	<b>Digital Trust Process</b>	
	<b>ILNAS/PSCQ/Pr005</b>	
Approved by:	Version 1.1 – 16.05.2019	Page 1 of 5


# **ILNAS/PSCQ/Pr005**

## **Recognition of other identification methods at the national level**

Modifications: Clarify requirements regarding GDPR

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

[confiance-numerique@ilnas.etat.lu](mailto:confiance-numerique@ilnas.etat.lu)  
[www.portail-qualite.public.lu](http://www.portail-qualite.public.lu)

	<b>Digital Trust Process</b>	
	<b>ILNAS/PSCQ/Pr005</b>	
Approved by: Alain Wahl	Version 1.1 – 16.05.2019	Page 2 of 5

## 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.

This document describes the scheme, requirements and process applied by the ILNAS – Digital Trust Department for the remote identification of clients of QTSP. The supervision scheme is based upon 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].

## 2. Purpose of the procedure

The purpose of this procedure is to describe the process applied by ILNAS for recognizing other 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.


## 3. Definitions

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

## 4. 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] Bundesamt für Sicherheit in der Informationstechnik (BSI): [Technische Richtlinie TR-03147: Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen](#);
- [4] Bundesamt für Sicherheit in der Informationstechnik (BSI): [Prüfberichtsvorlage zur Prüfung von Identifikationsverfahren](#)

	<b>Digital Trust Process</b>	
	<b>ILNAS/PSCQ/Pr005</b>	
Approved by: Alain Wahl	Version 1.1 – 16.05.2019	Page 3 of 5

## 5. 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: eIDAS Regulation

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 has to be **certified** by a conformity assessment body (CAB), accredited according to Article 3(18) of the eIDAS Regulation.
- 3) The CAB needs to have recognized expertise in the field of video identification methods.
- 4) ~~An authorization concerning the processing of personal data granted by the National Commission for Data Protection (CNPD)~~ The conformity of the QTSP with the General Data Protection Regulation (GDPR) needs to be verified by the CAB.

c) Certification Report Requirements: confirmation of equivalence (as required by eIDAS).

d) Recommendations:

- 1) The technical guidelines entitled “TR-03147 Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen” [3] should be used to demonstrate that video identification can be carried out by the QTSP with an assurance level of “high” (cf. Article 8(2) of the eIDAS Regulation).
- 2) The audit report should follow the structure given in [4].


- **Video identification based on interacting with machines**

a) Criteria: To be defined by the CAB (chosen by the QTSP and to be agreed upon with ILNAS)

b) Requirements:

- 1) Certification by an eIDAS accredited CAB with recognized expertise in the field of video identification methods.
- ~~2)~~ An expert opinion in the field of artificial intelligence and/or machine learning (the expert has to be agreed upon in advance with ILNAS – Digital Trust Department).
- ~~2)3)~~ The conformity of the QTSP with the General Data Protection Regulation (GDPR) needs to be verified by the CAB.

c) Certification Report Requirements: confirmation of equivalence (as required by eIDAS).

	<b>Digital Trust Process</b>	
	<b>ILNAS/PSCQ/Pr005</b>	
Approved by: Alain Wahl	Version 1.1 – 16.05.2019	Page 4 of 5

- **Other identification methods**

a) Criteria: To be defined by the CAB (chosen by the QTSP) and to be agreed upon with ILNAS

b) Requirements:

1) Certification by a CAB who is accredited according to eIDAS and having recognized expertise in the field of the identification method in question

2) An expert opinion is required in the relevant field (the expert has to be agreed upon in advance with ILNAS – Digital Trust Department).

2)3) The conformity of the QTSP with the General Data Protection Regulation (GDPR) needs to be verified by the CAB.

c) Certification Report Requirements: confirmation of equivalence (as required by eIDAS).

## 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) The requirements with respect to which the identification method has been audited.

3) If necessary, the opinion of an expert in the field.

## 5.3) Decision by ILNAS

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


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 explicitly states the conditions under which the recognition of the identification method in question is valid.

**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;

	<b>Digital Trust Process</b>	
	<b>ILNAS/PSCQ/Pr005</b>	
Approved by: Alain Wahl	Version 1.1 – 16.05.2019	Page 5 of 5

- 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.