Finnish Transport and Communications Agency

Guideline

215/2019 O
9.10.2019

Assessment reports on qualified eIDAS trust services

Traficom Guideline

215/2019 O

Contents

1 Introduction

1.1 Purpose of the Guideline

This Guideline applies to qualified trust services referred to in the eIDAS Regulation.

The Guideline is designed for accredited conformity assessment bodies assessing the conformity of both qualified trust service providers and qualified trust services. The Guideline specifies the minimum contents and structure of the resulting assessment reports.

A separate guideline has been published on the notifications to be submitted to the Finnish Transport and Communications Agency Traficom (214/2016 O).

Under the Act on Strong Electronic Identification and Electronic Trust Services (617/2009; the 'Identification and Trust Services Act'), it is the Finnish Transport and Communications Agency's task to supervise compliance with the Act and the EU eIDAS Regulation. This Guideline has been issued pursuant to the general authorisation referred to in section 42 of the Identification and Trust Services Act.

1.2 Entry into force of the Guideline

Guideline 215/2019 O enters into force on 9 October 2019.

The Guideline is valid until further notice, and it may be supplemented and amended as necessary. In that case, the Guideline number 215 will be maintained, but the date and the year will be changed accordingly. The amended versions of the Guideline are listed in the following table:

The valid guideline is published on Traficom's website at https://www.kyberturvallisuuskeskus.fi/en/electronic-identification and https://www.traficom.fi/en/regulations

Version	Date	Description/change	Author
215/2019 O Assessment reports on qualified trust services	9 Oct 2019	Second published version ▪ The section concerning assessment reports on identification services has been transferred to Guideline 211/2019 O ▪ Technical amendments have been made to the text due to the Agency's new name; the titles have been modified.	Finnish Transport and Communications Agency (Traficom), NCSC-FI

215/2016 O Identification and trust service assessment reports	2 Nov 2016	First published version	Finnish Communications Regulatory Authority (FICORA), NCSC-FI

1.3 Legal provisions, definitions and abbreaviations

eIDAS: 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 and repealing Directive 1999/93/EC.

Identification and Trust Services Act: Act on Strong Electronic Identification and Electronic Trust Services (617/2009, as amended).

Qualified trusted service provider (QTSP):

> ***eIDAS Article 3 Definitions***
>
> *20) 'qualified trust service provider' means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;*

Qualified trusted service (QTS):

> **eIDAS Article 3 Definitions**
>
> *16) 'trust service' means an electronic service normally provided for remuneration which consists of:*
>
> *a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or*
>
> *b) the creation, verification and validation of certificates for website authentication; or*
>
> *c) the preservation of electronic signatures, seals or certificates related to those services;*
>
> *17) 'qualified trust service' means a trust service that meets the applicable requirements laid down in this Regulation;*

Conformity assessment body (CAB):

> ***eIDAS Article 3 Definitions***
>
> *18) 'conformity assessment body' means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, 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;*

Conformity assessment report (CAR):

See eIDAS Article 20 Supervision of qualified trust service providers

1. Qualified trust service providers shall be audited [...] by a conformity assessment body. The purpose of the audit shall be to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. The qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body [...].

[…]

See eIDAS Article 21: Initiation of a qualified trust service

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

[…]

2 Submission of conformity assessment reports

The assessment report shall be submitted to Traficom:

1. before commencing operations, if trust service providers without qualified status intend to provide qualified trust services; and

2. at least every 24 months after the trust service provider has submitted the assessment report to be provided at the time of commencing operations to Traficom.

PROVISIONS

eIDAS Regulation Article 20 Supervision of qualified trust service providers

1. Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The purpose of the audit shall be to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. The qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it.

2. Without prejudice to paragraph 1, the supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers, at the expense of those trust service providers, to confirm that they and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. Where personal data protection rules appear to have been breached, the supervisory body shall inform the data protection authorities of the results of its audits.

[…]

eIDAS Regulation Article 21 Initiation of a qualified trust service

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

2. The supervisory body shall verify whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, and in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide.

If the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements referred to in the first subparagraph, the supervisory body shall grant qualified status to the trust service provider and the trust services it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1), not later than three months after notification in accordance with paragraph 1 of this Article.

If the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider specifying the reasons for the delay and the period within which the verification is to be concluded.

3. Qualified trust service providers may begin to provide the qualified trust service after the qualified status has been indicated in the trusted lists referred to in Article 22(1).

[…]

Section 32 of the Identification and Trust Services Act

A conformity assessment body inspects the conformity of a qualified trust service provider and a qualified trust service pursuant to the provisions of the EU Regulation on Electronic Identification and Trust Services.

Provisions on the right of the Finnish Transport and Communications Agency to issue further provisions on the criteria used for assessing conformity are laid down in section 42. The Finnish Transport and Communications Agency may order as criteria for assessment regulations or guidelines issued by the European Union or another international decision-making body, published or commonly or regionally applied instructions on information security and commonly used information security standards or procedures.

3 Trusted list

If the notified service meets the requirements of a qualified trust service provider and a qualified trust service, Traficom shall grant the trust service provider and the trust services it provides a qualified status and enter the services in the trusted list.

The trusted list of Finland is available online at https://dp.trustedlist.fi/fi-tl.pdf

eIDAS Article 22 Trusted lists

1. Each Member State shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.

4 Contents of assessment reports

The assessment report of a qualified trust service shall contain at least the following basic details:

4.1 Basic details of the conformity assessment body

1. name of the company or organisation and a unique registration number or identifier;

2. if the company or organisation is located in an EEA state other than Finland, the register in which the foreign company or organisation has been entered;

3. postal address and contact persons; Email addresses for enquiries by Traficom.

4.2 Basic details of the trust service subject to assessment

4. name(s) of the qualified trust service subject to assessment or the service applying for a verification of a qualified status, as well as service types in accordance with chapter 4.1.1, paragraph 4 of the notification guideline 2014/2016 O, that is:

    a. qualified certificate for electronic signatures (eIDAS Article 28);

    b. qualified validation service for qualified electronic signatures (eIDAS Article 33);

    c. qualified preservation service for qualified electronic signatures (eIDAS Article 34);

    d. qualified certificate for electronic seals (eIDAS Article 38);

    e. qualified validation service for qualified electronic seals (eIDAS Article 40);

    f. qualified preservation service for qualified electronic seals (eIDAS Article 40);

    g. qualified electronic time stamp (eIDAS Article 42);

    h. qualified electronic registered delivery services (eIDAS Article 44); or

    i. qualified certificate for website authentication (eIDAS Article 45).

4.3 Basic details of the conformity assessment procedure

5. description of the part of the trust service covered by the assessment;

6. description of the methods employed to assess the different parts of the service;

7. details of the documentation used in the conformity assessment; and

8. date(s) and duration (person-days or hours) of the conformity assessment.

The assessment report shall identify the qualified trust service(s) covered by the assessment and describe whether the service is assessed in part or in full. The provider of a qualified trust service may also have the assessment made in several parts by two or more conformity assessment bodies. It is essential that the assessment report is unambiguous in detailing whether the assessment report prepared by the conformity assessment body covers all requirements referred to in section 4.4 or only some of them.

The assessment report shall indicate the methods employed in the conformity assessment. A mere list of standards cannot be considered adequate; instead, the assessment report shall describe the method employed in the assessment of each area referred to in section 4.4.

The assessment report shall list the assessed items of documentation of the service provider. It is not necessary to attach all materials related to the assessment to the assessment report submitted to Traficom. Traficom may request more detailed documents to be submitted where necessary. Traficom's right to obtain information is based on section 43 of the Identification and Trust Services Act, under which Traficom has, secrecy provisions notwithstanding, the right to obtain information necessary for performing its tasks from the parties whose rights and obligations are laid down in the said Act or who act on their behalf.

4.4 Demonstration of conformity

The purpose of the conformity assessment of a trust service is to demonstrate that a qualified trust service notified to Traficom meets the requirements laid down in the eIDAS Regulation.

The assessment report shall indicate the method for assessing compliance with the requirements below and the grounds for assessing the trust service as compliant with the requirements below:

4.4.1 Specific requirements for service providers

9. requirements for data processing and protection (eiDAS Article 5);

10. provisions concerning liability and burden of proof (eIDAS Articles 13(1) and 13(2) and Identification and Trust Services Act, section 41);

11. requirements for accessibility for persons with disabilities (eIDAS Article 15);

12. security requirements applicable to trust service providers (eIDAS Article 19(1)); and

13. requirements for qualified trust service providers (eIDAS Article 24, excl. 24(2)(k)).

4.4.2 Specific requirements for qualified trust services

14. general assessment criteria for trust services provided in sections 20 and 21 of Regulation 72;

15. requirements for qualified certificates (eIDAS Article 24(1)(a)–(d), 24(2)(k) and 24(3)–(4));

16. requirements for qualified certificates for electronic signatures (eIDAS Article 28(1));

17. requirements for qualified validation services for qualified electronic signatures (eIDAS Articles 32 and 33);

18. requirements for qualified preservation service for qualified electronic signatures (eIDAS Article 34);

19. requirements for qualified certificates for electronic seals (eIDAS Article 38);

20. requirements for qualified validation services for qualified electronic seals (eIDAS Articles 40, 32 and 33);

21. requirements for qualified preservation services for qualified electronic seals (eIDAS Articles 40 and 34);

22. requirements for qualified electronic time stamps (eIDAS Article 42);

23. requirements for electronic registered delivery services (eIDAS Article 44); and

24. requirements for qualified certificates for website authentication (eiDAS Article 45).

4.5 Reporting of irregularities

Irregularities and deviations are typically found during a conformity assessment and corrected during the assessment or shortly thereafter. Normally, any detected irregularities are corrected before submitting the assessment report Traficom.

However, if any irregularities remain, they must be clearly identified in the assessment report. In this case, the assessment report shall contain details of any minor or other irregularities remaining in the system and indicate how and when they will be corrected. Traficom will not prepare a scale indicating the severity of irregularities, but leaves their evaluation to the discretion of the trust service provider and the assessment body at the assessment and notification phase. Traficom makes the final assessment on whether the irregularities may be accepted. Traficom may also require the detected irregularities to be corrected.