Advisory memorandum for periodic assessments 2021

1 General

In this memorandum, the Finnish Transport and Communications Agency (Traficom) highlights different themes for commissioning/conducting the 2021 periodic assessment. The themes concern recurrent shortcomings in previous periodic assessments and suggestions for improvements in the assessment process. The purpose of these guidelines is to reduce the need to request supplementary information and to speed up the processing of assessments by identification service providers and Traficom.

The memorandum can be divided into two parts:

- themes that require particular attention because of shortcomings in their reporting in previous periodic assessments

a voluntary reporting tool in the form of a standard Excel table to ensure that assessments and reports cover the required elements and to speed up the processing of assessments.

2 Legal framework

Section 29 of the Act on Strong Electronic Identification and Electronic Trust Services (617/ 2009, hereinafter referred to as 'the Identification and Trust Services Act') requires providers of strong electronic identification services to regularly subject their service to an assessment by an assessment body referred to in section 28 to evaluate whether the identification service meets the requirements on interoperability, information security, data protection and other reliability 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.

Pursuant to section 31 of the Identification Act, the assessment report is in force for the period defined in the standard that was used in the assessment, but not longer than two years.

Provisions on Traficom's right to issue more detailed regulations on the criteria for assessing the conformity of an identification service are laid down in section 42.

The conditions for identification services are laid down in the Identification Act and, as referenced in the Act, in the Commission Implementing Regulation (EU) 2015/1502 (hereinafter referred to as 'the Assurance Level Regulation') and the Annex to the Regulation.

Section 15 of Regulation 72A/2018 M (hereinafter also referred to as 'M72') issued by the Finnish Communications Regulatory Authority (FICORA) specifies the requirement items that must be included in the independent audit. Section 16 of the Regulation specifies the requirement items for which the identification service provider can submit its own self-prepared report.

Traficom Guideline 211/2019 O *Assessment guideline for electronic identification services* includes general assessment criteria for auditing identification services and special criteria for mobile identification solutions. Identification service providers can use the above-mentioned criteria, some other criteria that meet the requirements of section 15 of Regulation M72 or a combination of these criteria.

3 Deadlines

The deadline for submitting assessment reports and their appendices to Traficom is 31 December 2021. The deadline in 2021 is the same for all operators that have begun their identification service operations before 2021.

Periodic assessments can be submitted to Traficom before the deadline without this affecting the deadline of the following assessment round.

When necessary, Traficom will separately determine the periodic assessment deadlines for any new identification services registered and inform service providers of these deadlines.

4 Traficom's supervisory policy concerning ChaCha20+Poly1305 encryption solutions

Traficom is preparing an amendment to the Regulation 72A/2018 M. The amendment is intended to enter into force in early 2022. According to section 7 of the current Regulation, the encryption algorithm used in symmetrical encryption shall be AES or Serpent. The hash function shall be SHA-2, SHA-3 or Whirlpool.

The periodic conformity assessments of identification services and the preparatory work for the Regulation have revealed that in addition to the algorithms and hash functions listed in the current Regulation there are other widely used newer alternatives that are sufficiently secure. Preparations are underway to amend the Regulation to also allow the encryption algorithm ChaCha20 and authentication code Poly1305.

When supervising conformity with the encryption requirements of identification services, Traficom will not interfere with the use of the ChaCha20 algorithm and Poly1305 authentication code or require that they be abandoned.

5 Themes that require particular attention in periodic assessments

5.1 Description of identification means

The assessment report must include a description and/or documentation of the identification means and the authentication mechanism. The descriptions must have sufficient technical detail that conclusions on all matters relevant for the assessment can be drawn based on them. The specification documents must also cover all subcontractors.

– What are the authentication factors used in the identification means (a minimum of two from different categories are required)?

– How is their independence of each other ensured?

– How are the authentication factors connected to the holder of the identification means?

– What is the authentication method used (technical specification of how the identification events are implemented)?

The assessment report must also specify the product or service names used by the users and the eServices to identify the services. It is also recommended to include the names used internally in the identification service, if they are used in the assessment report or in the documentation of the identification service.

5.2 Subcontracting

Section 15 of Traficom's regulation M72 sets the assessment criteria for identification services. The assessment must cover the identification service in its entirety.

This means that the identification service provider must also assess its entire subcontracting chain and its conformity. The service provider must identify all of its subcontractors and evaluate their roles in the implementation of the identification scheme.

A subcontractor organisation's own certificates (e.g. ISO 27001) can be taken into account, but the assessment must consider the scope and applicability of such certificates with respect to the functions involved in the implementation of the identification scheme. The mere acceptance of certificates is usually not sufficient to cover all elements; therefore, the identification service provider has the obligation to ensure that periodic assessments include an assessment of the conformity of its subcontractor network.

If a material change in the operations occurs, an assessment must be carried out, and a notification of the change and an assessment report must be submitted before the change is transferred to production. Examples of material changes include also the changes in or replacement of subcontractors that supply maintenance services, hardware, systems or software.

5.3 Descriptions of architecture

As a rule, the 2019 periodic assessment reports submitted to Traficom included comprehensive descriptions of architecture.

The report must include a figure, a diagram or another clear presentation of the identification system'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 description must also cover all subcontractors.

- The system architecture description must indicate all system components related to identification operations.
- Based on the report, 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.
- 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.

5.4 Technical observation

Section 2.5.2 of the assessment guideline discusses methods that can be used in the assessment. In addition to an audit of documentation, interviews and on-site observations, the periodic assessment report must also be accompanied by reports on technical observation.

5.5 SDKs for mobile identification applications

Many mobile identification applications have been implemented by purchasing from the market an SDK for the identification element that is connected to a larger entity (e.g. online banking application) or integrated into the identification service provider's own identification application. The SDK is an essential part of the identification means and should therefore also be assessed. The assessment can be carried out with the assessment criteria for mobile identification solutions published by Traficom, but conformity can also be proven with a third-party assessment report provided by the manufacturer. In the latter case, Traficom must also be provided with the details of the assessment method used, the organisation that carried out the assessment and the version assessed (and whether the assessed version is the one used in the identification application).

6 Reports to Traficom and Excel template

Traficom has prepared an optional model for a reporting table. To ensure the ease and smoothness of periodic assessments, the table is highly recommended for the 2021 assessments. The optional table also makes it easier for identification service providers to tender assessments out and to ensure that all necessary parts are assessed. The table is based on the assessment criteria set out in the Traficom Guideline 211/2019 O.

Traficom underlines that the more comprehensive assessment reports and their accompanying documents it receives, the quicker it can inspect the periodic assessment. If shortcomings are detected in the assessment report, the identification service provider must provide comprehensive details of the planned corrective measures and their schedule.