


| | | |
|---|------------------------------|-------------|
|  | Digital Trust Process | |
| | ILNAS/PSCQ/Pr005A | |
| Approved by: | Version 1.4 – 22.02.2024 | Page 1 of 9 |


ILNAS/PSCQ/Pr005A

Recognition of other identification methods at the national level

Modifications: clarify the role of the procedure ILNAS/PSCQ/Pr005B

1, avenue du Swing
L-4367 Belvaux
Tél.: (+352) 247 743 50
Fax: (+352) 247 943 50

confiance-numerique@ilnas.etat.lu
www.portail-qualite.public.lu

| | | |
|---|------------------------------|-------------|
|  | Digital Trust Process | |
| | ILNAS/PSCQ/Pr005A | |
| Approved by: Alain Wahl | Version 1.4 – 22.02.2024 | Page 2 of 9 |

1. Introduction

The Luxembourg Institute for standardisation, accreditation, safety, and quality of goods and services (ILNAS, “Institut Luxembourgeois de la Normalisation, de l’Accréditation, de la Sécurité et qualité des produits et services”) is placed under the administrative supervision of the Minister of the Economy of the Grand Duchy of Luxembourg. The legal missions of ILNAS – Digital Trust Department are based on the Law of 4 July 2014 on the reorganisation of ILNAS [1].

ILNAS, via its “Digital Trust Department”, is notably charged with the supervision of QTSPs (Qualified Trust Service Providers) that are established in the Grand Duchy of Luxembourg and offer qualified trust services. According to the « Loi du 17 juillet 2020 portant modification de la loi modifiée du 14 août 2000 relative au commerce électronique » [4], ILNAS publishes on its website the minimal requirements for the identification methods under Article 24 paragraph 1 letter d) of Regulation (EU) 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (the eIDAS Regulation) [2].

This document describes the minimal requirements that have to be met by other identification methods in the context of Article 24 paragraph 1 letter d) of the eIDAS Regulation [2] and the process applied by the ILNAS – Digital Trust Department – regarding the recognition at national level of these identification methods.

Purpose of the procedure

The purpose of this procedure is to specify the minimal requirements for the identification methods under Article 24 paragraph 1 letter d) of the eIDAS Regulation [2] and to describe the process applied by ILNAS for recognizing these alternative identification methods at the national level in conformance with Article 24, paragraph (1) letter (d) of the eIDAS regulation. The procedure primarily addresses the (qualified) trust service providers established in Luxembourg and the staff of ILNAS – Digital Trust Department as well as the director of ILNAS.


2. Definitions

For the requirements of this document, the definitions given in the eIDAS Regulation [2] apply.


3. References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

- [1] Loi du 4 juillet 2014 portant réorganisation de l’Institut luxembourgeois de la normalisation, de l’accréditation, de la sécurité et qualité des produits et services et portant organisation du cadre général pour la surveillance du marché dans le contexte de la commercialisation des produits
- [2] Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (the eIDAS Regulation)
- [3] [Bundesnetzagentur Mitteilung Nr. 208/2018](#), Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Referat IS 15, Canisiusstraße 21, 55122 Mainz
- [4] Loi du 17 juillet 2020 portant modification de la loi modifiée du 14 août 2000 relative au commerce électronique

| | | |
|---|------------------------------|-------------|
|  | Digital Trust Process | |
| | ILNAS/PSCQ/Pr005A | |
| Approved by: Alain Wahl | Version 1.4 – 22.02.2024 | Page 3 of 9 |

- [5] Supplementary Assessment Criteria for Conformity Assessment Bodies for the Review of the Requirements in the Administrative Order pursuant to section 11(1) VDG (available upon request)
- [6] Procedure ILNAS/PSCQ/Pr005B - Supplementary Assessment Criteria for Conformity Assessment Bodies for the verification of the requirements in the Annex of procedure ILNAS/PSCQ/Pr005A
- [7] Technical Guideline of the Federal Office for Information Security (BSI) TR-02102
- [8] Loi modifiée du 14 août 2000 relative au commerce électronique et aux services de confiance

| | | |
|---|------------------------------|-------------|
|  | Digital Trust Process | |
| | ILNAS/PSCQ/Pr005A | |
| Approved by: Alain Wahl | Version 1.4 – 22.02.2024 | Page 4 of 9 |

4. Process for handling requests concerning the recognition of other identification methods according to article 24, paragraph (1) letter (d) of the eIDAS regulation

5.1) General requirements

- **Video identification based on interacting with natural persons**

a) Criteria:

- 1) eIDAS Regulation
- 2) Requirements in the annex of this procedure
- 3) Supplementary assessment criteria for conformity assessment bodies for reviewing the requirements in the procedure LNAS/PSCQ/Pr005A, which are available upon request from ILNAS [6]

b) Requirements:

- 1) The identification method has to provide equivalent assurance in terms of reliability to physical presence.
- 2) The equivalent assurance under point 1 above has to be **certified** by a conformity assessment body (CAB) according to the requirements in the Annex of this Procedure.

Conformity assessment bodies **must evaluate the additional assessment criteria** defined in the procedure ILNAS/PSCQ/Pr005B - Supplementary Assessment Criteria for Conformity Assessment Bodies for the Verification of the Requirements in the Annex of the Procedure ILNAS/PSCQ/Pr005A [6], which is available upon request from ILNAS.

- 3) The CAB has to be accredited according to Article 3(18) of the eIDAS Regulation.


c) Certification Report Requirements: confirmation of equivalence (as required by eIDAS). Certification with respect to the requirements in the annex of this procedure

5.2) Documents required by ILNAS

- 1) Certificate of conformity by a CAB certifying equivalent assurance of the identification method to physical presence according to the eIDAS Regulation. The audit report should be submitted to ILNAS as well.
- 2) Certificate of conformity/Audit by a CAB verifying the correct implementation of the method at QTSP side (see note on page 4)

5.3) Decision by ILNAS

The final decision on recognition at the national level is taken by ILNAS.

| | | |
|---|------------------------------|-------------|
|  | Digital Trust Process | |
| | ILNAS/PSCQ/Pr005A | |
| Approved by: Alain Wahl | Version 1.4 – 22.02.2024 | Page 5 of 9 |

The Digital Trust Department, after validation of its decision by the Director of the ILNAS, issues a letter stating the recognition or refusal of the identification method based on the following elements:

- The documents under section 5.2),
- Any relevant research results regarding the identification method,
- The scope of the certification by the CAB & the requested scope by the (qualified) trust service provider, and
- The competence of the auditors of the CAB to perform the requested audit.

The letter issued by the ILNAS states the conditions under which the recognition of the identification method in question is valid.

According to [8], the ILNAS publishes on its website the identification methods in the sense of Article 24, paragraph 1, letter d) of the eIDAS Regulation that are recognized in Luxembourg.


5.4 Supervision by ILNAS

The ILNAS monitors the identification methods that have been recognised at national level (in particular, it regularly checks whether new attacks on video identification systems have been published).

In case security risks of the video identification method arise, ILNAS may update the list, published on its website, of identification methods in the sense of Article 24, paragraph 1, letter d) of the eIDAS Regulation recognised in Luxembourg as well as the requirements in the annex of this procedure.

Note: The certification of an identification method in the form of a module by an eIDAS accredited CAB does not imply that the QTSP can simply make use of this identification method. It is still necessary that a CAB verifies the implementation and the correct use of the identification method within the QTSP. ILNAS may only authorize the use of the identification method for issuing qualified certificates after such an additional integration audit has been carried out with a positive result. Here is a non-exhaustive list of eIDAS requirements that the CAB must verify at the QTSP side:

- Art. 24 (2) (d) of the eIDAS Regulation: in particular, the CAB has to check the general terms and conditions of the QTSP and whether they include specific elements regarding the identification method used;
- Art. 24 (2) (e) of the eIDAS Regulation: in particular, the CAB needs to check that the risks related to the identification method are included in a risk analysis;
- Art. 24 (2) (h) of the eIDAS Regulation: in particular, the CAB has to check whether the QTSP stores and keep records of data collected or generated during the identification process (e.g., photos, voice/video recordings, copy of ID card or passport, logs, consent to general terms and conditions of subcontractors).
- Art. 24 (2) (j) of the eIDAS Regulation: the CAB has to check whether the QTSP is compliant with data protection legislation (e.g., is consent properly obtained, is the user informed of the processing of personal data).
- The CAB has to check whether there is a procedure in place for handling security incidents that affect the identification method in question.

| | | |
|---|------------------------------|-------------|
|  | Digital Trust Process | |
| | ILNAS/PSCQ/Pr005A | |
| Approved by: Alain Wahl | Version 1.4 – 22.02.2024 | Page 6 of 9 |

1. Annex

The requirements in Section 2.1 below mainly correspond to the requirements of the Bundesnetzagentur regarding video identification methods (see, [3]).

2.1 Requirements for video identification methods

1. Requirements deriving from standards of the European Telecommunications Standards Institute (ETSI)

Identification methods must match the requirements for registration authorities in the relevant ETSI standards for electronic trust service providers. Relevant in this case are the latest published versions of ETSI EN 319 401, ETSI EN 319 411-1 and 319 411-2

2. Requirements for staff

Video identification may be performed only by specialist, qualified and reliable staff.

a) Specialist knowledge

To demonstrate the specialist knowledge of their employees the trust service provider must keep available proof of initial and regular follow-up training courses. If the activities are outsourced to a mandated third party this proof is to be transmitted to him by the latter before the person in question begins work.

The training courses must cover, as a minimum, knowledge of the features verifiable by video identification, including the verification procedures to be applied in relation to the documents permitted for video identification (see section 5). Employees must be trained as regards common ways of forging these documents. Further, knowledge of the relevant legal rules, most notably data protection regulations and the requirements set out in this procedure, is necessary.


These requirements must be suitably imparted to the employees before they can begin their identification duties. Subsequently, training courses are to be repeated both at regular intervals (once a year minimum) and if deemed necessary by the (Q)TSP¹.

b) Qualification

Qualification of a member of staff for employment as an identification expert is measured according to their ability to perform the process of identification, in particular, that is, to compare the applicant against their identity document. Staff must be able to employ the relevant verification criteria. Suitable methods (eg voice, foreign language, sign language) must be available for communication with the applicant, depending on the trust service provider's offer.

¹ The need for training can, for example, arise from :

- A change in the legal requirements (for example, data protection)
- A change of the procedure ILNAS/PSCQ/Pr005A
- New methods of fraud or attacks in the context of video identification

| | | |
|---|------------------------------|-------------|
|  | Digital Trust Process | |
| | ILNAS/PSCQ/Pr005A | |
| Approved by: Alain Wahl | Version 1.4 – 22.02.2024 | Page 7 of 9 |

c) Reliability

To demonstrate the reliability of his employees the trust service provider must inspect an up to date criminal record certificate for natural persons before the employee begins work. Solely employees with a clean criminal record certificate may act as identification experts. Inspection of an up to date criminal record certificate is to be repeated by the trust service provider at two-yearly intervals. If the work is outsourced to a mandated third party the requirements the trust service provider has to meet apply analogously to the third party.

3. Premises requirements

During the identification process the identification experts must remain in restricted access areas which authorised staff alone may enter.


4. General requirements for the identification process

- a) Assigning identification procedures to the employees requires the deployment of mechanisms that counteract predictable assignment and hence the possibility of manipulation provided by such predictability.
- b) Video identification must be performed in real time and without interruption.
- c) Audio-visual communication between the employee and the identification subject is to be adequately secured in terms of integrity and confidentiality. Here, compliance is required with the recommendations set out in the Technical Guideline of the Federal Office for Information Security (BSI) TR-02102.
- d) The sound and picture quality of the communication must be sufficient to fully enable unambiguous identification using all the tests stipulated in this procedure.
- e) The identification process is to be discontinued if the verification described above – owing, for instance, to poor light or poor sound or picture transmission quality – and/or voice communication with the identification subject is not possible.
- f) The provider must take suitable measures to ensure that his procedures are up to date.

5. Requirements for suitable identity documents

Solely identity documents with security features that are sufficiently forgery-proof and capable of being tested in the procedure may be used for the identity check².

² Driving licenses shall not be used for the identity check.

| | | |
|---|------------------------------|-------------|
|  | Digital Trust Process | |
| | ILNAS/PSCQ/Pr005A | |
| Approved by: Alain Wahl | Version 1.4 – 22.02.2024 | Page 8 of 9 |

6. Requirements for checks of the identity document and of the applicant

The authenticity of the identity document and its unique linkage to the identification subject must be reliably verified. The provider must take suitable measures to enable detection of any manipulation of the video image, that is to say the identity document, or of the person. These may include organisational measures which, through interaction with the identity document in accordance with the instructions of the employee, or interaction with the identification subject, can reveal manipulation. Further, the provider can take technical measures in order to detect any change in the videostream.

7. Requirements for recording and retention

a) Consent to recording

The identification subject has, at the beginning of video identification, to declare their explicit consent to passages of the identification process being recorded.

The user must be given a detailed description of what they are consenting to (eg what consent specifically refers to, the nature of the data processing, by whom and for how long the data will be stored, what will happen to the data in the event of the identification process being broken off).

5

b) Content and duration of the recording

Compliance is needed with the requirements of Article 32 of [8] in conjunction with Article 24(2) points (f) to (h) of Regulation (EU) No 910/2014 in respect of the contents of the recording of the identification process by means of video technology and the retention of the data acquired in this process.

Article 24(2) points (f) to (h) of Regulation (EU) No 910/2014:

[A qualified trust service provider... shall]


“f) use trustworthy systems to store data provided to it, in a verifiable form so that:

- i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained,*
- ii) only authorised persons can make entries and changes to the stored data,*
- iii) the data can be checked for authenticity;*

g) take appropriate measures against forgery and theft of data;

h) record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings [...].”

The principles of necessity and data minimisation are to be aligned with the purpose of enduring non-repudiation of the identification with regard, in particular, to the requirement set out in Article 24(2) point (h) of Regulation (EU) No 910/2014. The essential passages of the

| | | |
|---|------------------------------|-------------|
|  | Digital Trust Process | |
| | ILNAS/PSCQ/Pr005A | |
| Approved by: Alain Wahl | Version 1.4 – 22.02.2024 | Page 9 of 9 |

identification process are to be recorded on a lasting basis using sound and photos/screenshots of the person and the particular identity document.

The identification subject and the front and back of the document the subject uses for identification and the particulars entered on the front and back are to be recorded on the photos/screenshots in clearly recognisable form. Data not needed for the issuance of the qualified certificate are to be blurred. The data that are needed can be taken from ETSI EN 319 411-2, Chapter 6.2.2.

For the recording to be suitable for the purpose of providing evidence within the meaning of Article 24(2) point (h) of Regulation (EU) No 910/2014 it is necessary that the applicant is recognisable without trace of doubt and is clearly discernible when speaking or using sign language. Both the contents and the approved security arrangements of the identity document used must be recorded. A sequence of at least 15 seconds is to be recorded from the qualitatively useable video material.

Consent to the recording of the identification process is to be recorded in addition to the sequence of 15 seconds duration and retained for as long as the data record to which it relates.

An assessment of the recording and retention requirements must be made using a system of double checks ("four-eyes" principle). This involves verifying the accuracy of the data collected and confirming and clearing the match of identity documents used to the applicant.

9. Reporting of suspected cases of fraud

The trust service provider shall report any suspected attempts of fraud to ILNAS.

10. Determination of suitable implementation

Suitable implementation of the requirements set out in this procedure is to be appraised by a conformity assessment body as part of confirmation pursuant to Article 24(1) second subparagraph point (d) first sentence of Regulation (EU) No 910/2014. The appraisal is to reflect the state of the art. This includes the Supplementary Criteria for the assessment of other identification methods pursuant to Article 24(1) second subparagraph point (d) first sentence of Regulation (EU) No 910/2014 as amended at the time of the assessment. The Supplementary Criteria will be made available by the ILNAS, upon request, given legitimate interest.

11. Limitations

The video identification method can only be used by the trust service provider for the issuance of qualified certificates for electronic signatures and the issuance of qualified certificates for electronic seals. For the latter, only the legal representative of the legal person who requests a qualified certificate for electronic seals can be identified via the video identification method.