# The Finnish Transport and Communications Agency's interpretation memorandum on separating strong and unregistered electronic identification services

## Table of Contents

# 1 Purpose and content of the interpretation memorandum

## 1.1 Background and revision 2020-2021 of the previous 2017 interpretation memorandum

On 3 October 2017, the Finnish Communications Regulatory Authority (FICORA) published an interpretation memorandum on the provision of strong and weak identification services (reg. no. 657/620/2017). The purpose of the memorandum was to provide proactive advice on the interpretation of the Act on Strong Electronic Identification and Electronic Trust Services (617/2009, hereinafter "the Identification Act") in situations where the provider of a strong electronic identification service also provides weak electronic identification.

In 2017, operators' questions of interpretation were primarily associated with whether, in certain situations, identification provided by banks are allowed to be non-compliant with the requirements for strong electronic identification in the interface for online services.

In 2020, the Finnish Transport and Communications Agency (Traficom) prepared a new elaborated interpretation memorandum. As a result of the development of electronic identification services, it has become necessary to specify the interpretation of what type of separation between strong and unregistered electronic identification is sufficient considering the Identification Act. Current questions are particularly related to mobile applications and the upgrading of unregistered identification means to strong identification.

Here, the previously used term "weak identification" has been replaced by "unregistered identification", which better represents the situation, because the question is that the means has not been notified to a register pursuant to the Identification Act within the scope of official supervision.

On 27 March 2020, Traficom requested statements on the draft version of the memorandum. A summary of the statements and any revisions made on the basis of them are attached to this memorandum.

## 1.2 Proactive advice on regulated requirements

The legal nature of this memorandum is to provide advice. This means that in supervisory procedures the obligations are interpreted on the basis of case-specific facts and the provisions of the relevant act and regulation. The memorandum clearly indicates when the question is Traficom's opinions in the interpretation of requirements and when a recommendation is in question.

The requirements set in regulations on strong electronic identification apply to all identification service providers registered with Traficom and their strong identification services. The interpretation of the law will equally apply to all current and also future Finnish and non-Finnish identification service providers registering in Finland.

The purpose of the memorandum is to provide operators with proactive advice on how Traficom interprets the obligations laid down in the Identification Act in a situation where a single identification service provider provides strong and unregistered electronic identification side by side. The memorandum examines the sufficient separation of strong and weak electronic identification means and the identification scheme that provides them, considering the requirements of the act, so that:

- users of identification means and parties relying on identification can clearly distinguish the strong identification used from unregistered identification
- the provision of unregistered identification does not technically corrupt the implementation of the strong electronic identification scheme.

While the advisory memorandum presents examples, it is not possible or purposeful to foresee and define advisory questions regarding all current and future technical implementations.

The most typical example, in which advice has been requested from Traficom, is the provision of identification means based on a single mobile identification app using initial identification procedures with different assurance levels. Therefore, the examples concern such a situation and, in particular, upgrading the level of the mobile app from unregistered to strong identification means. The same principles also apply to other identification means.

### 1.3 Supervision and registration in guaranteeing the reliability of a strong electronic identification service

The reliability requirements laid down in the Identification Act apply to an identification service that has been notified and entered in Traficom's register in accordance with the Identification Act. The reliability of strong electronic identification is partly based on official supervision. All requirements of the Identification Act apply to notified identification services as a whole.

A single service provider may provide both strong and unregistered identification. A company or organisation may, the Identification Act notwithstanding, provide a strong electronic identification service as a notified service and an unregistered identification service outside the scope of the Identification Act's provisions.

In the light of the Identification Act, the same identification means cannot be provided with two different statuses as strong and unregistered. Instead, the means must be sufficiently separated.

Users of identification means and parties relying on strong electronic identification must be able to trust that the identification services of identification service providers entered in Traficom's register fulfil all requirements set for identification services. Users and relying parties must be able to distinguish strong and unregistered identification means and methods.

Any exemptions set out in the section 1 of the Identification Act to the applicability of the requirements on the services of an identification means provider cannot reduce the reliability of a notified identification service which is to be provided for the general public.

The assessment of the clarity and reasonability of the agreement terms and conditions is within the scope of general consumer protection regulations and the powers of the Consumer Ombudsman.

The Data Protection Ombudsman is the supervisory authority for the processing of personal data.

The Financial Supervisory Authority supervises banking and payment services.

### 1.4 A legal policy goal to increase the use of strong identification

Legal policy factors are not legal interpretation grounds when assessing whether a service meets the requirements set for it. Here, Traficom brings forth goals set out in the legislation.

The Government proposal (36/2009, pp. 7–11) refers to the national guidelines prepared by the 2008 electronic identification development group for strong electronic identification. The goal of the guidelines is, for example, to also promote the use of strong identification in services that may not require strong identification:

> *Also in services that may not necessarily require strong identification, the ultimate goal is that users can use familiar and easy-to-use strong identification means. To this end, the cost level of a strong identification event must be sufficiently low for all operators. One goal of a well-functioning market is to maintain a reasonable price level, which is possible if sufficient options are available on the market. However, even though the goal is that each user can use the selected strong identification means in as many services as possible, service providers cannot be forced to accept certain means or strong electronic identification service providers.*

According to Traficom's understanding, this goal remains topical. The serious personal data breach targeted at psychotherapy services in 2020 shocked Finnish society at large and initiated extensive public debate in Finland regarding the need to increase the use of strong electronic identification in private sector services. In assessing the needs to revise the EU eeIDAS regulation, the European Commission has also highlighted the need to increase the use of electronic identification in the private sector.

## 2 Terms

**Strong electronic identification or identification means** refers, in this memorandum, to identification, the provision of which has been notified and approved in an identification service register in accordance with the Identification Act. The compliance of a strong identification service with requirements has been assessed, and it is supervised in accordance with regulations. The assurance level of the service may be substantial or high.

**Unregistered or weak identification service or identification means** refers, in this memorandum, to an electronic identification service that has not been notified in a register in accordance with the Identification Act. Therefore, the reliability of the unregistered identification service has not been assessed, and is not supervised in accordance with regulations.

**Identification means provider** provides identification means for the general public, i.e. users, and provides their identification means for an identification broker service provider for forwarding in a trust network.

**Identification broker service provider** forwards identification events (delivers authentication) to relying parties, i.e. electronic service providers.

**Identification means holder** is a natural or legal person to whom the identification service provider has issued an identification means based on an agreement. In this memorandum, "holder" is mainly referred to as "user".

**Relying party** is a natural or legal person who relies on electronic identification. Relying parties include services that acquire the electronic identification of their customers from an identification broker service.

**Electronic identification means** refers to the devices and methods of authentication in regulations: a material and/or immaterial unit containing personal identification data, and which is used for authentication for an online service. An identification means is based on **authentication factors** that are related to the user's knowledge, physical attribute or possession, and on **a dynamic authentication mechanism** which guarantees the uniqueness of each identification event.

**Identification scheme** refers to a system, within the scope of which electronic identification means are granted and provided for users. The identification scheme covers an identification service provider's technical systems, information security management and other regulated reliability requirements. The identification scheme also covers all subcontracted parts and functions that are associated with the provision of an identification service.

At the time of preparing this memorandum, identification means providers include banks, mobile telecommunications operators and the Digital and Population Data Services Agency. Some of these also act as an identification broker service. In addition, the register includes two operators that only provide an identification broker service.

# 3 Provisions and Traficom's opinions

## 3.1 Reliability and scope of application of the provision of strong electronic identification based on the law

### 3.1.1 Provisions

According to section 1 of the Identification Act (617/2009 as amended), the act lays down provisions on strong electronic identification and on the offering of identification services to service providers, the general public and other providers of identification services. The act does not apply to the provision of identification services within an organisation. Neither does the act apply to services where an organisation uses its own identification means for the identification of its own customers in its own services.

According to section 10 of the act, an identification service provider who intends to offer services shall, prior to the commencement of such services, submit a written notification to the Finnish Transport and Communications Agency, and provide the information on the service provider and service as laid down in this section. According to section 11 of the act, the notification may also be submitted by an identification service provider based in the European Economic Area.

According to section 12 of the act, the Finnish Transport and Communications Agency maintains a public register of identification service providers who have submitted a notification according to section 10, and their services.

According to section 14 of the act, the identification service provider shall have identification principles in place that define how the provider will perform its obligations set out in this act. The identification service provider shall keep the identification principles updated and in a generally accessible location.

Government proposal 36/2009 states the following:

> *The existence of a register is one of the cornerstones of the planned arrangement. A person acquiring identification means, often a consumer, and a service provider acquiring an identification service have to answer the question what identification service provider they can trust. The public register on Finnish Communications regulatory authority's website gives easy access to information on the service providers that can initially be expected to follow the provisions laid down in this act and that are supervised by the authorities.*
>
> *…*
>
> *The majority of electronic services do not require electronic identification or electronic signatures. However, different legal actions, for example, can be carried out in some electronic services. These electronic services require a relationship of trust between the parties. The service user must be able to trust that the service provider has, when building its service, taking into account the requirements of information security and privacy protection. The service provider must, in turn, be able to trust that the remotely connected service user is who they claim they are. Therefore, the development and use of electronic services require well-functioning electronic identification services.*

The justification in section 12 a of Government proposal 272/2014 states the following:

> *An identification service can also be provided without submitting a notification to Finnish Communications regulatory authority, but in this case the identification service provider does not have the position of a strong identification service provider. Identification service providers operating in trust networks must comply with the regulations that lay down provisions on strong electronic identification and [electronic signatures], such as the general obligations of an identification service provider.*

### 3.1.2 Traficom's opinion

On the basis of the Identification Act and its justification, Traficom sees that reliability requirements apply to identification services notified to Traficom and published in the register as a whole and that the reliability of strong electronic identification is partly based on official supervision.

A situation where a factually same identification means is provided with two different statuses cannot legally be separated from a situation where defined requirements are not complied with (example: providing the strong identification of customers for a service without the encryption required). Requirements for strong electronic identification apply, in any case, to the provision of a strong electronic identification service.

It is a different situation where the Identification Act does not apply, based on the exemption permitted by section 1 of the act, to the use of an organisation's own identification means to identify its own customers in its own services. Therefore, the requirements laid down in the Identification Act for an identification service notified to a register in accordance with the Identification Act do not need to be complied with in the services of an identification service provider. Such exemptions cannot reduce the reliability of a notified identification service provided for the general public.

For example, online banking credentials can be provided for the general public as strong electronic identification means as laid down in the Identification Act, and the same identification means can, based on the exemption permitted by the act, be used as limited online banking credentials to identify the bank's own customers in

the bank's own services without complying with all the requirements laid down in the Identification Act in these service situations.

The Financial Supervisory Authority supervises banking and payment services.

## 3.2 Initial identification and upgrading unregistered identification means to strong identification means

### 3.2.1 General

**"Initial identification"** means the procedures that are used to verify the identity of an applicant for identification means to ensure that strong electronic identification means are certainly issued for the correct person and are in the possession of the correct person.

**Trusted sources and initial identification.** Section 17 of the Identification Act lays down optional procedures and trusted sources accepted in Finland, on which the proofing of identity can be based. Trusted sources are defined nationally. In the Identification Act, initial identification procedures correspond to the procedures laid down in the EU Assurance Level Regulation. Trusted sources include passports and identity cards issued by the authorities.

In place of showing a passport or identity card, initial identification can also be based on other strong electronic identification means, initial identification by the police for issuing identification means or other procedure based on the law, which is separately approved by Traficom.

In addition, the identity must be verified from the Population Information System. Therefore, strong electronic identification means is always based on an identity guaranteed by the state.

**Remote identification.** Currently, questions of interpretation are related, on a European scale, to how reliably the identity of an applicant for identification means can be proven and verified from official identity documents using an electronic procedure. Traficom has summarised the viewpoints to be examined in section 3.10 of assessment guidelines for electronic identification services (211/2019 S). Traficom is monitoring international debate and will elaborate the interpretation.

**Upgrading the assurance level of identification means.** There may also be questions of interpretation regarding how unregistered electronic identification means can be upgrated to strong electronic identification means. In the provision of mobile apps, in particular, many operators are planning to deploy their app as an unregistered identification means without the initial identification laid down by law and to later upgrade the app to a strong identification means when reliable initial identification is carried out.

In the example situation, a similar mobile app is available to users using two different issuance procedures.

- The lighter issuance procedure does not meet the Identification Act's initial identification requirements, and a notification of the provision based on this procedure is not notified to the identification service register.
- By means of initial identification, which meets the regulated requirements, a user can upgrade the assurance level of their identification app to a strong level, and a notification of this issuance procedure and the provision of an identification service must be submitted to the identification service register.

3.2.2 Traficom's opinion

**The issuance of strong electronic identification means must always be based on an initial identification procedure and sources required by law.**

Initial identification can be based on the verification of identity using strong electronic identification, the showing of a passport or identity card when visiting a service location, or using reliable remote identification. When showing a passport or identity card, it must be ensured that the document is genuine and belongs to the person showing it.

**Unregistered identification means can be part of the issuance of strong identification means and initial identification, i.e. the verification of the applicant's identity.**

Unregistered identification means and the verification of identity used in conjunction with their issuance alone cannot form the basis of strong initial identification. However, they can be part of the process of issuing strong identification means and initial identification, i.e. the verification of the applicant's identity.

**The procedure must address, already at the substantial level of assurance, the risk that an unregistered identification means and a passport or identity card may have been misplaced, or that the passport or identity card may have been forged.**

For example, an app may have originally been deployed using incorrect personal data, a mobile device may have been misplaced or an unauthorised instance of an app may have been generated for a third party.

**Upgrading/converting an unregistered identification means and its authentication factors (such as banking credentials or a mobile app) into a strong identification means requires such additional verifications that the requirements set out for verifying the identity of an applicant for strong identification means can be assessed to be fulfilled as a whole.**

Additional verifications must ensure that an unregistered identification means upgraded/converted into a strong identification means is and remains in the possession of the correct applicant.

The **overall assessment** can consider the following:

- the reliability of verifying the authenticity of a passport or identity card
- verifying the validity of a passport or identity card
- comparing the applicant's physical attributes to the identity document shown
- different additional controls, such as questions regarding factors that only the genuine applicant can know
- notifying the holder after the issuance using different channels
- monitoring, identifying any non-conformities and reacting to them
- verifications made when issuing, delivering and using unregistered identification means
- verifications related to the delivery procedure when upgrading the assurance level

3.2.3 Provisions

***Section 8 of the Identification Act (29 June 2016/533), Requirements posed on the electronic identification scheme***

*An electronic identification scheme must fulfil the following requirements:*

*1) The identification means shall be based on initial identification according to section 17 and section 17 a, where the relevant data can be verified afterwards as set out in section 24;*

*2) The identification means can be used for unambiguously identifying the holder of the identification means in a way that, at a minimum, fulfils the requirements on assurance level substantial laid down in sections 2.1.2, 2.1.3 and 2.1.4 of the Annex to the Commission Implementing Regulation (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of 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, hereinafter the Act on Level of Assurance in Electronic Identification.*

*[…]*

***Section 17 (23 November 2018/1009), Identifying a natural person applying for an identification means***

*The initial identification of a natural person shall be made personally or electronically in a way that fulfils the requirements for assurance level substantial or high laid down in section 2.1.2 of the Annex of the Act on Level of Assurance in Electronic Identification. The proofing of a person's identity may be based on a document issued by an authority showing the person's identity or a strong electronic identification means referred to in this Act In addition, the proofing of an identity may be based on a procedure used at an earlier date by a public or private entity for a purpose other than the issuing of a strong electronic identification means, which the Finnish Transport and Communications Agency approves pursuant to regulations and regulatory control on the procedure or pursuant to a confirmation by a conformity assessment body referred to in section 28, subsection 1.*

*In initial identification that is solely based on a document issued by an authority showing the person's identity, the only acceptable documents are a valid passport or a personal identity card issued by an authority of a member state of the European Economic Area, Switzerland or San Marino. If the identification means provider so desires, they may also verify the identity from a valid passport granted by an authority of another state.*

*If the identity of an applicant cannot be reliably established, the police will perform the initial identification for the application. Expenses incurred to the identification means applicant by the initial identification performed by the police are expenses of a service under public law. Provisions regarding charges levied for the service are issued in the Act on Criteria for Charges Payable to the State.*

*[…]*

***Section 7 of the Identification Act (20 February 2015/139)**, **Use of data stored in the Population Information System***

*The provider of an identification means and a certification service provider offering a trust service must use the Population Information System to obtain and update the data they need in order to be able to offer a service for identifying a natural person. The identification service provider shall also ensure that the data it needs for the purpose of offering identification services are up-to-date with the data in the Population Information System.* (29 June 2016/533)

*[…]*

## 3.3 Separating strong and unregistered identification means in the user's identification means

### 3.3.1 General

**User authentication factors.** The use of identification means and the authentication method includes authentication factors detectable by the user, and

the technical implementation of authentications mechanism not detectable by the user.

This section examines the characteristics that are detectable by the user, on the basis of which the user can distinguish one identification means from other identification means and, therefore, strong identification means from unregistered identification means. Therefore, the question is of differences, on the basis of which the user can clearly understand that they are using different identification means in electronic services, involving a different level of regulatory protection.

**Productisation.** Traficom states that the Identification Act does not, naturally, lay down any express provisions on productisation or branding, and interpretation must be based on as objective general assessment and feasibility as possible. The requirements set by the operating environment characteristic to electronic identification means must be considered because, for example, the use of a OTP device , web browser, mobile app and chip card differs from one another.

**Common practices of identification services.** Traficom also states that in productisation it would be desirable to seek to find good common practices in cooperation between trust network's identification services that all identification service providers could act similarly to separate strong and unregistered identification. This would improve the ability of users to understand differences in identification services and rely on strong identification.

### 3.3.2 Traficom's opinion

**Traficom sees that the separation of strong and unregistered identification means must consider the following characteristics detectable by users:**

1) **The names of identification means must be sufficiently different.**
2) **The visual appearance of identification means must be sufficiently different.**
3) **Authentication factors of different categories can be considered to be used in strong and unregistered identification means if this is technically feasible.**
4) **Users' opportunities to store strong identification means with care must be protected.**
5) **Accessibility must be considered.**

Traficom sees that the separation of strong and weak identification means must consider the following characteristics detectable by users:

**1) The names of identification means must be sufficiently different.** Identification products of completely different names help to sufficiently distinguish strong identification means. However, if the product names of strong and unregistered identification means need to be largely the same, strong means must be separated by a clearly understandable and distinguishing part of a name or an addition to the name. Persons with disabilities should be considered regarding the separation of names.

**2) The visual appearance of identification means must be sufficiently different.** Different logos, colours, words and other visually distinguishing features can be used. Persons with disabilities should be considered so that separation by visual means alone cannot be regarded as sufficient.

**3) Authentication factors of different categories can be considered to be used in strong and weak identification means if this is technically feasible.**

Feasibility can cover the operating environment and usability.

In regulations, authentication factors have been divided into the following categories:

- a possession-based authentication factor
- a knowledge-based authentication factor
- an inherent authentication factor that is based on a physical attribute of a natural person

Traficom sees that different knowledge-based authentication factors (such as a PIN code or other password) can always be used in strong and unregistered identification means. The use of authentication factors of the same authentication factor category is therefore acceptable. An identification means provider can consider the definition of different PIN codes or passwords when providing strong and weak identification using a single identification app, for example. On the basis of the clarification of identification service providers, it is, however, justifiable to consider observations whether users can handle different PIN codes or passwords in such uses.

A possession-based authentication factor (such as a password/OTP device, a list of OTP passwords, a mobile app or a SIM card) may be separable, while there may be technical feasibility issues in the implementation of separation, and there may be a negative impact on the usability of the means.

An inherent authentication factor (a fingerprint, facial image, etc.) can be separated, for example, so that no biometric factor is used in either means, different attributes are used in both means or a combination of several biometric attributes is used in strong means. Any observations of the typical behaviour of users should also be considered here.

**4) Users' opportunities to store strong identification means with care must be protected.**

Section 23 of the Identification Act lays down the obligations of identification means holders to store their identification means with care and not to make the use of their means available to any other person.

Traficom sees that the characteristics of strong and unregistered identification means should be defined considering users' opportunities to store their identification means with care in accordance with the obligation laid down in the act so that the use of unregistered identification means does not endanger the factors of strong means only remaining in the possession and use of the user.

**5) Accessibility**

Certain requirements laid down in the Act on the Provision of Digital Services (306/2019) apply to providers of strong electronic identification services. According to section 2, subsection 4, *accessibility means the principles and techniques that must be followed in the design, development, maintenance and updating of digital services to make them better accessible to users, especially persons with disabilities*.

The requirements laid down in the act are associated with international standards regarding web browsers and mobile apps.

Traficom does not supervise the act but, in this context, advises to consider any impact of the requirements laid down in the Act on the Provision of Digital Services on separation. Traficom also sees that any users with disabilities must be able to identify whether they are using strong or unregistered identification means.

3.3.3 Provisions

***Section 8 a of the Identification Act (29 June 2016/533)*, *Authentication factors used in the identification means***

*The identification means must use at least two of the following authentication factors:*

*1) a knowledge-based authentication factor that the subject is required to demonstrate knowledge of;*

*2) a possession-based authentication factor that the subject is required to demonstrate possession of;*

*3) an inherent authentication factor that is based on a physical attribute of a natural person.*

*[…]*

***Section 8 of the Identification Act (29 June 2016/533)*, *Requirements posed on the electronic identification scheme***

*An electronic identification scheme must fulfil the following requirements:*

*[…]*

*3) The identification means can be used verify that only the holder of the identification means can use the means in a way that, at a minimum, meets the conditions for assurance level substantial laid down in sections 2.2.1 and 2.3 of the Annex to the Act on Level of Assurance in Electronic Identification.*

*[…]*

*[…]*

## 3.4 Technical requirements for the authentication mechanism and identification scheme

3.4.1 General

Sections 8 and 8 a of the Identification Act and section 2.3 of the annex to the EU Assurance Level Regulation define that identification means can only be used by the identification means holder and that the authentication mechanism must withstand an attack of a severity level defined in accordance with the assurance level. Section 23 of the Identification Act lays down the user's obligation to store their identification means with care.

The requirements set for the authentication mechanism are particularly targeted at secrets of different levels related to identification means. The specifications set out in section 6 of Traficom Regulation 72 are also related to this.

Otherwise, requirements set for the identification scheme are laid down in section 13 of the Identification Act, and sections 2.4.4 (Record keeping), 2.4.5 (Facilities and staff) and 2.4.6 (Technical controls) of the EU Assurance Level Regulation. The requirements are specified in Traficom Regulation 72 in section 5 (Technical information security measures of the identification scheme) and section 7 (Encryption requirements of the identification scheme and interfaces).

Not all requirements are intended to be described in this memorandum. However, references to key reliability provisions are presented under "Provisions".

3.4.2 Traficom's opinion

**Protection of secrets in strong electronic identification means covers secrets known by the user and secrets associated with the characteristics of the means.**

Connecting authentication factors of strong identification means to a person who has passed a strong initial identification must particularly address the security of the secret (private key) of the authentication factors and the authentication mechanism.

A secret related to identification means is typically a private signature key that is invisible to the user, related to the PKI implementation of a mobile certificate and saved on a SIM card or a private key of a mobile app that is saved in a mobile device's protected SE or TEE component.

**The implementation of the identification means and the authentication mechanism must ensure the protection of the secrets used in the authentication mechanism of strong identification means in all phases of the lifecycle of the identification means.**

**The parallel provision of an unregistered identification means cannot, in any way, reduce the protection of the secrets of strong identification against an attack of a severity level in accordance with the assurance level.**

Traficom sees that, if an identification means issued through weak initial identification is upgraded to a strong means through initial identification in accordance with the law, special attention must be paid to ensuring that the secrets used in the identification means and the authentication mechanism are created and that they are stored with care in accordance with the requirements set for strong identification.

Furthermore, Traficom sees that, if the processing of key data/secrets in a mobile app used in an unregistered identification means does not fulfil the requirements set for a strong identification means, a new private key/secret must primarily be created in the strong identification means.

Traficom considers that at least a secret saved in an SE or TEE component is so reliably protected that the use of the same secret can be considered in both strong and unregistered identification means. However, the security of the secrets must be assessed as a whole, considering available security controls.

Traficom sees that the protection of the authentication mechanism and secrets must be ensured in the entire identification scheme, i.e. also in the background systems that affect the reliability and attack resilience of the identification so that the provision of unregistered identification does not endanger the protection of strong identification means. The following, among other things, must be considered in the identification scheme:

- The connection of authentication factors to the user in the background system
- The technical implementation of authentication factors
- The storage of data
- The management of access to the scheme and data
- Interface encryption and connection practices

3.4.3 Provisions

***Section 8 of the Identification Act (29 June 2016/533). Requirements posed on the electronic identification scheme***

*An electronic identification scheme must fulfil the following requirements:*

*[…]*

*4) The identification scheme is reliable and safe so that, at a minimum, it meets the conditions for assurance level substantial laid down in sections 2.2.1, 2.3.1 and 2.4.6 of the Annex to the Act on Leve of Assurance in Electronic Identification and takes into account the threats to the information security of the technology available at the time, and that the premises used for providing an identification service are safe in compliance with the provisions laid down in section 2.4.5 of the Annex to the Act on Level of Assurance in Electronic Identification.*

*5) Information security management is ensured so that, at a minimum, the conditions for assurance level substantial laid down in the introduction to section 2.4 and in sections 2.4.3 and 2.4.7 of the Annex to the Act on Level of Assurance in Electronic Identification are met.*

*[…]*

***Section 8 a of the Identification Act(29 June 2016/533)**, **Authentication factors used in the identification means***

*The identification means must use at least two of the following authentication factors:*

*[…]*

*Every identification means must use a dynamic authentication referred to in section 2.3.1 of the Annex to Act on Level of Assurance in Electronic Identification that changes in every new authentication event between the person and the system certifying his or her identity.*

***EU Assurance Level Regulation, Annex, 1. Applicable definitions***

*(3) 'dynamic authentication' means an electronic process using cryptography or other techniques to provide a means of creating on demand an electronic proof that the subject is in control or in possession of the identification data and which changes with each authentication between the subject and the system verifying the subject's identity;*

***Section 13 of the Identification Act, General obligations of an identification service provider***

*The storage of data, the personnel and subcontracted services used by an identification service provider in association with identification shall, at a minimum, meet the requirements laid down for assurance level substantial in sections 2.4.4 and 2.4.5 of the Annex to the Act on Level of Assurance in Electronic Identification. Moreover, the identification service provider shall have in place an effective plan for terminating the identification service. (29 June 2016/533)*

*[…]*

***Section 23 of the Identification Act, Obligations of the identification means holder***

*The identification means holder shall use the means according to the terms and conditions of the agreement. The holder shall store the identification means with care. The holder's duty of care for the identification means starts with its acceptance.*

*The identification means holder shall not make the use of the means available to any other person.*

***EU Assurance Level Regulation, Annex, 2.3.1 Authentication mechanism***

*LOW*

*[…]*

*2. Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline.*

*[…]*

*SUBSTANTIAL*

*Level low, plus:*

*1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication.*

*2. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.*

*HIGH*

*Level substantial, plus:*

*The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.*

***Traficom Regulation M72, section 6, Information security requirements of the identification means***

*An identification means shall not be connected to an applicant before the applicant has passed initial identification or it has been otherwise ensured in the process of granting an identification means that the identification means is not available before the initial identification referred to in section 17 of the Identification and Trust Services Act has been performed.*

*The service provider shall ensure that secret information related to the identification device are not revealed to its staff under any circumstances.*

*The service provider shall not make copies of any secret information related to the identification means.*

***Section 13 of the Identification Act, General obligations of an identification service provider***

*The storage of data, the personnel and subcontracted services used by an identification service provider in association with identification shall, at a minimum, meet the requirements laid down for assurance level substantial in sections 2.4.4 and 2.4.5 of the Annex to the Act on Level of Assurance in Electronic Identification. Moreover, the identification service provider shall have in place an effective plan for terminating the identification service. (29 June 2016/533)*

*[…]*

***EU Assurance Level Regulation, section 2.4.4 Record keeping***

*LOW*

*1. Record and maintain relevant information using an effective record-management system, taking into account applicable legislation and good practice in relation to data protection and data retention.*

*2. Retain, as far as it is permitted by national law or other national administrative arrangement, and protect records for as long as they are required for the purpose of*

*auditing and investigation of security breaches, and retention, after which the records shall be securely destroyed.*

*SUBSTANTIAL/HIGH*

*Same as level low, plus:*

*Sensitive cryptographic material, if used for issuing electronic identification means and authentication, is protected from tampering.*

***EU Assurance Level Regulation, section 2.4.5 Facilities and staff***

*LOW/SUBSTANTIAL*

*1. The existence of procedures that ensure that staff and subcontractors are sufficiently trained, qualified and experienced in the skills needed to execute the roles they fulfil.*

*2. The existence of sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures.*

*3. Facilities used for providing the service are continuously monitored for, and protect against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service.*

*4. Facilities used for providing the service ensure that access to areas holding or processing personal, cryptographic or other sensitive information is limited to authorised staff or subcontractors.*

***EU Assurance Level Regulation, Annex, section 2.4.6 Technical controls***

*LOW/SUBSTANTIAL*

*1. The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed.*

*2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay.*

*3. Access to sensitive cryptographic material, if used for issuing electronic identification means and authentication, is restricted to the roles and applications strictly requiring access. It shall be ensured that such material is never persistently stored in plain text.*

*4. Procedures exist to ensure that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents and security breaches.*

*5. All media containing personal, cryptographic or other sensitive information are stored, transported and disposed of in a safe and secure manner.*

***M72, section 5: Technical information security measures of the identification scheme***

*The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme:*

*1) telecommunication security*
   - *a) structural network security*
   - *b) zoning of the communications network*
   - *c) filtering rules according to the principle of least privilege*
   - *d) administration of the entire life cycle of the filtering and control systems*
   - *e) control connections*

*2) computer security*
   - *a) access rights control*
   - *b) identification of the users of the scheme*

*c) hardening of the scheme*
*d) malware protection*
*e) tracing of security events*
*f) security incident observation capability and recovery*
*g) internationally or nationally recommended encryption solutions in other respects than those laid down in section 7*

*3) operator security*
*a) change management*
*b) processing environment of secret materials*
*c) remote access and remote management*
*d) management of software vulnerabilities*
*e) backup copies*

*Production network together with its control connections referred to paragraph 1(1)(e) and remote access and remote management referred to in paragraph (1)(3)(c) above must be implemented in such a way that the information security threats caused by other services of the organisation such as e-mail or web browsing, or information security threats caused by other functions than those essential to management in a terminal used for the management, are*

*a) at substantial assurance level specifically assessed and minimised, and*
*b) at high level of assurance prevented when assessed as a whole.*

***Traficom Regulation M72, section 7, Encryption requirements of the identification scheme and interfaces***

*Interfaces between identification service providers and interfaces between an identification service provider and an eService shall be encrypted. The following methods shall be used in the encryption, key exchange and signcryption:*

*1) **Key exchange**: In key exchange, DHE methods or ECDHE methods with elliptic curves shall be used. The size of the finite field to be used in calculations shall be at least 2048 bits in DHE and at least 224 bits in ECDHE.*

*2) **Signature**: When using the RSA for electronic signatures, the key length shall be at least 2048 bits. When using the elliptic curve method ECDSA, the underlying field size shall be at least 224 bits.*

*3) **Symmetrical encryption**: The encryption algorithm shall be AES or Serpent. The key length shall be at least 128 bits. The encryption mode shall be CBC, GCM, XTS or CTR.*

*4) **Hash functions**: The hash function shall be SHA-2, SHA-3 or Whirlpool. SHA-2 refers to functions SHA224, SHA256, SHA384 and SHA512.*

*Encryption settings shall be technically forced to the minimum levels listed above to avoid a situation where settings weaker than the minimum levels are adopted following connection handshakes.*

*If the TLS protocol is used, version 1.2 of TLS or newer shall be used. Version 1.1 of TLS may only be used if the user's terminal does not support newer versions.*

*The integrity and confidentiality of messages containing personal data shall be protected by encryption referred to paragraph 1 above and also at a message level in accordance with paragraph 1.*

*The integrity and confidentiality of the identification scheme record keeping shall be ensured. If the data protection is only based on encryption, requirements laid out in paragraph 1 above concerning signatures, symmetrical encryption and hash functions shall apply.*

### 3.5 The user's agreement terms and conditions, and responsibilities

#### 3.5.1 General

Section 20 of the Identification Act states that the issuance of an identification means is based on the agreement between the applicant for the identification means and the identification service provider. The agreement must be in writing. The agreement can be in electronic format, provided that its content cannot be changed unilaterally and that it remains available to the parties.

Section 15 of the Identification Act defines the information (agreement terms and conditions) that the identification service provider must provide for the user before making an agreement.

Section 23 of the Identification Act lays down the user's obligation to store identification means with care, and sections 21–27 define the rights, obligations and responsibilities of the identification means provider and holder.

Traficom supervises the requirement laid down in section 15 of the Identification Act, according to which the electronic identification service provider must provide the applicant for an identification means (user) with the information laid down in the law before making an agreement. The assessment of the clarity and reasonability of the agreement terms and conditions is within the scope of general consumer protection regulations.

Questions related to provision may also be assessed considering the general consumer protection law or the general competition law. These belong to the Finnish Competition and Consumer Authority or the Consumer Ombudsman operating under it.

#### 3.5.2 Traficom's opinion

**A single identification means cannot be provided as both strong and unregistered means from the perspective of the user's rights on the basis of claiming to fulfil the rights similar to those laid down in the Identification Act with agreement terms and conditions.**

The reliability of strong electronic identification is partly based on official supervision. The mandatory provisions of the Identification Act on the user's rights do not apply to an unregistered identification service, and Traficom does not have the powers to supervise the implementation or agreement terms and conditions of unregistered electronic identification. Fulfilling rights similar to those laid down in the Identification Act with agreement terms and conditions is not sufficient to replace the legal protection of the user and the relying party/service as laid down in the Identification Act, which does not apply to unregistered identification means.

**Traficom does *not* see that completely separate agreements and agreement terms and conditions should be in place for both strong and weak identification means on the basis of the Identification Act.**

However, agreement terms and conditions must clearly indicate the terms and conditions of strong identification in accordance with section 15 of the Identification Act, and the terms and conditions of unregistered identification must remain separate from them.

**If an identification means provider prepares agreement terms and conditions that apply to both strong and unregistered identification,**

**fulfilling the identification means provider's obligation to provide information requires special care:**

- The service provider must, in detail, present any differences related to factors listed in section 15 of the Identification Act and any other relevant factors in strong and unregistered identification services and in terms and conditions applied to them. It is in Traficom's powers to supervise that the information laid down in section 15 of the Identification Act is presented to the user regarding strong electronic identification means as referred to in the Identification Act.

- An increased obligation to provide information results from the user needing to understand any differences between strong identification means and any other identification presented in the same agreement (information regarding provided services, the inclusion of the service and service provider within the scope of public supervision regarding strong identification only) and any differences in the user's legal position according to which of the two identification means the user uses (information on the parties' rights and obligations). One difference in the legal position inevitably arises from the user's responsibility for unauthorised use being only regulated regarding strong electronic identification on the basis of the Identification Act[1].

- In addition, terms and conditions provided for consumers must be clear and understandable by virtue of the Consumer Protection Act. This is supervised by the Consumer Ombudsman. Traficom does not have the authority to take a stand on the marketing of identification services from the perspective of the Consumer Protection Act.

**The lifecycle management of strong and unregistered identification means must be clearly separated if different procedures are used in them.**

For example, a strong identification means or its authentication factor cannot be renewed at a level other than the assurance level required by law, and any lighter renewal procedures applied to unregistered identification means cannot weaken strong identification means. The simultaneous issuance of both strong and unregistered means is possible if it is carried out as required to issue a strong means. Similarly, their simultaneous revocation is possible.

**Traficom sees that the user must always know what identification means they need to use and what identification means they are using.**

The user must always be able to trust that the use of an identification means provided as a strong identification means on the basis of an agreement always complies with all legal obligations.

### 3.5.3 Provisions

***Section 3 of the Identification Act, Binding nature of the provisions***

*Any contractual terms that differ from the provisions of this Act to the detriment of the consumer are deemed void unless otherwise provided below.*

*[…]*

[1] These differences cannot possibly be fully eliminated on the basis of an agreement because, for example, the user's responsibility for unauthorised use relative to third parties cannot be fully restricted with agreements between the user and identification service provider.

***Section 15 of the Identification Act, Duty of the provider of an identification means to provide information before making an agreement (29 June 2016/533)***

*Prior to entering into an agreement with an applicant for an identification means, the service provider shall provide the applicant with information about: (29 June 2016/533)*
*1) the service provider;*
*2) the services offered and their prices;*
*3) the identification principles referred to in section 14;*
*4) the rights and responsibilities of the parties;*
*5) possible limits of liability;*
*6) complaint and dispute settlement procedures;*
*7) possible restraints and restrictions on use referred to in section 18; and*
*8) other possible terms of use related to the identification means.*

*The data in subsection 1 shall be submitted in writing or in electronic form so that the applicant for an identification means can store and reproduce them unaltered. If, upon an identification means holder's request, an agreement is entered into by distance communication that will not allow submission of data and contract terms in the aforementioned manner prior to entering into agreement, such data shall be submitted in the said manner immediately after the agreement has been executed.*

*Provisions on the duty of providing information regarding the processing of personal data are issued in the Personal Data Act.*

***Section 20 of the Identification Act, Issuing an identification means (29 June 2016/533)***

*The issuance of an identification means is based on the agreement between the applicant for the identification means and the identification service provider. The agreement must be in writing. The agreement can be in electronic format, provided that its content cannot be changed unilaterally and that it remains available to the parties. The identification service provider shall treat its customers in a non-discriminatory way and the identification means applicants fairly when entering into the agreement.*

*The agreement can be temporary or for a limited time period. The identification means can have a validity period that is shorter than the term of the agreement.*

*An identification means is always issued to a natural person or a legal person. The binding of a natural person and a legal person to an identification means shall be implemented in accordance with section 2.1.4 of the Annex of the Act on Level of Assurance in Electronic Identification. The identification means must be person-specific. If needed, data may be linked to the identification means allowing the person, on a case-by-case basis, to represent another natural or legal person. (29 June 2016/533)*

***Section 21 of the Identification Act(29 June 2016/533)**, **Delivering the identification means to the applicant***

*The identification service provider shall deliver the identification means to the applicant as stated in the agreement. The identification service provider must ensure that when the identification means is handed over, it does not become subject to unauthorized possession. The method for ensuring this must meet, at a minimum, the requirements laid down for assurance level substantial in section 2.2.2 of the Annex of the Act on Level of Assurance in Electronic Identification.*

***EU Assurance Level Regulation, section 2.2.2 Issuance, delivery and activation***

*SUBSTANTIAL*

*After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed that it is delivered only into the possession of the person to whom it belongs.*

***Section 22 of the Identification Act (29 June 2016/533)**, **Renewal of the identification means***

*The identification service provider may provide a new identification means without explicit request to the holder only if a previously delivered identification means needs to be replaced. The renewal of the identification means must follow, at a minimum, the requirements laid down for assurance level substantial in section 2.2.4 of the Annex of the Act on Level of Assurance in Electronic Identification.*

***EU Assurance Level Regulation, section 2.2.4 Renewal and replacement***

*LOW/SUBSTANTIAL*

*Taking into account the risks of a change in the person identification data, renewal or replacement needs to meet the same assurance requirements as initial identity proofing and verification or is based on a valid electronic identification means of the same, or higher, assurance level.*

***Section 25 of the Identification Act, Cancellation and prevention of use of identification means***

*The identification means holder shall notify the identification service provider or a designated party if the identification means has been lost, is in the unauthorized possession of another person or of any unauthorized use immediately upon detection of this fact. (29 June 2016/533)*

*The identification means provider shall provide an opportunity to submit a notification as set out in subsection 1 at any time. Upon receipt of the notification, the identification service provider shall immediately cancel the identification means or prevent its use. (29 June 2016/533)*

*The identification means provider shall properly and without delay enter in its system the information about the time of cancellation or prevention of use. The holder of the identification means has the right to request proof of submitting a notification mentioned in subsection 1. Such request must be made within 18 months from the notification. (29 June 2016/533)*

*The system shall be designed to allow a service provider using identification service to easily verify the information entered at any time. However, such obligation to create an opportunity to verify information does not exist if the use of the identification means can be prevented or blocked by technical means.*

*A service provider using identification service shall check the systems and registers maintained by the identification service provider for potential cancellations or restrictions to use in connection with the use of the identification means. However, no checking is needed, if the use of the identification means can be prevented or blocked by technical means.*

*If the identification service is based on certificates and information on cancelled certificates is given via Block Lists, the certification service provider may store the data obtained from the Block List for the purpose of verifying the validity of a certificate. Alternatively, the certification service provider may store the Block List.*

***Section 26 of the Identification Act (29 June 2016/533)**, **Identification service provider's right to suspend or revoke the use of an identification means***

*In addition to the provisions of section 25, the identification service provider may suspend or revoke the use of an identification means if:*

*1) the identification service provider has reason to believe that someone other than the person to whom the means was issued is using it;*

*2) the identification means is obviously defective;*

*3) the identification service provider has reason to believe that the safe use of the means is at risk;*

*4) the identification means holder is using the identification means contrary to the agreed terms of use; or*

*5) the identification means holder has died.*

*The identification service provider shall notify the holder as soon as possible about the revocation or suspension of use of the identification means, as well as the time of and reasons for such action.*

*The identification service provider shall renew, reactivate or replace the ability to use the identification means or give the identification means holder a new means immediately after removal of reasons referred to in subsection 1 (2 and 3).*

***Section 27 of the Identification Act, Restrictions to the identification means holder's liability for unauthorised use of the identification means***

*The identification means holder shall be liable for unauthorised use of the identification means only if:*

*1) he or she has made the use of the identification means available to someone else;*

*2) the loss of the means or unauthorised possession or use is the result of the holder's gross negligence, or*

*3) the holder has failed to notify the identification service provider or a designated party that the means has been lost, is in the unauthorised possession of another person or of any unauthorised use immediately upon detection of this fact.*

*However, the identification means holder shall not be liable for unauthorised use:*

*1) to the extent that the identification means has been used after the holder has reported to the identification service provider of the loss, unauthorised possession or use of the means;*

*2) if the identification means holder has not been able to report the loss, unauthorised possession or use of the means without undue delay after detecting it, because the identification service provider has failed to perform its obligation referred to in section 25 subsection 2 to ensure that the holder can report at any time; or*

*3) a service provider using identification services has failed to check the restrictions on use or prevention or blocking of the means as set out in section 18 subsection 4 or section 25 subsection 5.*

## 3.6 Processing of personal data, identification events and logs

### 3.6.1 General

Sections 6 and 7 of the Identification Act lay down provisions on the processing of personal data in strong electronic identification. In Government proposal 237/2020, section 6 is proposed to be amended. The Population Information System has been defined as a trusted source of data.

The processing of personal data is primarily defined in the EU General Data Protection Regulation (GDPR) and the processing of personal identity codes is defined in section 29 of the Data Protection Act.

The Data Protection Ombudsman supervises the processing of personal data by virtue of the Identification Act, the Data Protection Decree and the Data Protection Act.

Section 24 of the Identification Act lays down provisions on the storage of authentication event data and the permitted grounds for the use of data. The section also sets an obligation to maintain processing logs.

Section 12 of Traficom Regulation 72 defines the mandatory personal data (*mandatory attributes*) that an identification service must be able to provide in the trust network and the optional personal data (*optional attributes*), the provision of

which must be a planned capacity. The purpose of the regulation is to secure the interoperability of identification. The data fully corresponds with the eIDAS statutes (Commission Implementing Regulation (EU) 1501/2015), and the purpose of the regulation is also to secure cross-boundary interoperability, if necessary.

It should be noted that the regulation on strong electronic identification does not require that mandatory or optional attributes be provided or confirmed for a relying party. A strong electronic identification service can also be productised so that only a pseudonym or, for example, information that the party being identified is at least 18 years of age is provided for the relying party.

### 3.6.2 Traficom's opinion

Traficom sees that the regulation on strong identification is the grounds for processing personal data in accordance with the GDPR regarding the personal data that is laid down in section 12 b, subsection 2 of the Identification Act and the Traficom Regulation issued under the Identification Act. In addition to identifying and additional/descriptive personal data, the provisions laid down in the Identification Act apply to the storage of authentication events, and its information security obligations require the maintenance of different technical logs.

**The Identification Act does not apply to unregistered identification or provide grounds for the processing of personal data in an unregistered identification service.** Therefore, the controller must justify and assess the grounds for the processing of personal data, the disclosure of personal data to services and the maintenance of event logs in unregistered identification separately in accordance with the GDPR and the Data Protection Act. It should be noted that the grounds for the processing of personal data also affect the rights of data subjects. In unregistered identification, the maintenance of event logs must also be assessed based on grounds other than section 24 of the Identification Act.

Similarly, if personal data other than the data referred to in identification regulations is provided in conjunction with strong identification (enriched data), the grounds for the processing of such data must be assessed separately based on the GDPR.

### 3.6.3 Provisions

Section 6 of the Identification Act has been proposed to be amended (Government proposal 237/2020). The obligation to process personal identity codes is proposed to still be regulated. The purpose of the amendment is not to change the legal status, as the obligations laid down in act 533/2016 are already considered to result from the GDPR and the Data Protection Act.

***Proposed section 6 of the Identification Act, Processing of personal identity codes***

*The identification service provider and a certification service provider offering trust services must, when checking the identity of an applicant, demand the applicant to indicate their personal identity code.*

See also the Data Protection Act (1050/2018) and (EU) 2016/679 (GDPR).

***Section 7 of the Identification Act (20 February 2015/139)*, *Use of data stored in the Population Information System***

*The provider of an identification means and a certification service provider offering a trust service must use the Population Information System to obtain and update the data they need in order to be able to offer a service for identifying a natural person. The identification service provider shall also ensure that the data it needs for the purpose of offering*

*identification services are up-to-date with the data in the Population Information System. (29 June 2016/533)*

*[…]*

***Section 8 of the Identification Act (29 June 2016/533)**, **Requirements posed on the electronic identification scheme***

*[…]*

*The provisions of subsection 1 do not prohibit offering a specific service in a way that the identification service provider discloses to the service provider using the identification service the pseudonym of the identification means holder or only a limited amount of personal data.*

***Section 24 of the Identification Act (29 June 2016/533)**, **Storage and use of data regarding the authentication event and means***

*The identification service provider shall store:*

*1) data required for performing an individual authentication event and an electronic signature;*

*2) data on preclusions or restrictions on the use of identification means referred to in section 18; and*

*3) data content of the certificate as set out in section 19.*

*The provider of an identification means shall store the necessary data about the initial identification of an applicant referred to in section 17 and 17 a and the document or electronic identification used therein.*

*The data referred to above in section 1 subsection 1 shall be stored for five years from the authentication event. Other data referred to above in section 1 subsection 2 shall be stored for five years from the termination of a permanent customer relationship.*

*Personal data generated during the authentication event shall be destroyed after the event, unless they are required to be kept to verify an individual authentication event.*

*The identification service provider may process stored data only to perform and maintain the service, for invoicing, to protect its rights in case of disputes, to investigate misuse of personal data as well as upon request by the service provider using identification service or the holder of the identification means. The identification service provider shall store data on processing, the time, reason, and person processing it.*

*If the service provider only issues identification means (devices):*

*1) subsection 1, paragraph 1 and subsection 4 do not apply to the provider;*

*2) the five-year record-keeping period referred to in subsection (3) above will then be calculated from the date the identification means validity expires.*

***Traficom Regulation 72, section 12, Minimum set of data to be relayed in a trust network***

*The following minimum set of data shall be relayed at the interface between the identification device provider and the provider of an identification broker service:*

*1) in identification events concerning natural persons: at least the first name, family name, date of birth and the unique identifier of the person;*

*2) in identification events concerning legal persons: at least the first name, family name and the unique identifier of the natural person representing the legal person as well as the unique identifier of the organisation; and*

*3) an indication of whether the level of assurance is substantial or high.*

*The interface between the identification device provider and the provider of an identification broker service must enable the relay of the following information:*

*1) an indication of whether the identification event concerns a public administration eService or a private eService;*

*2) in identification events concerning natural persons: forename(s) and surname(s) at the time of birth, place of birth, current address and gender;*

## 3.7 Regulations on contractual obligations and cooperation in a trust network

### 3.7.1 General

Section 12 a of the Identification Act defines the trust network of strong identification service providers. The trust network consists of identification services that have submitted the notification laid down in the Identification Act and that Traficom has approved in its register. The term "trust network" is largely used as synonymous with strong electronic identification, while "trust network" actually means an obligation imposed on an identification means provider to provide an identification broker service with access rights to the identification service, and provisions on related agreement terms and conditions. In addition, identification services have a cooperation obligation to ensure technical interoperability.

Section 16 of the Identification Act lays down provisions on notifying the agreement parties in the trust network of any significant threats or disruptions to the operation of the service, information security or the use of an electronic identity.

Section 12 a, subsection 5 of the Identification Act sets restrictions on the processing of data of another identification service provider obtained as a result of the transfer of access rights or on the basis of section 16, and the obligation to compensate for any losses resulting from the use of data in breach of the provisions.

### 3.7.2 Traficom's opinion

Regulations on trust networks in accordance with the Identification Act, meaning the transfer of access rights to an identification service, provisions on agreement terms and conditions, the management of disruptions and related specific confidentiality obligations, only apply to strong electronic identification.

**The forwarding of unregistered electronic identification is not within the scope of regulations on access rights to the trust network, while the Identification Act does not prevent delivery on other grounds.**

### 3.7.3 Provisions

***Section 12 a of the Identification Act (29 March 2019/412), Trust network of identification service providers***

*By submitting a notification to the Finnish Transport and Communications Agency in accordance with section 10, an identification service provider becomes a member of a trust network.*

*An identification means provider shall offer an access right to the providers of identification broker services so that they can forward authentication events to the party relying on electronic identification. The identification means provider shall draw up delivery terms and conditions concerning access right to their identification service and must use them when making agreements with providers of identification broker services. The terms and*

*conditions of access right shall be compliant with this Act, reasonable and non-discriminatory. The provider of an identification means shall accept a request by a provider of an identification broker service concerning the making of an agreement in accordance with the terms and conditions of delivery and shall grant an access right to the identification service immediately, in any case no later than within a month of the submission of the request. The provider of an identification means may refuse to make an agreement only if the provider of an identification broker service acts in violation of this Act or regulations issued pursuant to it or if another important justification for the refusal exists.*

*Identification service providers must collaborate to ensure that the technical interfaces of the members of a trust network are interoperable and that they enable the provision of interfaces that implement commonly known standards to the relying parties.*

*An identification service provider shall implement maintenance, alteration and information security measures in a way that causes as little harm as possible to other identification service providers, users and relying parties. In addition to the provision laid down in section 25 and 26, an identification service provider may temporarily suspend the provision of an identification service or restrict access to it without the consent of another identification service provider, if it is necessary for the successful completion of a measure referred to above. The suspension and alteration shall be effectively communicated to the other identification service providers whose services it may affect.*

*An identification service provider may use data on another identification service provider it has obtained pursuant to an access right transfer or section 16, but only for the purpose for which they were disclosed to the identification service provider. The only people who may process the data are those in the service of the identification service provider or acting on behalf of it who absolutely need the data in their work. Information shall also otherwise be handled in such a way that the business secrets of another identification service provider are not endangered. An identification service provider that causes damage to another identification service provider by acting contrary to this subsection has an obligation to compensate any damage caused by the action.*

*Further provisions on the administrative procedures, technical interfaces and administrative responsibilities of the trust network are issued by Government Decree.*

***Section 16 of the Identification Act (29 March 2019/412) Notifications of the identification service provider concerning threats or disruptions to their operations and protection of data***

*Notwithstanding any secrecy provisions, an identification service provider shall inform the parties relying on their identification service, holders of identification means, other agreement parties operating in the trust network and the Finnish Transport and Communications Agency without undue delay of all significant threats or disruptions to the operation of the service, information security or the use of an electronic identity. The notification shall also include information about measures the parties involved have for use to counter such threats and risks, as well as the estimated expenses incurred by these measures.*

*An identification service provider can, without prejudice to secrecy provisions, notify all members of a trust network of the threats and disruptions referred to in subsection 1 and of service providers of whom there is reason to believe that they are seeking unauthorised financial gain, giving false or misleading information that is significant or processing personal data illegally.*

*The Finnish Transport and Communications Agency may forward information between the parties of a trust network on behalf of the notifying party by technical means without prejudice to the provisions in the Act on the Openness of Government Activities (621/1999).*

# Annex: Summary of statements of the draft memorandum dated 27 March 2020

Statements were issued by Avaintec Oy, Danske Bank A/S, Branch Finland, the Digital and Population Data Services Agency (DVV), Elisa Corporation, the Finnish Federation for Communications and Teleinformatics (FiCom), Finance Finland, the Finnish Competition and Consumer Authority (FCCA), Nets Denmark A/S, Branch Norway, OP Cooperative and S-Bank Ltd.

Several statements (FCCA, Nets, Elisa, FiCom, DVV) were in favour of the starting points of the memorandum, as well as specifying it, safeguarding the requirements for strong identification, the sufficient separation between strong and unregistered identification, and clarity of the user's position. The memorandum and its policies were regarded as justified.

Danske and S-Bank presented requests for specifications.

**The statements are presented below per theme**

**Promoting the markets and development**

The FCCA stated that the use of a single identification scheme for the provision of both strong and weak identification means may facilitate entry in electronic identification markets, which helps to promote competition and the functioning of the markets.

The statements issued by Elisa, all the different banks and Finance Finland presented opposing views regarding whether the advice provided in the interpretation memorandum creates conditions for the development of identification services or whether it prevents the utilisation of technological development.

Elisa saw that the policies proposed by Traficom enable domestic operators to compete with the most advanced operators, such as Google, Facebook and Apple.

The proactivity of the requirements was regarded to have a positive impact on the ongoing development of services, while it was also pointed out that rigid and detailed specifications are not purposeful and, for example, the development opportunities offered by biometric authentication factors cannot yet be predicted.

- Traficom regards both of these perspectives as correct and justified. Official guidance must find a good balance between proactive requirements and flexible technological development. Therefore, the advice in question has been issued in the form of an interpretation memorandum, not as a regulation.

- **A clarification of the legal nature relative to regulations has been added to the memorandum, and certain opinions have been changed to be more general.**

**Rights of users**

The FCCA and the banking sector presented rather opposing views regarding whether it is significant to clarify for users when they are using strong identification and when unregistered identification.

The FCCA considered it important that the sufficient separation of means and the clarity of agreement terms and conditions be ensured as described in the draft memorandum. When using identification means, it must not remain unclear for consumers whether they are using weak identification or strong identification, which is prescribed by law. As described in the draft memorandum, the implementation of strong and weak identification means should address the separation of the identification method from features detectable by users and the fulfilment of users' rights. It must be possible to identify any differences in strong and weak identification services from terms and conditions applied to them. Furthermore, the terms and conditions of strong and weak identification must not make it unclear to which consumers commit when approving the terms and conditions.

Finance Finland and OP saw the level of identification means and the separation presented in the draft memorandum are insignificant for users. Users appreciate the ease of use, and their trust is based on the service provider, not on the strong status of the identification service. On the basis of this, it was considered that the separation between strong and unregistered identification means and the level of identification are insignificant for users. The strength of identification was seen to be in the interests of the party relying on identification, not of users.

- Traficom states that estimates of the level of interest of average users in the status of the identification service may be relevant, while this rather emphasises the need for information on the identification service. Users must be able to easily see what identification service they are using and what its terms and conditions are.

OP and Finance Finland saw that, from the users' perspective, it is better to use the processes and technologies of the provider of strong electronic identification means with fewer identification elements or controls than to develop different solutions and distribute many different identifiers to users or to only use universal identification means that operate at a low level. In its statement, OP pointed out that separation may cause unclarity when closing identification means, for example.

- The purpose of the interpretation memorandum is to clarify on what conditions lower level identification means can also be provided in a single scheme.

- **The section concerning the closing of identification means and the management of lifecycles has been clarified.** Separation must be ensured if different procedures are used in strong and unregistered identification.

**The term "weak authentication"**

In its statement, Avaintec criticised the use of the term "weak authentication".

- Traficom agrees that the term is unnecessarily biased, and the definition used in the memorandum clearly indicates that the question is of registration and supervision, not of the quality of identification. Traficom sees that a challenge in the use of the term "low" is that it refers to the lowest assurance level set out in the eIDAS Regulation, and there can be no objective information on its implementation.

- **The term "weak authentication" has been replaced by the term "unregistered identification means" in the memorandum.**

**PSD2**

The statements issued by representatives of banks pointed out that key regulations on bank identification is based on the Payment Services Directive (PSD2) and that the requirements for strong identification in payment services come from the European Commission's technical regulatory standard and the interpretations of the European Banking Authority (EBA) and the Finnish Financial Supervisory Authority (FIN-FSA). It was asked whether it is purposeful to add references and any new interpretations to the memorandum concerning the relationship between *responsibility provisions* of the Payment Services Act and the Identification Act regarding unregistered/weak electronic identification. Cooperation between Traficom and FIN-FSA in terms of interpretations was requested.

One statement saw that the Payment Services Act is applicable in place of the Identification Act when identification means are used for the purposes of payment services. Furthermore, it was stated that the purpose cannot be that Finland starts to develop dedicated identification means for the approval of payments pursuant to PSD2 alone.

- **Traficom has added a reference to PSD2 to the memorandum.**

- Unfortunately, technical questions or questions of the coordination of responsibility issues cannot be covered in any more detail in this memorandum, and these will be discussed separately, if possible. The statements pointed out the card payment interface and responsibility provisions. Otherwise, the statements did not present any requirements, to the coordination of which the opinions could be related.

- Traficom and FIN-FSA reviewed the technical requirements in 2018 from the perspective that different acts are applicable side-by-side and any differences must fulfil the strictest or the most detailed regulatory requirements. Traficom states that, as the regulations and EU-level interpretations develop, there will be new coordination questions to be answered, requiring cooperation between the supervisory authorities.

- **The goal of Traficom's steering and supervisory activities is that a single identification means can be used as a general/universal means and in the PSD2 sector.**

**Authentication factors and secrets**

Of the detailed opinions of the draft memorandum, the use of different passwords in strong and weak identification means was considered to be inappropriate. Reasons for this included experiences obtained from the provision of services in that the requirement to remember different passwords causes harm that supersedes any benefits obtained from separation. In comparison, it was stated that a single password can be used for the debit and credit features of payment cards without any problems.

- **On the basis of the statements, Traficom has changed the opinion on the separation of authentication factors in the interpretation memorandum.**

- **Furthermore, Traficom has assessed the separation of cryptographic secrets and alleviated the interpretation presented in the draft.**

**Initial identification**

In addition to the actual topic of the memorandum, the statements emphasised the need to define requirements for remote identification.

- Assessment requirements for remote identification will be specified separate from this interpretation memorandum.

- However, the interpretation memorandum presents policies on what needs to be considered when upgrading unregistered identification means to strong means.

**Other**

The statements presented individual requests and proposals for specifying the text.

- **Traficom has specified the wording of the memorandum.**

The statements requested Traficom to increase users' understanding of any differences between identification and electronic signatures, and also to present and promote electronic services other than strong electronic identification.

- **Traficom would like to thank all the issuers of statements for presenting these comments and will take these into consideration otherwise, if possible and in accordance with its authorities.**