Announcement to e-services using identification services

The purpose of this announcement is to improve the display of the correct electronic service name during an authentication flow and prevent the misuse of strong electronic identification.

The Finnish Transport and Communications Agency Traficom requires identification service providers to ensure that the authentication requests are not accepted without digital signature and that the validity of the digital signature is verified.

Traficom also requires that the name of the e-service being authenticated to is displayed to users as clearly and descriptively as possible.

1 Presentation of the correct e-service name (SP name)

Traficom's Regulation on Electronic Identification and Trust Services M72 (Traficom/245890/03.04.05.00/2020, entered into force 1 June 2022) requires that users must be presented with the name of the relying party, i.e. the e-service to which the user is authenticating.

Based on the information provided by the identification means provider, the user is able to connect an e-service transaction to an authentication flow and will not confirm unauthorized authentication requests.

For this purpose, e-service owners must update the name that describes their e-service and that they want the user to see. Adding/updating the name can be discussed with the party forwarding the identification, i.e. typically the provider of the identification broker service.

2 Request object and digital signature

The providers of identification broker services must require their customers to use digitally signed authentication request (the so-called request-object in the OIDC protocol).

This means that the digital signature of authentication request is verified and only approved requests are forwarded to provider of the electronic identification means.

Existing e-services must check that the authentication requests comply with the obligations of the Regulation and, if necessary, fix the

implementation if the signing of identification requests has not been implemented by 31 December 2025.

3 Objectives

Regarding the presentation of the name of the e-service, the objective is to improve the security of the e-service user so that the user understands which service he or she is logging into throughout the authentication flow.

The deadline for meeting the requirement has passed. Therefore, Traficom will monitor compliance with this obligation during 2026 with an enhanced focus.

Regarding authentication requests, the objective is that an authentication flow cannot be initiated from a fraudulent website, appearing to represent a known and trusted e-service. Another goal is to prevent data from being changed and to ensure the origin and accuracy of the information presented.

The protection requirement applies equally to connections between identification service providers and between identification broker service and relying party.

The deadline for meeting the requirement has passed. Therefore, Traficom will monitor compliance with this obligation during 2026 with an enhanced focus.

4 Background

Traficom is the supervisory authority for strong electronic identification in Finland. Service providers established in Finland must submit a written notification to Traficom before starting operations. Traficom monitors compliance with the requirements, issues regulations specifying the law, and maintains a public register of identification service providers that meet the requirements.

5 Regulation

The requirement is based on the Traficom Regulation that entered into force 1 June 2022. The Regulation imposes obligations on the providers of identification and trust services and ensures the security and interoperability of the services. From the perspective of the customers of identification and trust services, the Regulation ensures information security and privacy protection. Traficom monitors compliance with the Regulation.

Finnish Transport and Communications Agency's Regulation on Electronic Identification and Trust Services, Traficom/245890/03.04.05.00/2020

6.2 Specific security measures

6.2.2

The identification service must present the identification means user with information concerning the relying party, for whom the identification is carried out, during the identification event. This information must be presented in identification means that have the technical ability to do so.

9.1 Protecting messages between identification services and relying parties

9.1.1

The integrity and confidentiality of authentication messages containing personal data must be protected in communications between identification services and between identification services and relying parties [...]

9.1.2

Authentication messages between identification broker services and relying parties must be authenticated with signatures.

6 More information

National Cyber Security Centre Finland (NCSC-FI) at the Finnish Transport and Communications Agency Traficom

https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/electronic-identification

Finnish Transport and Communications Agency's Regulation on Electronic Identification and Trust Services, Traficom/245890/03.04.05.00/2020

https://www.finlex.fi/fi/viranomaiset/normi/480001/48237

Contact

eidas@traficom.fi