN 319 122-1 ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); CADES DIGITAL SIGNATURES; PART 1: BUILDING BLOCKS AND CADES BASELINE SIGNATURES

ETSI EN 319 122-2 ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); CADES DIGITAL SIGNATURES; PART 2: EXTENDED CADES SIGNATURES

ETSI EN 319 142-1 ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); PADES DIGITAL SIGNATURES; PART 1: BUILDING BLOCKS AND PADES BASELINE SIGNATURES

ETSI EN 319 142-2 ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); PADES DIGITAL SIGNATURES; PART 2: ADDITIONAL PADES SIGNATURES PROFILES

ETSI EN 319 162-1 Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers

ETSI EN 319 162-2 Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers

CAB will have a pre-prepared sample of electronically signed documents to verify the quality of validation of qualified electronic signatures/seals. CAB can verify this sample in advance using (for example) ETSI Signature Conformance Checker (https://signatures-conformance-checker.etsi.org/pub/index.shtml - check of conformity of format AdES with ETSI TS / EN and demo DSS (https://ec.europa.eu/cefdigital/DSS/webapp-demo/home).

2.5. Requirements for QTSP providing qualified preservation service for qualified electronic signatures and/or qualified electronic seals

Requirements for QTSP providing qualified preservation service for qualified electronic signatures and/or qualified electronic seals (with reference to Articles 34 and 40 eIDAS Regulation) consist of the requirements for all trust service providers (see Chapter 2.1), and the requirements determined for all QTSP (see Chapter 2.2) and following:

eIDAS - Article 34.1 : the use of procedures and technologies that are capable of extending the trustworthiness of a qualified electronic signature beyond the technical validity period.

eIDAS Article 34(2)	PDF/A Specification (ISO 19005-1, Adobe) Audit and Certification of Trustworthy Digital Repositories (ISO 16363:2012, CCSDS) Storage of electronic invoices (CWA 15580) Design Criteria Standard For Electronic Records Management Software Applications (DoD 5015.2) Data Preservation Systems Security; Parts 1-2 (ETSI/ TS 101 533) Policy requirements for trust service providers signing and/or storing data objects (ETSI/CEN TS 102 573) Evidence Record Syntax (ERS)(IETF RFC 4998)

	Electronic archiving - Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation (ISO/IEC ISO 14641-1:2012) Information and documentation – Records management (ISO/IEC ISO 15489-1:2001) Information technology – Metadata registries (MDR)(ISO/IEC ISO/IEC 11179) Space data and information transfer systems - Open archival information system (OAIS) - Reference model (ISO/IEC ISO 14721:2012) Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Long-Term Preservation of Electronic Documents International Standard for Archival Description (General)(ISAD(G)) Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques (ETSI TS 119 511) DRAFT Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services protocols for long-term preservation (DRAFT ETSI TS 119 512 – prerequisite publication approved TS 04/2020)

eIDAS Regulation does not specify requirements for procedures and technologies that can be used to ensure the trustworthiness of qualified electronic signature/qualified electronic seal even after the technical validity period has expired. Therefore, it is not possible to assess the conformity of standards with eIDAS Regulation.

2.6. Requirements for QTSP issuing qualified electronic time stamps

Requirements for QTSP issuing qualified electronic time stamps (with reference to Article 42 of eIDAS Regulation) consist from requirements for all trust service providers (see Chapter 2.1), and requirements determined for all QTSP (see Chapter 2.2) and following:

eIDAS - Article 42.1 : Qualified time stamp shall meet following requirements:

- it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably; and
- it is based on an accurate time source linked to Coordinated Universal Time; and
- 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.

eIDAS Article 42(2)	Time-stamping System (CC3.1) (ANSSI DCSSI-PP 2008/07)	PP for trustworthy product TST.
	Politique d'Horodatage Type (ANSSI RGS A5)	Assessment.
	EESSI Conformity Assessment Guidance - Part 8 - Time-stamping Authority services and processes (CEN CWA 14172-8)	Assessment.
	Policy and security requirements for TSPs providing time-stamping services (ETSI EN 319 421)	Assessment, trustworthy systems, time management.
	Profiles for TSPs providing time-stamping services (ETSI EN 319 422)	Assessment, trustworthy systems.

Conformity with the standard shall ensure that connection of date and time with data is done in such a way that the possibility of undetectable data change is reasonable prevented and also the requirements for a source of accurate time that is associated with Coordinated Universal Time are ensured. Standard ETSI TS 102 023, which was used for time stamp authorities certification, has been updated under mandate M460 and divided into two standards:

- *ETSI EN 319 421* specifying requirements for policy and security requirements related to operation and management practices of TSP issuing time stamps. *ANSSI RGS A5* further reinforces these requirements, but contains some specific French requirements, which may not be compatible with current practice in other states.
- Conformity with *ETSI EN 319 422* ensures binding the date and time with data in issued electronic time stamps.

ANSSI DCSSI-PP 2008/07 and CEN EN 419 231 are protection profiles evaluated according to Common Criteria for time stamp authority system.

3. Requirements for basic content of conformity assessment report

Conformity assessment body shall issue so-called conformity assessment report following the conformity assessment.

Trust service provider has to submit this report to the supervisory authority (MV ČR) not only in connection with notification of intention of the trust service provider to initiate providing of qualified trust service, but also in connection with regular audit (qualified trust service providers shall be audited by the conformity assessment body at least once every 24 months at their own expense) or in connection with ad-hoc audit (the supervisory authority may audit the QTSP at any time at their expense or ask conformity assessment body to carry out conformity assessment to confirm that the QTSP and the qualified trust services provided by the QTSP meet the requirements laid down in this Regulation).

In particular, the conformity assessment report should contain recommendations, whether it is possible to make a certification decision. The report should also state the result of audit, e.g. the audited service is in compliance and meets the requirements or the audited service does not meet the requirements, in this case, the certificate cannot be issued (see 7.6 and 7.7 of ČSN EN ISO/IEC 17065:2013). This does not apply if non-conformities were found during the audit but do not affect meeting the requirements or provision of the service in question and if the non-conformities have to be rectified within 3 months depending on the seriousness of the error, see Chapter 7.6 **ČSN EN 319 403**. In certification decision, at least identification of conformity assessment body, identification of trust service provider, identification of assessed trust service, the start date and the end date of the assessment, result of the assessment and specification of the requirements (applicable requirements of eIDAS Regulation) against which the conformity assessment has been carried out, shall be stated. In conformity assessment report, it should be specified how the provider complies with the applicable requirements of eIDAS Regulation (e.g. by complying with certain provision of specific standard), see requirements laid down on content of audit report in Chapter 7.4.4. **ČSN EN 319 403.**

4. Abbreviations

[1] DKP - Document specifying the requirements for qualified trust service providers and qualified trust services provided by them

[2] eIDAS Regulation – 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 Directive 1999/93/ES)

[3] CAB - conformity assessment body

[4] NAB - national accreditation body

[5] QTSP - qualified trust service providers

[6] TSP - trust service providers

[7] REQ it indicates a specific requirement given in the standard (REQ - requirement)

[8] GDPR - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to processing of personal data and on the free movement of such data, and repealing Directive 95/46/ES (General Data Protection Regulation)

[9] AdES – advanced electronic signature

[10] DSS – Digital Signature Service

5. Sources

[1] ENISA: Analysis of standards related to Trust Service Providers Mapping of requirements of eIDAS to existing standards, https://www.enisa.europa.eu/publications/tsp_standards_2015.

[2] ETSI TR 119 000 V1.2.1 Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview

[3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23. July 2014 on elektronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/ES), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[4] Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1438256835547&uri=CELEX:32016D0650.

[5] 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 Article 27(5) and 37(5) of Regulation (EU) No 910/2014 of European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0006.

[6] ENISA: Article 19 Incident reporting, https://www.enisa.europa.eu/publications/article19-incident-reporting-framework