Viestintävirasto

12 December 2018

Record no.: 1003/620/2018

Advice from the Finnish Communications Regulatory Authority (FICORA)[1] on assessing compliance of identification services in 2019

1 Background

1.1 Nature of this interpretation memorandum

In this memorandum, FICORA has included advice based on common questions on the application of identification service assessment requirements. The advice is offered at a general level. FICORA controls compliance with all the requirements on the assessment of identification services by using the policies laid down in Sections 2.1 and 2.2.

FICORA may supplement this memorandum as required.

Identification service providers are obligated to ensure the management of the information security of their identification service and appropriately consider all risks and threats related to their service. If FICORA is forced to make a control decision on a specific service provider, the facts and the regulations will be considered on a case-by-case basis.

1.2 Regulations

Section 29 of the Act on Strong Electronic Identification and Electronic Trust Services (laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista, 617/2009; the “Identification Act”) includes regulations on the obligation of a provider of a strong electronic identification service to periodically have its service audited by an assessment body as laid down in section 28 in terms of the compatibility, information security, data protection and other reliability requirements laid down in the Act. The purpose of the audit is to assess how the identification service and the business operations comply with the set requirements.

FICORA’s right to issue further regulations on the assessment criteria to be employed when assessing the compliance of the identification service is laid down in section 42.

Section 15 of FICORA’s regulation 72A/2018 M specifies the requirement areas that must be included in the independent audit. Section 16 of the regulation specifies the requirement areas for which the identification service provider can submit its own report.

Pursuant to section 31 of the Identification Act, the assessment report will be valid for the period defined in the standard applied to the conformity assessment, but no more than two years.

[1] The Finnish Communications Regulatory authority (FICORA) continues its operations as a part of the Finnish Transport and Communications Agency (Traficom) on 1 January 2019.

The said regulations of the Identification Act entered into force on 1 July 2016, and according to the period of transition specified in the Act, the report was to be submitted to FICORA by 31 January 2017.

Pursuant to section 10 of the Identification Act, the commencement notification must include a report prepared by a conformity assessment body, another external assessment body or an internal assessment body on the independent assessment in the manner laid down in section 29, and a notification of any changes in the information must be submitted to FICORA in writing without delay.

FICORA has prepared instructions on the assessment criteria (211/2016) and on the report (215/2016). A project of updating and further supplementing the instructions was started on 28 November 2018.

1.3 Processing of reports submitted in January 2017

By the deadline, FICORA received reports from all of the providers of strong electronic identification services that were included in the register as laid down in section 12 of the Identification Act before the entry into force of the legislative amendments.

Further information on all of the reports was requested; twice in the case of some of them.

Furthermore, some of the identification service providers submitted notifications of changes and related reports.

In July 2017, FICORA carried out the first intermediate assessment of all of the reports. The assurance levels of almost all of the strong electronic identification services were included in the register as laid down in section 12 of the Act, regardless of the fact that there were some deficiencies in the information or implementation method of some of the reports. Of the identification certificates issued by the Population Register Centre, citizen and organisation certificates were included in the register. The processing of the other certificates is still unfinished.

1.4 Notifications and reports submitted at other times

In addition to those mentioned above, FICORA has received notifications and reports from new identification service providers. Further information on all of the material parts of these reports was requested before the identification services were entered into the register.

2 Questions and FICORA's advice and policies

2.1 When will the identification service providers who submitted their reports in January 2017 have to submit new reports?

The Act states that a report is valid for a maximum of two years. In its instructions (215/2016), FICORA stated that a new report must be submitted at the latest two years after the approval of the previous report.

As further information on the reports had to be requested and FICORA has not completed its process of assessing the reports yet, the date from which the period of two years starts is subject to interpretation.

As an advance notice to the identification service providers, FICORA has stated that it is investigating two alternative interpretations of when an report can be considered to be approved:

- Registration date of an identification service that was already included in the register (which was completed in the case of most of the old services in July 2017); or
- the date when a specific identification service provider submitted all of the required further information to their report.

Hence, the earliest possible date is July 2019 and the latest possible dates – depending on the service provider – are mainly in 2020, as a large part of the requested further information has not been processed yet. Therefore, FICORA will **not** require the submission of new reports in January 2019 or within two years from the deadline for the submission of the first report as specified in the Act.

In its interpretation, FICORA considers the Act and its justification, as well as the fact that FICORA's processing of the reports has been delayed, and the assessment instructions will be updated in 2018 and 2019. This means that the instructions to support the new audits will not be available in full in early 2019. Furthermore, FICORA considers the fact that due to the processing backlog, the identification service providers have not been fully able to influence themselves the time when FICORA completes its assessment of the compliance and adequacy of the report.

FICORA is aware of the fact that as many of the assessments submitted in January 2017 were completed in late 2016, information security threats and risks have subsequently changed and the new assessments should not be unnecessarily delayed.

FICORA provides the following advice:

- All parties will be specified the same schedule based on which FICORA will oversee the submission of the reports.
- If the preparation or acquisition of the assessments has not been started yet, it should be started in early 2019 as soon as the identification service providers have sufficient information on the assessment requirements (see more information in the next paragraph).
- The reports will have to be submitted without delay, as soon as they are completed.
- The reports will have to be submitted by the end of 2019 at the latest.

2.2 When will the identification service providers who were entered into the register in 2017 or later have to submit a new report?

A new report must be submitted within two years of the new identification service provider having been entered into FICORA's register compliant with section 12 of the Identification Act.

2.3 How extensive must the follow-up reports to be submitted every two years be?

FICORA provides the following advice:

1. Any identification service operations that are already in the register need not be comprehensively reassessed.

2. Any issues on which FICORA requested company-/corporation-specific further information or in the case of which FICORA stated in its request for further information that future assessments or reports must be more specific or more comprehensive must be taken into account in the assessment.

3. The assessment must also consider any changes, unless a notification and a report on them have already been submitted to FICORA.

4. In the case of the management of information security, verifying that the requirements for identification services (based on the Identification Act, the eIDAS Regulation, the Assurance Level Regulation and the FICORA regulation) have been taken into account in the management system suffices.

5. When assessing the management of disruptions, the identification service’s capability and readiness to observe disruptions and report them as necessary must be considered. FICORA receives a fairly small number of disruption reports and considers paying attention to the management of disruptions in identification services important.

6. The report must include a figure, a diagram or another clear presentation of the identification system’s (scheme's) overall architecture. The reader must be able to verify, based on the description of the architecture and the report, that all relevant issues influencing the security of the system were taken into account in the assessment and the system architecture is secure.

    - The system architecture description must indicate identification-related system components.

    - The reader must be able to understand the different sections of the identification system and their suppliers, connections/gateways between the sections, connection security policies, interfaces between the system sections and other related issues based on the report.

    - The description of the architecture must indicate functional relations between all of the identification system components, such as the separation of data resources, the separation of the presentation layer and business logic, gateways/connections between environments and their protection, as well as security controls between the system and external parties.

    - The description must indicate the network topology, L3 level components, such as firewalls, servers and connections to other environments, and management connections, if they have been separated.

    - Data flows connected to the identification process should also be described.

- If the system uses productized components or products included in cloud services (Amazon Web Services, Google, Microsoft Azure, etc.), the product components must be named and the external components must be included in the scope of the subcontractor assessment.

7. If a mobile identification application is used, it must be assessed in all respects that influence the compliance of the identification service. If the application also includes other features, the other features need not be included in the assessment insofar as they cannot influence the reliability of the identification.

8. In addition to the assessment report, a scanning report which indicates the TLS- and encryption profiles of the identification system's external interface must be submitted for M72A, section 7 assessments.

9. Subcontractors' compliance must be assessed in all the respects mentioned above.

10. Compliance of the methods used when issuing the identification means (initial identification, creation, delivery) need not be reassessed, except if changes have occurred.

    - If electronic initial identification has been introduced, the initial identification events being saved in compliance with section 24 of the Identification Act and data being available in compliance with section 16 of the Identification Act should be assessed.

    - In the case of mobile applications, please see Section 7.

2.4 Notifying and assessing changes

If a material change occurs in the operations, an assessment must be carried out and a notification on the change and an assessment report must be submitted before the change is transferred to production.

The following are always considered to be material changes, for example:

- Changes of the identification method, i.e. the authentication factors and the authentication mechanism

- Technical changes in the identification system, i.e. changes of the maintenance and production systems or software

- Changes in or replacement of subcontractors supplying maintenance services, hardware, systems or software

FICORA has been asked whether the replacement of a Tupas interface with a SAML or OIDC interface must be assessed.

- An interface execution method that will be abandoned in 2019 (Tupas or other) need not be assessed.

- Any new execution methods must be assessed in terms of the encryption requirements and the management of cryptographic keys. Customer services are not included in the scope of the assessment, but any management practices for cryptographic keys required for the services or provided as part of the services must be assessed.

- If a change of protocol involves any other material changes in the identification system in addition to the configuration of the interface or architecture, the changes must be assessed.