facephi

ETSI 116 461 Certification Self-Assessment

Unattended and Remote Identity Proofing compliance

Version 2.0

Confidencial information

Confidentiality declaration

This document contains confidential and proprietary information. All the information presented is provided on the basis of the consent not to use or disclose It, except in commercial agreements with FacePhi Biometrics.

The recipient of this document agrees to inform all employees and partners, both current and future, that consult have access to the content of the document, about its confidentiality. The recipient agrees to give precise instructions to employees so that they do not disclose information related to this document, except in the case of matters of public knowledge and that are available for public use. The recipient also agrees not to reproduce or distribute, or permit others to reproduce or distribute, any material contained herein without the express, written consent of FacePhi Biometría.

FacePhi Biometrics retains all rights of possession and ownership of the material and trademarks contained herein, including supporting documentation, files, marketing material and multimedia.

The acceptance of this document implies that the recipient agrees to be legally bound by the above declaration.

Version

	Produced by	Approved by
Name	Raúl López Cantó	Miguel Santos LUPARELLI MATHIEU
Position	GRC Officer	Product Innovation Director
Date	31/07/2024	31/07/2024

Versions	Dates	Observations
1.0	07/06/2024	First Version
2.0	31/07/2024	Control BIN-8.4.2-07 updated

Contents

01 Introduction

This document is a self-assessment of Facephi's Identity Verification (IDV) technology compliance with the Technical Specification ETSI 119 461 "[...] for trust service components providing identity proofing of trust service subjects." This document lists the main controls that an Unattended and Remote IDV must fulfill to be considered ETSI 119 461 compliant.

02 Unattended and Remote Identity Verification compliance

2.1. [9.2.3.] Use cases for unattended remote identity proofing

USE-9.2.3.1-01: The applicant shall receive automated guidance throughout the identity proofing process.

- UX/UI for guidance throughout the whole onboarding process.

USE-9.2.3.1-02: The automated process' handling of deviations from expected results or expected behaviour of the applicant shall be specified, including the conditions where the identity proofing process shall be aborted, and the information to convey to the applicant when an identity proofing process is aborted.

- UX/UI interaction with the user to let them know the causes of an error.

USE-9.2.3.1-03: Attribute collection shall be according to the requirements of clause 8.2.2.1 of the present document.

- COL-8.2.2.1-01. Identity Platform.
- COL-8.2.2.1-02. Minimum Identity Information is collected. See Identity Platform.
- COL-8.2.2.1-03. The attributes collected are compliant with a KYC/AML context.
- COL-8.2.2.1-04. All the information collected are used to complete the process of Identity Verification and evidence validation.

USE-9.2.3.1-04: The process shall use at least one digital or physical identity document as authoritative evidence.

- The onboarding application uses a physical document: ID Card, Driving Licence, or Passport, among others authoritative (government issued) identity documents that "offer comparable reliability of the identity".

USE-9.2.3.1-05: Collection of evidence shall be according to the requirements in clause **8.2.3** of the present document.

- COL-8.2.3-01. A physical identity document is used.
- COL-8.2.3-02. The document used contains a portrait photo of the owner of the Identity Document.
- COL-8.2.3-03. The user is presented with a list of documents allowed.

- [CONDITIONAL] COL-8.2.3-04. Only physical passports, national ID cards, or other identity documents that "offer comparable reliability of the identity" are used.
- [CONDITIONAL] COL-8.2.3-05. Documents are presented in their original form.
- [CONDITIONAL] COL-8.2.3-06. N/A (digital identity documents)

USE-9.2.3.1-06: The capture of the face image of the applicant shall be according to the requirements in clause **8.4.2** of the present document.

- BIN-8.4.2-01. The SDK captures a video stream. Then, images are extracted from that video.
- BIN-8.4.2-02. Passive Liveness detection is implemented. Both Presentation Attack Detection (PAD) and Injection Attack Detection (IAD). It takes place at the time of the identity proofing. Pre-recorded videos are not allowed, and there are Injection Attack Detection measures to avoid that. The option of Active Liveness with randomness is optional.
- BIN-8.4.2-03. There is Injection Attack Detection (IAD) implemented in the Identity Verification process.
- [CONDITIONAL] BIN-8.4.2-04. The capture of the evidences takes place in a controlled SDK, and the communication between the SDK and the Identity Verification Service (backend) is end-to-end and it is encrypted.
- [CONDITIONAL] BIN-8.4.2-05. The extraction of face images for both liveness detection and face matching implements techniques for Image Quality Analysis (IQA).
- BIN-8.4.2-06. Presentation Attack Detection (PAD) is implemented according to ISO 30107-3 (iBeta Level 1 and iBeta Level 2).
- BIN-8.4.2-07. Facephi's R&D team continuously evaluates the PAD components according to the ISO-IEC 19989-3 (i.e. functional testing, penetration testing, and taking into consideration Elapsed time, Expertise, Knowledge of the TOE, Window of Opportunity, and Equipment for each of the possible use cases.)
- BIN-8.4.2-08. Facephi's evaluates their engines APCER at the NIST FRTE PAD. It has industry level performance.
- BIN-8.4.2-09. Facephi's evaluates their engines BPCER at the NIST FRTE PAD. It has industry level performance.
- BIN-8.4.2-10. The APCER and BPCER are continuously monitored and evaluated.

USE-9.2.3.1-07: The identity proofing may use trusted registers and/or proof of access and/or documents and attestations as supplementary evidence.

- When available, the Identity Verification process checks the identity attributes against government databases.

USE-9.2.3.1-08: The identity proofing may use additional digital or physical identity documents as supplementary evidence.

- N/A. Optional.

USE-9.2.3.1-09: The identity proofing may use existing eID means as supplementary evidence.

- N/A. Optional.

USE-9.2.3.1-10: The identity proofing may use existing digital signature means as supplementary evidence.

- N/A. Optional.

2.2. Use Case for Hybrid manual and automated operation

Note: For the purpose of completing this self-assessment, only the requirements related to physical documents will be considered ([CONDITIONAL] USE-9.2.3.3-03).

[CONDITIONAL] If the identity proofing is based on the remote presence of the applicant with unattended online communication, and validation of evidence is either automated using a digital identity document or combined automated and manual for physical identity document, and binding to applicant is either by manual face verification or a combination of manual face verification and face biometrics, then the following requirements apply.

USE-9.2.3.3-01: The identity proofing process shall specify how the registration officer shall handle deviations from expected results or expected behaviour of the applicant, including the conditions where the identity proofing process shall be aborted, and the information to convey to the applicant when an identity proofing process is aborted.

- N/A

[CONDITIONAL] USE-9.2.3.3-02: If a digital identity document is used as evidence, evidence validation shall be according to the requirements in clause 8.3.2 of the present document.

- N/A

[CONDITIONAL] USE-9.2.3.3-03: If physical identity document is used as evidence, evidence validation shall be according to the requirements in clause 8.3.3 of the present document, including the following conditional requirements:

- VAL-8.3.3-01. The IDV process implements an automatic document classifier.
- [CONDITONAL] VAL-8.3.3-02. The IDV process captures a video streaming of the document, and then extracts a frame (image) of good quality.
- VAL-8.3.3-03. The IDV process implements a Document Presentation Attack Detection method that detects forgery, falsified and counterfeited documents.
- [CONDITIONAL] VAL-8.3.3-04. N/A.
- [CONDITIONAL] VAL-8.3.3-05. The capture of the evidences takes place in a controlled SDK, and the communication between the SDK and the Identity Verification Service (backend) is end-to-end and it is encrypted.
- [CONDITONAL] VAL-8.3.3-06. N/A
- [CONDITIONAL] VAL-8.3.3-09. When available, the Identity Verification process checks the identity attributes against government databases.

- VAL-8.3.3-10. The IDV process implements OCR to extract identity attributes from the document.
- [CONDITONAL] VAL-8.3.3-11. Portrait is extracted.
- [CONDITONAL] VAL-8.3.3-12. MRZ is read.
- [CONDITONAL] VAL-8.3.3-13. N/A.
- [CONDITONAL] VAL-8.3.3-14. N/A.
- [CONDITONAL] VAL-8.3.3-15. N/A.
- [CONDITONAL] VAL-8.3.3-16. N/A.
- [CONDITONAL] VAL-8.3.3-17. N/A.
- [CONDITONAL] VAL-8.3.3-20. The Machine Learning technology used for evaluating the authenticity of the documents are systematically tested against reference datasets and kept updated to cope with changes in the threats and risk situation.

[CONDITIONAL] USE-9.2.3.3-04: If a physical identity document is used as evidence, requirements COL-8.3.3-18 and COL-8.3.3-19 of the present document shall apply as additional to manual validation of the identity document.

- VAL-8.3.3-18. Machine Learning engines are used to evaluate the authenticity of the physical identity documents.
- [CONDITONAL] VAL-8.3.3-19. Image Quality Analysis (IQA) techniques are implemented to extract the images used to evaluate the authenticity of the evidences.

USE-9.2.3.3-05: Binding to applicant shall be according to one of the following alternatives:

- By applying both manual binding to applicant (clause 8.4.4) and face biometrics (clause 8.4.3) in parallel.
  - N/A
- By applying face biometrics (clause 8.4.3) with fallback to manual binding (clause 8.4.4) where the outcome of the face biometrics does not yield a reliable match.
  - N/A
- By applying only manual binding to applicant (clause 8.4.4).
  - N/A

USE-9.2.3.3-06: If binding to applicant is achieved by a combination of manual face verification and automated face biometrics, and the two binding methods yield different results, either the result of the manual face verification shall prevail, or the identity proofing process shall be aborted.

- N/A