Advisory memorandum for the periodic assessments of identification services in 2023

General

In this memorandum, the Finnish Transport and Communications Agency (Traficom) highlights different themes for commissioning/conducting the 2023 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.

Legal framework

Section 29 of the Act on Strong Electronic Identification and Electronic Trust Services (617/ 2009, hereinafter referred to as 'the Identification 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 specified 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 Commission Implementing Regulation (EU) 2015/1502 (hereinafter referred to as 'the Assurance Level Regulation') and the Annex to the Regulation.

Section 15 of Traficom Regulation M72B/2022 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-declaration.

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 M72B or a combination of these criteria.

Deadlines

The deadline for submitting assessment reports and their accompanying documents to Traficom is 31 December 2023.

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

Use of other assessments or certificates

If the identification scheme has been assessed in 2022 and 2023, these assessments can be used as part of the periodic assessment and the relevant parts of the assessment do not need to be repeated if the assessed entity has not changed since the previous assessment. The assessments must be submitted to Traficom even if they have already been provided in connection with a previous change notification.

Certificates can be accepted insofar as they comply with the provisions of the Identification Act and Regulation M72B. Traficom must be provided with information detailing the parts of the identification service assessment covered by the certificate and explaining how the certificate's compliance with the Identification Act and Regulation M72B/2022 has been assessed.

Themes that require attention in the 2023 periodic assessment

Auditor's observations and corrective measures

If any nonconformities that must be immediately addressed are detected in the assessment, they must be included in the material submitted to Traficom. The operator must record the auditor's observations in an Excel file to be submitted to Traficom and respond to the observations in the file.

If the necessary corrective measures are feasible, they should be implemented without delay and addressed in the material submitted to Traficom. If the assessment report includes shortcomings detected in the assessment and corrective measures cannot be taken immediately, the identification service provider must provide comprehensive details of the planned corrective measures and their schedule.

The aim is to avoid having to include in the decision on the periodic assessment matters that have already been recognised by the auditor and recorded as "to be corrected". The operator is already aware of these observations.

Assessment duration and scope

The assessment must cover the entire identification scheme. It must also include technical samples (technical observation).

The scope of the audit must determine the extent and limits of the audit, such as the places of business, organisational units, information systems, functions and processes audited. Audits may employ sampling. This means, for example, that all places of business do not have to be audited during each assessment round. If the audit as a whole includes more than one individual audit, the whole audit process must nonetheless cover the entire identification scheme.

Required corrective measures recorded in the decision and assessment of the measures

If Traficom's decision on the periodic assessment includes critical nonconformities that require corrective measures to be taken as soon as possible, these measures must be implemented and verified in accordance with assessment practices. Traficom must be provided with a finalised response without accompanying documents by the deadline set by Traficom. The evidence verifying corrective measures should also include a statement by the auditor.

The objective is that the requested corrective measures have been implemented or a plan has been drawn up for corrective measures and Traficom is provided with a related response. Service providers should not provide Traficom with separate accompanying documents that would require Traficom to undertake another assessment when reviewing the corrective measures.

Termination plan

Under the Identification Act, an identification service provider must have in place an effective plan for terminating the identification service. The purpose of the plan is to assist the service provider if the provider needs to make changes to or terminate its service. The level of detail in the plan is less relevant; instead, it is important that the measures and steps required are planned and listed.

The plan should focus on, for example, how to carry out the possible shutdown of systems, how and when to inform users, the trust network and relying parties about terminating the service, and how to ensure the storage of information in accordance with section 24 of the Identification Act after terminating the service. The termination plan must be dated and up to date.

Risk assessment

An identification means must be based on a risk assessment, which must be included in the assessment report. The risk assessment must prove that the means and the related risk management features meet the requirements of the level of assurance (LoA) 'substantial' (e.g., a list of one-time passwords, operating system version supported by a mobile terminal). Suitability can be proven by calculating attack potential.

Reports to Traficom and Excel template

Traficom has prepared a model for a reporting table. To ensure the ease and smoothness of periodic assessments, it is highly recommended to use the table in connection with periodic assessments to support the verbal assessment report prepared by the assessment body or as an appendix to the report.

The table also makes it easier for identification service providers to put assessments out to tender 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. Both the table and the Guideline 211 will be updated over the course of spring 2023. If assessments are underway before the new guidelines are published, operators must ensure that the amendments made to Regulation M72B are taken into account in the assessment.

Traficom underlines that the more comprehensive assessment reports and their accompanying documents Traficom receives, the better it can inspect the periodic assessments. Deadlines must also be met in order to standardise assessment round schedules and to ensure that the deadlines set for corrective measures are equal and fair for all operators.