



ISO/IEC JTC 1/SC 27/WG 3 "Security evaluation, testing and specification"
Convenorship: UNE
Convenor: Bañón Miguel Mr



CEN/TC 224/WG 18 European requirements for biometric products Part 5 WD

Document type	Related content	Document date	Expected action
Project / Other		2024-03-27	INFO

Replaces: N 2593 CEN/TC 224/WG 18 European requirements for biometric products Part 5 WD



CEN/TC 224/WG 18 "Biometrics"
WG Secretariat: **AFNOR**
Convenor: **Gacon Pierre M.**



TS ERBP-5 WD7

Document type	Related content	Document date	Expected action
Meeting / Document for discussion	Meeting: Berlin (Germany) 5 Jun 2024 Project: 00224280 - -	2024-03-22	COMMENT/REPLY by 2024-05-21

CEN/TC XXX

Date: 20XX -XX

(ERBP-5 WD7) prEN XXXXX: XXXX

Secretariat: XXX

Personal identification — European requirements for biometric products — Part 5: Face biometrics

Einführendes Element — Haupt-Element — Ergänzendes Element

Élément introductif — Élément central — Élément complémentaire

ICS:

CCMC will prepare and attach the official title page.

Contents

Page

- European foreword.....
- Introduction.....
- 1 Scope.....
- 2 Normative references.....
- 3 Terms and definitions.....
- 4 Symbols and abbreviations.....
- 5 General concepts.....
- 6 Common resources for the face biometrics evaluations.....
 - 6.1 Introduction.....
 - 6.2 Test crew.....
 - 6.3 Capture devices.....
 - 6.4 Background and scenarios.....
 - 6.5 Biometric reference data.....
 - 6.6 Tools for improving results interoperability.....
 - 6.6.1 Reference application (REF_APP).....
 - 6.6.2 Toolboxes.....
- 7 Phase 2 – TOE performance.....
 - 7.1 Introduction.....
 - 7.2 Technology evaluation.....
 - 7.2.1 Test T2-1-1: Technology evaluation.....
 - 7.3 SUBJECT variation tests.....
 - 7.3.1 Test T2-2-1: Check correct behaviour under different SETTINGS.....
 - 7.3.2 Test T2-2-2: Check correct behaviour under different capture devices.....
 - 7.4 Scenario variation tests.....
 - 7.4.1 Test T2-3-1: Check correct behaviour under different reference data.....
 - 7.4.2 Test T2-3-2: Differentiation among twins.....
 - 7.4.3 Test T2-3-3: Proof-of-life detection.....
- 8 Phase 3 – Bona-fide robustness.....
 - 8.1 Introduction.....
 - 8.2 SUBJECT variation tests.....
 - 8.2.1 Test T3-1-1: Variations of lighting conditions.....
 - 8.2.2 Test T3-1-2: Variations of background.....
 - 8.3 Scenario variation tests.....
 - 8.3.1 Test T3-2-1: Variations in facial expressions.....
 - 8.3.2 Test T3-2-2: Variation in face orientation towards the TOE.....
 - 8.3.3 Test T3-2-3: Significant SUBJECT esthetical variations.....
- 9 Phase 4 –Attack Detection.....
 - 9.1 Introduction.....
 - 9.2 Common parameters for Phase 4 tests.....
 - 9.2.1 Introduction.....
 - 9.2.2 Materials.....

- 9.2.3 ATTEMPTS.....
- 9.2.4 Data to be included in the ETR.....
- 9.3 Zero-Effort attacks.....
- 9.3.1 Test T4-1: Zero-effort imposter attack.....
- 9.4 Enrolment-based attacks.....
- 9.4.1 Test T4-2-1: Basic attack to the biometric reference storage.....
- 9.4.2 Test T4-2-2: Use of morphing techniques during enrolment.....
- 9.5 Attacks during recognition process.....
- 9.5.1 Test T4-3-1: Still images as ARTIFACTS.....
- 9.5.2 Test T4-3-2: Videos as ARTIFACTS.....
- 9.5.3 Test T4-3-3: Low-cost masks as ARTIFACTS.....
- 9.5.4 Test T4-3-4: Advanced masks as ARTIFACTS.....
- 9.5.5 Test T4-3-5: Make-up-based attacks.....
- 9.5.6 Test T4-3-6: Biometric data injection attacks.....

Annex A (normative) Profile 1: Remote identity verification using video-conferencing tools and pre-issued documents, with human supervision before final decision.....

- A.1 Introduction.....
- A.2 TOE description.....
- A.3 Levels of assurance.....
- A.4 Phase 1: Interoperability requirements.....
- A.5 Decision criteria for functional tests (Phases 2 and 3).....
- A.5.1 Phase 2 parameters and passing criteria.....
- A.5.1.1 Overall requirements.....
- A.5.1.2 T2-1-1: Technology evaluation.....
- A.5.1.3 T2-2-1: Check correct behaviour under different SETTINGS.....
- A.5.1.4 T2-3-3: Proof-of-life detection.....
- A.5.2 Phase 3 parameters and passing criteria.....
- A.5.2.1 Overall requirements.....
- A.5.2.2 T3-1-2: Variations of background.....
- A.6 Phase 4 parameters and passing criteria.....
- A.6.1 Overall requirements.....
- A.6.2 T4-1: Zero-effort imposter attack.....
- A.6.3 T4-3-2: Videos as ARTIFACTS.....
- A.6.4 T4-3-3: Low-cost masks as ARTIFACTS.....
- A.6.5 T4-3-4: Advanced masks as ARTIFACTS.....
- A.6.6 T4-3-5: Make-up based attacks.....
- A.6.7 T4-3-6: Biometric data injection attacks.....
- A.7 Overall assessment criteria.....

Annex B (normative) Profile 2: Face recognition for the on-boarding of credentials in and Identity Digital Wallet (eIDAS).....

- B.1 Introduction.....
- B.2 TOE description.....
- B.3 Levels of assurance.....
- B.4 Phase 1: Interoperability requirements.....
- B.5 Decision criteria for functional tests (Phases 1 and 2).....
- B.5.1 Phase 2 parameters and passing criteria.....
- B.5.1.1 Overall requirements.....

- B.5.1.2 T2.x.....
- B.5.2 Phase 3 parameters and passing criteria.....
- B.5.2.1 Overall requirements.....
- B.5.2.2 T3.x.....
- B.6 Phase 4: Decision criteria for security requirements.....
- B.6.1 Overall requirements.....
- B.6.2 T4.x.....
- B.7 Requirements for the overall decision.....
- Annex C (normative) Profile 3: Face recognition for the use of Identity Digital Wallet (eIDAS).....
- C.1 Introduction.....
- C.2 TOE description.....
- C.3 Levels of assurance.....
- C.4 Phase 1: Interoperability requirements.....
- C.5 Decision criteria for functional tests (Phases 1 and 2).....
- C.5.1 Phase 2 parameters and passing criteria.....
- C.5.1.1 Overall requirements.....
- C.5.1.2 T2.x.....
- C.5.2 Phase 3 parameters and passing criteria.....
- C.5.2.1 Overall requirements.....
- C.5.2.2 T3.x.....
- C.6 Phase 4: Decision criteria for security requirements.....
- C.6.1 Overall requirements.....
- C.6.2 T4.x.....
- C.7 Requirements for the overall decision.....
- Annex D (normative) Profile 4: Face biometrics under constrained and supervised recognition systems / Face recognition for Automated Border Control - eGates.....
- D.1 Introduction.....
- D.2 TOE description.....
- D.3 Levels of assurance.....
- D.4 Phase 1: Interoperability requirements.....
- D.5 Decision criteria for functional tests (Phases 1 and 2).....
- D.5.1 Phase 2 parameters and passing criteria.....
- D.5.1.1 Overall requirements.....
- D.5.1.2 T2-1-1: Technology evaluation.....
- D.5.1.3 T2-3-2: Differentiation among twins.....
- D.5.1.4 T2-3-3: Proof-of-life detection.....
- D.5.2 Phase 3 parameters and passing criteria.....
- D.5.2.1 Overall requirements.....
- D.5.3 T3-1-1: Variations of lighting conditions.....
- D.5.3.1 T3-2-1: Variations in facial expressions.....
- D.5.3.2 T3-2-2: Variations in face orientation towards the TOE.....
- D.5.3.3 T3-2-3: Significant SUBJECT esthetical variations.....
- D.6 Phase 4: Decision criteria for security requirements.....
- D.6.1 Overall requirements.....
- D.6.2 T4-1: Zero-effort imposter attack.....
- D.6.3 T4-2-2: Use of morphing techniques during enrolment.....

- D.6.4 T4-3-1: Still images as ARTIFACTS.....
- D.6.5 T4-3-2: Videos as ARTIFACTS.....
- D.6.6 T4-3-3: Low-cost masks as ARTIFACTS.....
- D.6.7 T4-3-4: Advanced masks as ARTIFACTS.....
- D.6.8 T4-3-5: Make-up-based attacks.....
- D.7 Requirements for the overall decision.....
- Annex E** (normative) Profile 5: Presentation Attack Detection systems.....
- E.1 Introduction.....
- E.2 TOE description.....
- E.3 Levels of assurance.....
- E.4 Phase 1: Interoperability requirements.....
- E.5 Decision criteria for functional tests (Phases 1 and 2).....
- E.5.1 Phase 2 parameters and passing criteria.....
- E.5.1.1 Overall requirements.....
- E.5.1.2 T2.1.1.....
- E.5.1.3 T2.2.2.....
- E.5.2 Phase 3 parameters and passing criteria.....
- E.5.2.1 Overall requirements.....
- E.5.3 T3.1.1.....
- E.5.4 T3.1.2.....
- E.6 Phase 4: Decision criteria for security requirements.....
- E.6.1 Overall requirements.....
- E.6.2 T4.1.....
- E.6.3 T4.3.1.....
- E.6.4 T4.3.2.....
- E.6.5 T4.3.3.....
- E.6.6 T4.3.4.....
- E.7 Requirements for the overall decision.....
- Bibliography.....

European foreword

This document (prEN XXXX:20YY) has been prepared by Technical Committee CEN/TC XXX “Title”, the secretariat of which is held by XXX.

This document is currently submitted to the CEN Enquiry/Formal Vote/Vote on TS/Vote on TR.

This document has been prepared under a standardization request addressed to CEN by the European Commission. The Standing Committee of the EFTA States subsequently approves these requests for its Member States.

For the relationship with EU Legislation, see informative Annex ZA, which is an integral part of this document.

[NOTE to the drafter: Add information about related documents or other parts in a series as necessary. A list of all parts in a series can be found on the CEN website: www.cencenelec.eu.]

Introduction

The use of remote services has increased significantly. This was boosted during 2020-2021, when many service providers and Administrations migrated most of their processes to online handling. We can find nowadays many online services, such as opening of a bank account, claiming expenses, paying taxes, starting legal actions, etc.

For all these services there is the need of identifying the persons claiming for that service, and doing it in a comfortable, universal, reliable and auditable way. Even though some of those services, in some countries, were deployed using PKIs (Public Key Infrastructures), as recommended by eIDAS, this approach was far away from being used by a significant part of the population.

This situation led to creating identification services using videoconferencing tools, such as using any device camera to scan a document, and capture your face for biometric recognition. This is deployed in many countries and sectors, but using ad-hoc solutions, limiting interoperability and increasing costs and risks.

In this context, service providers and Administrations have to define their own requirements, select the products and deploy the solution. On the other hand, manufacturers had to implement different solutions to different customers, in order to fulfil each of those requirement sets. Both sides would benefit from standards and regulations, on which to rely for the product definition.

Everybody will benefit from having a common way of defining those requirements, and a detailed evaluation methodology. These two items can be used by conformity assessment bodies or by business owners, to create their own certification schemes for this kind of technology/products, by following the international ISO/IEC 17000 series of standards.

This project is addressing this need for the case of Biometric Products, analysing and merging all current works, and defining a detailed set of requirements, a biometric-mode-specific evaluation methodology, and the passing criteria for different application profiles. This work will be developed in accordance with GDPR principles.

This will be written as a multipart project with the following structure:

- Parts 1-3: Defining the generic principles and methodologies, not requiring a biometric mode specific approach. In particular these parts will be:
 - Part 1: General requirements and application profile definition
 - Part 2: Interoperability tests
 - Part 3: Functionality evaluation methodology
- Parts 4-n: Defining the particularities of each biometric mode (e.g., specific tests, specific requirements), and containing, each of the parts, a set of application profiles, that will establish the test and requirements applicable for a specific application and context. Those application profiles will be written as individual annexes, following the structure provided in Part 1. The numbering of these parts, has been done trying to keep conformance with the numbering used by ISO/IEC 19794 series of standards (ISO/IEC_JTC1/SC37_WG3). Therefore:
 - Part 4: Fingerprint biometrics
 - Part 5: Face biometrics

prEN XXXX:XXXX (E) (ERBP-5 WD7)

— Etc.

1 Scope

This TS series provide a generic framework for the establishment of requirements and their evaluation methodology for biometric products. The requirements will be established depending on the biometric mode considered, and they will be adapted to each scenario, through the definition of a variety of application profiles.

This series of standards are expected to provide the evaluation methodology, the individual tests, and the application profiles (with their particular requirements).

This document is focussed on face biometrics, and provides the specifics of this biometric mode for the application of all the specifications provided in parts 1 till 3. It also defines a set of application profiles, that detail de applicable tests, the evaluation parameters and the assessment criteria.

In detail, this document defines, for face biometrics:

- General aspects of a face biometric product
- Common resources needed for the evaluation
- Each of the possible tests to be applied
- Application profiles for different kinds of face biometrics products

The Technical Specifications within this series can be taken by any certification body and/or sector, to define and evaluate the requirements for their biometric products within their selected applications. This may be used in coordination with other current National initiatives. For governmental applications, the relevant Government will decide if this evaluation is applicable or not.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

(WI=00224273) TS on Digital Injection Attacks

ISO/IEC 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 19795 (all parts), *Information technology — Biometric performance testing and reporting*

ISO/IEC 19989-3, *Information security — Criteria and methodology for security evaluation of biometric systems — Part 3: Presentation attack detection*

ISO/IEC 30107-1, *Information technology — Biometric presentation attack detection — Part 1: Framework*

ISO/IEC 30107-3, *Information technology — Biometric presentation attack detection — Part 3: Testing and reporting*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in parts 1 and 3 of this series, ISO/IEC 19795, ISO/IEC 30107, ISO/IEC 2382-37 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp/>
- IEC Electropedia: available at <https://www.electropedia.org/>

EDITOR'S NOTE : As from the LATE BSI comments in March, it is considered interesting to define the «proof-of-life» term. Call for contributions.

4 Symbols and abbreviations

For the purposes of this document, the symbols and abbreviations given in parts 1 and 3 of this series and the following apply.

- ATTACKER_SIM_TH – Similitude threshold for an ATTACKER
- BONAFIDE_SIM_TH – Similitude threshold for BONAFIDE users
- ETR – Evaluation Technical Report
- fps – frames per second
- REF_APP – Reference Application
- TL – Testing Laboratory
- TOE – Target of Evaluation

5 General concepts

This document defines the tests that can be requested for a comprehensive evaluation of a product based on facial biometrics. Clauses 5 to 8 define such test in a generic and parametrized way. Some of the tests, e.g. those for Phase 4, cannot be fully detailed, as the attack artifacts and strategies may differ with time. These definitions do not include limiting values, neither passing/fail criteria.

After all these clauses, a collection of annexes is provided, each of those annexes defining an application profile. In those profiles, following what is defined in Part 1, the applicable texts, their respective parameters and the passing/fail criteria, is given for such application.

6 Common resources for the face biometrics evaluations

6.1 Introduction

In order to execute the below detailed tests, some common resources are needed, that will be used throughout all or part of them. This clause describes such resources, allowing that a particular test may need additional resources for its execution. Those additional resources are explained in the subclause related to such particular test.

6.2 Test crew

Most of the test here provided are scenario evaluations, which require the use of test crews, involving individual subjects. The diversity of the test crew, following ISO/IEC 19795 series, shall be, as representative, as possible, to the target population where the product is to be applied.

It is true, that the larger the test crew size, the longer the evaluation takes and the higher the costs. Depending on requirements given by a certain application, such size may be limited.

The test crew involves 2 kinds of subjects:

- Bona-fide users: subjects that are going to use the system following its rules, and with the purpose of achieving a positive biometric comparison. These subjects will be used throughout the 3 phases of the evaluation.
- Attackers: subjects whose intent is to attack the system by any means (the means will depend on each of the tests applied), in order to obtain a positive biometric comparison against a bona-fide user.

For achieving reasonable interoperable results, it is important to determine some thresholds in the similarity among test subjects. This is particularly important in those cases where the test crew size is strongly limited. To achieve this goal, a reference application (from now on called REF_APP) shall be used to determine a baseline value for the similarity of test crew members (see subclause 6.6.1). Each application profile shall determine the accepted threshold for such similarity among bona-fide users, and also among the attacker and the bona-fide subject to be attacked, after applying the relevant artifacts.

Therefore, each application profile shall define, for either each or all of the tests, the following parameters:

- REF_APP: Reference application, if not using the one defined in 6.6.1
- MIN_BONAFIDE_USERS: Minimum number of bona-fide users in the test crew.
- BONAFIDE_SIM_TH: The threshold used to determine if the bona-fide test crew is diverse enough, by checking the similarity among the bona-fide users with the REF_APP.
- MIN_ATTACKERS: Minimum number of attackers in the test crew for Phase 4.
- ATTACKER_SIM_TH: The threshold used to determine the accuracy of the attack attempt, by measuring the similarity between the attacker and the bona-fide user to be attacked, once the attacker has applied all relevant attacking means.

6.3 Capture devices

Although there are some facial biometric products that have the capture device embedded (e.g., an ABC system), many others allow the capture device to be chosen by the user (e.g., an identification service using videoconferencing tools). In such kind of cases, the TL shall evaluate the behaviour of different capture devices, as it may result in significant differences when evaluating the biometric product.

The TL shall have several capture devices, all of them within the specifications given by the TOE. Different test may use different capture device, depending on the particular needs.

The capture devices used for the evaluation shall be described in the ETR, detailing for which tests each capture device has been used.

The PM or the Vendor shall specify the range of capture devices allowed by the TOE within the TOE Specification.

As a general rule, the TL shall use the worst allowed capture device, that fit the TOE requirements, in terms of resolution and/or quality.

6.4 Background and scenarios

Following the indications given in Part 3, the TOE will be evaluated under each SETTING defined for each of the TESTS.

The application profile shall define which SETTINGS are needed for each of the TESTS.

Some of the TESTS have additional requirements, independently of the application profile being applied

Certain facial biometric products may impose a fixed background (i.e., some ABC systems). But many others may not have any restriction, as the product is expected to be used at the own convenience of the user. This means that the background of the facial images taken may differ significantly (e.g., in videoconferencing-related products).

The TL shall have to adapt the background and the environment of the TOE to the target application.

In order to emulate these scenarios, the TL may use the following resources:

- A projection equipment that is able to reproduce the required SETTING at the back of the user to be identified. Such equipment should not impact the presentation of the biometric trait to the TOE (e.g., non-additional lighting to the face of the SUBJECT or significant backlight that might obscure the face of the SUBJECT). The requirements for such projection equipment are:
 - The screen size should be big enough (in relation to the distance between the SUBJECT and the TOE), so that no borders are captured by the TOE.
 - The projection equipment should be effective for the TOE, so that the TOE is able to acquire such background projected. For example, if the TOE uses an infrared camera, it might not be possible to use a TV as a projection system, as the background may be seen by the TOE as black.
 - In case the projection system is a TV, the resolution of such TV should be 4K or higher. This is to avoid artefacts in the image seen by the TOE.
 - In case the projection system is a projector with a rear-projection screen, it should comply with the following requirements:
 - Its size should be 90" or higher.
 - The aspect ratio might be 4:3 or 16:9, as long as the TOE is not able to capture the screen borders.
 - The minimum gain should be 1,0.
 - The view angle should be 90 degrees or higher.
 - Its installation should be done in a way that no wrinkles are seen by the TOE.
 - The projector should have a minimum resolution of Full HD (1920 x 1080), and able to be used for rear projection.
 - The projector luminosity should be 3000 lumens or higher
- At least one video for each of the required SETTINGS, following the requirements provided above for each of the SETTINGS.

In the case that a TOE is detecting virtual backgrounds as an attack, the use of different SCENARIOS in Phase 2 and Phase 3 may not be possible. If that is the case, this fact has to be reported in the ETR.

6.5 Biometric reference data

The application profile shall define how the reference data is obtained and where it is stored. Several options can be considered, such as:

- The TOE needs to perform the enrolment of each of the bona-fide users before the evaluation is started.
- The TOE gets the reference data for each of the bona-fide users from a digital storage device (e.g., from a database).
- The TOE gets the reference data for the bona-fide user involved in the test, by reading/scanning/etc. a previously created document (e.g., an ID card or passport), being such document issued by an entity not related to the TOE.

In case the reference data is obtained from an externally generated document, it may happen that the bona-fide users may have more than one document from which to obtain reference data. If such is the case, the application profile such define how this case is handled, whether it is not important from which document the reference data is obtained, or if each document represent a different case, i.e., the combination of bona-fide user and particular document, generates one test SUBJECT, and therefore a single bona-fide user may be part of more than one test SUBJECTS.

6.6 Tools for improving results interoperability

6.6.1 Reference application (REF_APP)

As mentioned in 6.2, for achieving reasonable interoperable results, it is important to determine some thresholds in the lack of similarity among test subjects. To achieve this goal, each application profile may provide a reference application for the calculation of the distance among test subjects. Such application is called REF_APP throughout that text.

It is important that the REF_APP does not show an excessive performance, that may outperform the TOE discrimination capabilities.

In case the selected application profile does not provide a REF_APP, the following has to be used. This basic REF_APP has been developed in Python using publicly available libraries. This REF_APP has been developed providing results in terms of distance, not similarity. So, when good similarity is to be demonstrated, the result shall be EQUAL OR HIGHER to BONAFIDE_SIM_TH. And when bad similarity is to be demonstrated, the result shall be EQUAL OR BELOW to ATTACKER_SIM_TH.

In case the relevant application profile or the certification scheme do not provide a REF_APP, the following one shall be used, with the decision criteria stated in the application profile. The REF_APP is developed using Python and open-source libraries, and can be downloaded from: <https://loreto.ccn-cert.cni.es/index.php/s/tfZwTe2iLGT5oRY>

6.6.2 Toolboxes

To reach interoperability among evaluations, it may become beneficial to use toolboxes that have been previously agreed by the biometric community. One example of these toolboxes, is the one developed by BIO-iTC (BIO-iTC, n.d.).

EDITOR'S NOTE – BIO-iTC COMMENT: There are 6 mobile devices that were evaluated or in evaluation based on [2], however, without PAD testing. Currently [2] defines the PAD requirement as an optional requirement because there was no common understanding of vulnerability assessment methodology for the PAD among the CCRA nations in early phase of development of [2]. However, one CC evaluation for fingerprint mobile biometrics with the PAD requirement is ongoing and PAD requirement will be mandatory in the near future.

The important factor to improve and enhance the evaluation methodology or testing is actual evaluation experiences, as our Fingerprint toolbox [3] is being improved based on the feedback from the ongoing

evaluation. CEN/TC 224/WG 18 can refer [3] when developing PAD testing for fingerprint biometric and BIO-iTC can also improve its Face toolbox [4] referring N 922.

Response: We consider PAD evaluation (i.e., Phase 4) essential, although different application profiles may be more or less strict in the acceptance criteria. It is good to know that you're also planning to make PAD evaluation mandatory in the near future.

Although there will be some inputs from our side for fingerprints, we have not started yet that project (which will be ERBP-4, and we may start it within 2025), as we're currently focused on solving the face recognition case. Face recognition is demanded currently by some EU Member States, and it is expected to be consider as an authentication factor for the future EU Digital Identity Wallet.

We will take a look to your Face toolbox in the next cycle, as to see how can it be integrated into ERBP-5, and/or our possibilities in contributing to such toolbox.

7 Phase 2 – TOE performance

7.1 Introduction

The main objective of this phase is to verify that the functionality claimed by the TOE manufacturer is maintained for the application profile defined, within the SETTINGS defined.

This phase is essential to be able to determine, if the product is not suitable for the application profile defined, and therefore to discontinue the rest of the phases of the evaluation.

The following subclauses define each of the possible tests that each application profile may claim to be applied.

7.2 Technology evaluation

7.2.1 Test T2-1-1: Technology evaluation

7.2.1.1 Description

The goal is to verify that the performance claimed by the TOE manufacturer for its face recognition algorithm (which shall be written in the SD_TOE, i.e., the Security Declaration for the TOE) are in line with the performance noted during a technology evaluation, according to ISO/IEC 19795-1.

In order to perform this test, the TOE shall provide an accessible version of the biometric subsystem, so that the TL can inject biometric samples from a database, and obtain the biometric comparison result. Then, a ISO/IEC 19795-1 evaluation can be performed.

To carry out this evaluation, the Sponsor and the TL shall agree on an API (Application Programming Interface), that allows the input of the biometric samples, and the output of the results.

EXAMPLE The NIST FRVT On-going evaluation provides this kind of API in XXXX.

This test can be performed by two means:

- Through the baseline of a report from an open competition such as the NIST FRVT program. The open competition report used shall be the last released report.
- With the following rules (see subclauses 7.2.x) based on the requirements from ISO/IEC 19795-1.

The application profile shall define if this test shall be performed on the basis of an open competition report or on the performance tests done by the TL.

7.2.1.2 SETTINGS

In addition to what is defined in 6.4, the SETTINGS and metrics used shall be based on the requirements of the ISO/IEC 19795-1.

7.2.1.3 Materials

For each of the TRIALS to be executed in this test, the following material is used:

- The face recognition algorithm used by the TOE including an API interface in order to send the images from the dataset used for the test.
- A dataset with the sufficient number of SUBJECTS and diversity according to the requirements from ISO/IEC 19795-1, and the confidence level required by the application profile.
- The targeted performance errors rates written in the SD_TOE.
- **The dataset shall be GDPR compliant**

7.2.1.4 TRIALS

During this test, a set of TRIALS for each SUBJECT and SETTING will be executed. The minimum number of TRIALS is given by MIN_TRIALS, specified in the applicable application profile and according to ISO/IEC 19795-1. The relevant application profile shall define the parameters of this test (e.g., whether the rule of 3 or the rule of 30 is used).

The steps to follow for each TRIAL are:

1. The TL will setup up the SETTING and will select the dataset containing the SUBJECTS.
2. An ATTEMPT is performed with a SUBJECT.
3. If the TRIAL for such SUBJECT results in an ERROR, the variables SUBJECT_ERRORS and TEST_ERRORS will be incremented, and the following checking is performed by the TL, in the order given:
 - a. If TEST_ERRORS gets higher than MAX_TEST_ERRORS, all TRIALS for this TEST will be finished, and the TEST will result in a FAIL.
 - b. If SUBJECT_ERRORS gets higher than MAX_SUBJECT_ERRORS, the TL will jump to step number 6.
4. If in that TRIAL for that SUBJECT the number of NON_MATCHES is higher than MAX_SUBJECT_NON_MATCHES, the TL will jump to step 6.
5. The TL returns to step 3, to repeat the process until MIN_TRIALS is reached for that SUBJECT.
6. The SUBJECT is changed, and the TL returns to step 1, until all SUBJECTS have been used for that SETTING.

As this is a technology evaluation, an ATTEMPT is picking up a file from the database and entering it into the TOE.

After checking the SD_TOE, the TL shall define, before executing the tests, which is the reasoning to consider an ATTEMPT as FTA (i.e., a Failure to Acquire). That decision will have to be documented into the ETR and applied to all ATTEMPTS.

The TL shall define which part of the dataset is used for enrolment, and which one is used for recognition. It is important to note that for each test subject that is going to be enrolled, the number of samples used for enrolment shall be smaller than the number of samples used as probes.. Also, both datasets shall not contain records/files in common. All this shall be documented in the ETR.

ISO/IEC 19795-1 and ISO/IEC 19795-2 shall be followed, including those aspects that relate the size of the datasets with the confidence level to be demanded by the application profile.

7.2.1.5 ATTEMPTS

For each TRIAL, a maximum number of ATTEMPTS is given by MAX_ATTEMPTS. MAX_ATTEMPTS will be defined according to the requirements of ISO/IEC 19795-1.

ATTEMPTS will be repeated for each TRIAL, until that number is reached, or a result of MATCH or NON_MATCH is returned.

If the number of ATTEMPTS becomes higher than MAX_ATTEMPTS for a TRIAL, then the TRIAL result is declared as an ERROR.

7.2.1.6 Data to be included in the ETR

For this test, the ETR shall contain the data required by ISO/IEC 19795-1 for technology evaluations.

At the end of this reporting, the application of the evaluation criteria given at the application profile shall be reported.

7.3 SUBJECT variation tests

7.3.1 Test T2-2-1: Check correct behaviour under different SETTINGS

7.3.1.1 Description

The goal is to verify that the TOE behaves correctly in the typical use-cases for the application profile, considering that the test SUBJECT behaves cooperatively and following the rules given by the TOE manual. Test SUBJECTS will be, only, bona-fide users.

7.3.1.2 Materials

For each of the TRIALS to be executed in this test, the following material is used:

- The TOE including a capture device (in case the capture device is not included in the TOE). If the capture device is not embedded in the TOE, the capture device to be used shall be one at the visible range, and with the lowest values in terms of resolution and auto-focus (from those allowed by the TOE specifications).
- The needed means to apply each of the SETTINGS required (e.g., one with the recommendations given in 6.4).
- A repository (in whatever form allowed by the application profile and/or TOE) of the reference data for each of the test crew members.

7.3.1.3 TRIALS

During this test, a set of TRIALS for each SUBJECT and SETTING will be executed. The minimum number of TRIALS is given by MIN_TRIALS, specified in the applicable application profile.

The steps to follow for each TRIAL are:

1. The TL will setup up the SETTING and will prepare the SUBJECT, telling him/her how to act and where to be placed
2. The SUBJECT will prepare himself/herself to interact with the TOE, and, if needed, will prepare the access to the reference data. This will be done following the operational guide of the TOE.
3. The SUBJECT will perform an ATTEMPT to identify/verify, following the indication of the operational guide of the TOE. The interaction with the TOE while performing an ATTEMPT may include actions that will be used for proof of life.
4. The SUBJECT will wait for the TOE outcome, and the TL will note the result obtained, increasing the number of MATCHES, NON_MATCHES or SUBJECT_ERRORS as applicable.
5. The SUBJECT will get himself/herself totally out of the point of interaction with the TOE (e.g., will stop staring at the capture device, moving himself/herself significantly). This shall be done to ensure that the next TRIAL is a completely new interaction with the TOE.
6. If the TRIAL for such SUBJECT results in an ERROR, the variables SUBJECT_ERRORS and TEST_ERRORS will be incremented, and the following checking is performed by the TL, in the order given:
 - a. If TEST_ERRORS gets higher than MAX_TEST_ERRORS, all TRIALS for this TEST will be finished, and the TEST will result in a FAIL.
 - b. If SUBJECT_ERRORS gets higher than MAX_SUBJECT_ERRORS, the TL will jump to step number 9.
7. If in that TRIAL for that SUBJECT the number of NON_MATCHES is higher than MAX_SUBJECT_NON_MATCHES, the TL will jump to step 9.
8. The TL returns to step 3, to repeat the process until MIN_TRIALS is reached for that SUBJECT.
9. The SUBJECT is changed, and the TL returns to step 1, until all SUBJECTS have been used for that SETTING.

7.3.1.4 ATTEMPTS

For each TRIAL, a maximum number of ATTEMPTS is given by MAX_ATTEMPTS. ATTEMPTS will be repeated for each TRIAL, until that number is reached, or a result of MATCH or NON_MATCH is returned.

If the number of ATTEMPTS becomes higher than MAX_ATTEMPTS for a TRIAL, then the TRIAL result is declared as an ERROR.

7.3.1.5 Data to be included in the ETR

In addition to all required information, the ETR shall include the following information for this test:

- Number and description (with photographs/videos) of the SETTINGS used.

- Number and type of reference data used. If reference data is obtained through a previously obtained document, images of such documents shall be attached in an anonymized way (except for the photograph included).
- Number and classification (e.g., age, gender, etc.) of the bona-fide users. The similarity values among the USERS, given by the REF_APP, shall be reported.
- Total number of SUBJECTS used in the test.
- Total number of TRIALS executed.
- A table with the information about SUBJECT_ERRORS, MATCHES and NON_MATCHES for each SUBJECT, TRIAL and SETTING. An example of such a table could be the following:

Table 1 — Example of results summary for T2-2

SUBJECT	TRIAL	SETTING 1			SETTING 2			TOTALS	
		MATCH	ERROR	NON_MATCH	MATCH	ERROR	NON_MATCH	ERROR	NON_MATCH
S1	1								
S1	2								
S1	n								
S2	1								
...	...								
Sn									
TOTALS									

- Test result after applying the evaluation criteria.

7.3.2 Test T2-2-2: Check correct behaviour under different capture devices

7.3.2.1 Description

The goal is to verify that the TOE behaves correctly in those cases where the capture device is not fixed by the TOE evaluated, allowing different kind of capture devices to be used.

EXAMPLE This test is suitable for those applications where the TOE is a remote service being executed in the mobile phone or computer belonging to the citizen. Each of those devices may have a different capture device.

During this test, it is considered that the test SUBJECT behaves cooperatively and following the rules given by the TOE manual. Test SUBJECTS will be, only, bona-fide users.

7.3.2.2 Materials

For each of the TRIALS to be executed in this test, the following material is used:

- The TOE.

- Each of the capture devices specified by the application profile, and compliant with the requirements of the TOE.
- A projection equipment (as defined in 6.4) in order to apply each of the SETTINGS required.
- A repository (in whatever form allowed by the application profile and/or TOE) of the reference data for each of the test crew members.

7.3.2.3 TRIALS

During this test, a set of TRIALS for each SUBJECT and biometric reference data will be executed. The minimum number of TRIALS is given by MIN_TRIALS, specified in the applicable application profile.

The steps to follow for each TRIAL are:

1. The TL will setup up the SETTING and will prepare the SUBJECT, telling him/her how to act and where to be placed
2. The TOE will be equipped with the biometric capture device.
3. The SUBJECT will prepare himself/herself to interact with the TOE, and, if needed, will prepare the access to the selected reference data. This will be done following the operational guide of the TOE.
4. The SUBJECT will perform an ATTEMPT to identify/verify, following the indication of the operational guide of the TOE. The interaction with the TOE while performing an ATTEMPT may include actions that will be used for proof of life.
5. The SUBJECT will wait for the TOE outcome, and the TL will note the result obtained, increasing the number of MATCHES, NON_MATCHES or SUBJECT_ERRORS as applicable.
6. The SUBJECT will get himself/herself totally or partially out of the point of interaction with the TOE (e.g., will stop staring at the capture device, moving himself/herself significantly). This shall be done to ensure that the next TRIAL es a completely new interaction with the TOE.
7. If the TRIAL for such SUBJECT results in an ERROR, the variables SUBJECT_ERRORS and TEST_ERRORS will be incremented, and the following checking is performed by the TL, in the order given:
 - a. If TEST_ERRORS gets higher than MAX_TEST_ERRORS, all TRIALS for this TEST will be finished, and the TEST will result in a FAIL.
 - b. If SUBJECT_ERRORS gets higher than MAX_SUBJECT_ERRORS, the TL will jump to step number 9.
8. If in that TRIAL for that SUBJECT the number of NON_MATCHES is higher than MAX_SUBJECT_NON_MATCHES, the TL will jump to step 9.
9. The TL returns to step 3, to repeat the process until MIN_TRIALS is reached for that SUBJECT.
10. The biometric capture device attached to the TOE is changed, and the execution returns to step 3. If all biometric capture devices have been used, it continues in step 11.
11. The SUBJECT is changed, and the TL returns to step 1, until all SUBJECTS have gone through the TRIALS with all biometric capture devices.

7.3.2.4 ATTEMPTS

For each TRIAL, a maximum number of ATTEMPTS is given by MAX_ATTEMPTS. ATTEMPTS will be repeated for each TRIAL, until that number is reached, or a result of MATCH or NON_MATCH is returned.

If the number of ATTEMPTS becomes higher than MAX_ATTEMPTS for a TRIAL, then the TRIAL result is declared as an ERROR.

7.3.2.5 Data to be included in the ETR

In addition to all required information, the ETR shall include the following information for this test:

- Number and description (with photographs/videos) of the SETTINGS used.
- Number and type of reference data used. If reference data is obtained through a previously obtained document, images of such documents shall be attached in an anonymized way (except for the photograph included).
- Number and type (with major features) of those biometric capture devices used.
- Number and classification (e.g., age, gender, etc.) of the bona-fide users. The similarity values among the USERS, given by the REF_APP, shall be reported.
- Total number of SUBJECTS used in the test.
- Total number of TRIALS executed.
- A table with the information about SUBJECT_ERRORS, MATCHES and NON_MATCHES for each SUBJECT, TRIAL and reference data, using SETTING 2. An example of such a table could be the following:

Table 2 — Example of results summary for T2-4

SUBJECT	TRIAL	CAPTURE DEVICE 1			CAPTURE DEVICE 2			TOTALS	
		MATCH	ERROR	NON_MATCH	MATCH	ERROR	NON_MATCH	ERROR	NON_MATCH
S1	1								
S1	2								
S1	n								
S2	1								
...	...								
Sn									
TOTALS									

- Test result after applying the evaluation criteria.

7.4 Scenario variation tests

7.4.1 Test T2-3-1: Check correct behaviour under different reference data

7.4.1.1 Description

The goal is to verify that the TOE behaves correctly in the typical use-case for the application profile, but when the user may be able to provide the biometric reference data from different sources.

EXAMPLE This test is suitable for those applications where the user provides also the reference data (i.e., it is not stored in the system), using different documents (e.g., a National ID Card, a driving licence, or an ePassport).

During this test, it is considered that the test SUBJECT behaves cooperatively and following the rules given by the TOE manual. Test SUBJECTS will be, only, bona-fide users.

7.4.1.2 Materials

For each of the TRIALS to be executed in this test, the following material is used:

- The TOE including a capture device (in case the capture device is not included in the TOE). If the capture device is not embedded in the TOE, the capture device to be used shall be one at the visible range, and with the lowest values in terms of resolution and auto-focus (from those allowed by the TOE specifications).
- A projection equipment (as defined in 6.4) in order to apply each of the SETTINGS required.
- The different sources for providing the biometric reference data (e.g., the different documents allowed/available).

7.4.1.3 TRIALS

During this test, a set of TRIALS for each SUBJECT and biometric reference data will be executed. The minimum number of TRIALS is given by MIN_TRIALS, specified in the applicable application profile.

The steps to follow for each TRIAL are:

1. The TL will setup up the SETTING and will prepare the SUBJECT, telling him/her how to act and where to be placed
2. The SUBJECT will prepare himself/herself to interact with the TOE, and, if needed, will prepare the access to the selected reference data. This will be done following the operational guide of the TOE.
3. The SUBJECT will perform an ATTEMPT to identify/verify, following the indication of the operational guide of the TOE. The interaction with the TOE while performing an ATTEMPT may include actions that will be used for proof of life.
4. The SUBJECT will wait for the TOE outcome, and the TL will note the result obtained, increasing the number of MATCHES, NON_MATCHES or SUBJECT_ERRORS as applicable.
5. The SUBJECT will get himself/herself totally or partially out of the point of interaction with the TOE (e.g., will stop staring at the capture device, moving himself/herself significantly). This shall be done to ensure that the next TRIAL es a completely new interaction with the TOE.
6. If the TRIAL for such SUBJECT results in an ERROR, the variables SUBJECT_ERRORS and TEST_ERRORS will be incremented, and the following checking is performed by the TL, in the order given:
 - a. If TEST_ERRORS gets higher than MAX_TEST_ERRORS, all TRIALS for this TEST will be finished, and the TEST will result in a FAIL.

- b. If SUBJECT_ERRORS gets higher than MAX_SUBJECT_ERRORS, the TL will jump to step number 9.
- 7. If in that TRIAL for that SUBJECT the number of NON_MATCHES is higher than MAX_SUBJECT_NON_MATCHES, the TL will jump to step 9.
- 8. The TL returns to step 3, to repeat the process until MIN_TRIALS is reached for that SUBJECT.
- 9. The SUBJECT changes the source of biometric reference data and returns to step 3. If all sources of biometric reference data have been used, it continues in step 10.
- 10. The SUBJECT is changed, and the TL returns to step 1, until all SUBJECTS have gone through the TRIAL.

7.4.1.4 ATTEMPTS

For each TRIAL, a maximum number of ATTEMPTS is given by MAX_ATTEMPTS. ATTEMPTS will be repeated for each TRIAL, until that number is reached, or a result of MATCH or NON_MATCH is returned.

If the number of ATTEMPTS becomes higher than MAX_ATTEMPTS for a TRIAL, then the TRIAL result is declared as an ERROR.

7.4.1.5 Data to be included in the ETR

In addition to all required information, the ETR shall include the following information for this test:

- Number and description (with photographs/videos) of the SETTINGS used.
- Number and type of reference data used. If reference data is obtained through a previously obtained document, images of such documents shall be attached in an anonymized way (except for the photograph included).
- Number and classification (e.g., age, gender, etc.) of the bona-fide users. The similarity values among the USERS, given by the REF_APP, shall be reported.
- Total number of SUBJECTS used in the test.
- Total number of TRIALS executed.
- A table with the information about SUBJECT_ERRORS, MATCHES and NON_MATCHES for each SUBJECT, TRIAL and reference data, using SETTING 2. An example of such a table could be the following:

Table 3 — Example of results summary for T2-3

SUBJECT	TRIAL	REFERENCE DATA 1			REFERENCE DATA 2			TOTALS	
		MATCH	ERROR	NON_MATCH	MATCH	ERROR	NON_MATCH	ERROR	NON_MATCH
S1	1								
S1	2								
S1	n								
S2	1								
...	...								

Sn									
TOTALS									

— Test result after applying the evaluation criteria.

7.4.2 Test T2-3-2: Differentiation among twins

7.4.2.1 Description

The goal is to verify that the TOE is able or not to differentiate twins in the typical use-cases for the application profile, considering that the test SUBJECTS behaves cooperatively and following the rules given by the TOE manual. Test SUBJECTS will be, only, bona-fide users and twins.

NOTE At the time of drafting this document, if an application profile requires this test and apply a strong acceptance criteria, it will lead to serious challenges both for getting products passing the criteria, and for the TL to be able to find test subjects.

7.4.2.2 Materials

For each of the TRIALS to be executed in this test, the following material is used:

- The TOE including a capture device (in case the capture device is not included in the TOE). If the capture device is not embedded in the TOE, the capture device to be used shall be one at the visible range, and with the lowest values in terms of resolution and auto-focus (from those allowed by the TOE specifications).
- A repository (in whatever form allowed by the application profile and/or TOE) of the reference data for each of the test crew members.

7.4.2.3 TRIALS

During this test, a set of TRIALS for each SUBJECT and SETTING will be executed. The minimum number of TRIALS is given by MIN_TRIALS, specified in the applicable application profile.

The steps to follow for each TRIAL are:

1. The TL will setup up the SETTING and will prepare the two SUBJECTS, telling them how to act and where to be placed. The two SUBJECTS shall be twins.
2. The first SUBJECT (TWIN1) will prepare himself/herself to interact with the TOE, and, if needed, will prepare the access to the reference data of the second SUBJECT (TWIN2). This will be done following the operational guide of the TOE.
3. The SUBJECT (TWIN1) will perform an ATTEMPT to identify/verify, following the indication of the operational guide of the TOE. The interaction with the TOE while performing an ATTEMPT may include actions that will be used for proof of life.
4. The SUBJECT (TWIN1) will wait for the TOE outcome, and the TL will note the result obtained, increasing the number of MATCHES, NON_MATCHES or SUBJECT_ERRORS as applicable.

5. The SUBJECT (TWIN1) will get himself/herself totally or partially out of the point of interaction with the TOE (e.g., will stop staring at the capture device, moving himself/herself significantly). This shall be done to ensure that the next TRIAL is a completely new interaction with the TOE.
6. If the TRIAL for such SUBJECT (TWIN1) results in an ERROR, the variables SUBJECT_ERRORS and TEST_ERRORS will be incremented, and the following checking is performed by the TL, in the order given:
 - a. If TEST_ERRORS gets higher than MAX_TEST_ERRORS, all TRIALS for this TEST will be finished, and the TEST will result in a FAIL.
 - b. If SUBJECT_ERRORS gets higher than MAX_SUBJECT_ERRORS, the TL will jump to step number 9.
7. If in that TRIAL for that SUBJECT (TWIN1) the number of NON_MATCHES is higher than MAX_SUBJECT_NON_MATCHES, the TL will jump to step 9.
8. The TL returns to step 3, to repeat the process until MIN_TRIALS is reached for that SUBJECT (TWIN1).
9. The SUBJECT (TWIN1) is changed, and the TL returns to step 1, until all SUBJECTS have been used for that SETTING.

7.4.2.4 ATTEMPTS

For each TRIAL, a maximum number of ATTEMPTS is given by MAX_ATTEMPTS. ATTEMPTS will be repeated for each TRIAL, until that number is reached, or a result of MATCH or NON_MATCH is returned.

If the number of ATTEMPTS becomes higher than MAX_ATTEMPTS for a TRIAL, then the TRIAL result is declared as an ERROR.

7.4.2.5 Data to be included in the ETR

In addition to all required information, the ETR shall include the following information for this test:

- Number and description (with photographs/videos) of the SETTINGS used.
- Number and type of reference data used. If reference data is obtained through a previously obtained document, images of such documents shall be attached in an anonymized way (except for the photograph included).
- Number and classification (e.g., age, gender, etc.) of the bona-fide users. The similarity values among the USERS, given by the REF_APP, shall be reported.
- Total number of SUBJECTS used in the test.
- Total number of TRIALS executed.
- A table with the information about SUBJECT_ERRORS, MATCHES and NON_MATCHES for each SUBJECT, TRIAL and SETTING. An example of such a table could be the following:

Table 4 — Example of results summary for T2-5

SUBJECT	TRIAL	SETTING 1			SETTING 2			TOTALS	
		MATCH	ERROR	NON_MATCH	MATCH	ERROR	NON_MATCH	ERROR	NON_MATCH

S1	1								
S1	2								
S1	n								
S2	1								
...	...								
Sn									
TOTALS									

— Test result after applying the evaluation criteria.

7.4.3 Test T2-3-3: Proof-of-life detection

7.4.3.1 Description

In order to enable PAD mechanisms, the TOE should implement some proof-of-life mechanisms to detect that the SUBJECT being recognized is a living SUBJECT.

EXAMPLE A proof-of-life mechanism, following the challenge-response philosophy, could be that the TOE asks the SUBJECT to perform some kind of movement (e.g., eye blinking or head movement). The TOE will have to detect the movement to see if it corresponds to the action requested.

Therefore, this test will verify if this kind of mechanisms is working as documented in the TOE operational guide. The test will force the SUBJECT to interact with the TOE without providing such proof-of-life, to check if the recognition is performed or not. If the recognition is performed, the test will result in a FAIL. If the SUBJECT is not able to be recognized, the test will result with a PASS.

Throughout this test, all TRIALS will be executed with bona-fide users as test SUBJECTS. Those bona-fide users will interact with the TOE following the TOE operational guide, except for the proof-of-life presentation.

This test will be executed for those proof-of-life mechanisms documented in the TOE documentation provided by the manufacturer, and only if those mechanisms require a specific interaction of the SUBJECT with the TOE. The proof-of-life mechanisms tested shall be reported in the ETR.

If the TOE documentation does not specify any proof-of-life mechanism involving specific interaction between SUBJECT and TOE, then this test is not applicable for that TOE.

It is important to note that not presenting the proof-of-life, may lead the TOE to stay into an infinity waiting loop. Therefore, a TIMEOUT is established for each ATTEMPT. If the TIMEOUT is exceeded for one ATTEMPT, the TRIAL will result in an ERROR. An ERROR in this test is considered as a desirable result, so no further ATTEMPT is required for that TRIAL.

Another possibility is that during the ATTEMPT, the TOE will result in an ERROR as the proof-of-life is not presented. This is also a desired result, so there is no need to repeat any other ATTEMPT.

Throughout this test, differently to what has been defined for any other test in Phase 2, the desired results (i.e., a PASS for the TRIAL) are either ERROR or NON_MATCH. The non-desired result (i.e., FAIL for the TRIAL) is MATCH. This means that, regarding the flowcharts of the methodology in Part 3 for Phases 1&2, the terms MATCHES and NON_MATCHES have to be exchanged, so that the comparisons resulting in a MATCH will end up in the FAIL of the TRIAL. Also, the following terms shall be exchanged:

- SETTING_NON_MATCHES with SETTING_MATCHES
- TEST_NON_MATCHES with TEST_MATCHES
- NON_MATCHES_SUBJECT with MATCHES_SUBJECT
- MAX_SETTING_NON_MATCHES with MAX_SETTING_MATCHES
- MAX TEST_NON_MATCHES with MAX_TEST_MATCHES
- MAX_SUBJECT_NON_MATCHES with MAX_SUBJECT_MATCHES.

7.4.3.2 Materials

For each of the TRIALS to be executed in this test, the following material is used:

- The TOE including a capture device (in case the capture device is not included in the TOE). If the capture device is not embedded in the TOE, the capture device to be used shall be one at the visible range, and with the lowest values in terms of resolution and auto-focus (from those allowed by the TOE specifications).
- A projection equipment (as defined in 6.4) in order to apply each of the SETTINGS required.
- A repository (in whatever form allowed by the application profile and/or TOE) of the reference data for each of the test crew members.

7.4.3.3 TRIALS

During this test, a set of TRIALS for each SUBJECT and SETTING will be executed. The minimum number of TRIALS is given by MIN_TRIALS, specified in the applicable application profile.

The steps to follow for each TRIAL are:

1. The TL will setup up the SETTING and will prepare the SUBJECT, telling him/her how to act and where to be placed. The TL will have to make it clear for the SUBJECT, that the interaction shall be as indicated in the TOE operational guide, **but without performing the proof-of-life interaction**. During the proof-of-life interaction the SUBJECT shall be kept as steady as possible.
2. The SUBJECT will prepare himself/herself to interact with the TOE, and, if needed, will prepare the access to the reference data. This will be done following the operational guide of the TOE.
3. The SUBJECT will perform an ATTEMPT to identify/verify, following the indication of the operational guide of the TOE. When reaching the moment of the proof-of-life interaction, the SUBJECT will have to ignore it, keeping his position and expression as steady as possible, until the TOE provide a result (either MATCH, NON_MATCH or ERROR), or the TIMEOUT is reached (whatever happens first).
4. If the TOE results in an ERROR which is not related to the TIMEOUT, a new ATTEMPT will be executed. This will be repeated until the number of MAX_ATTEMPTS is reached. If such limit is reached, then the TRIAL will result in an ERROR.
5. If the TIMEOUT has been reached, the TRIAL results in an ERROR.
6. The TL will note the result obtained, increasing the number of MATCHES, NON_MATCHES or SUBJECT_ERRORS as applicable.
7. The SUBJECT will get himself/herself totally or partially out of the point of interaction with the TOE (e.g., will stop staring at the capture device, moving himself/herself significantly). This shall be done to ensure that the next TRIAL es a completely new interaction with the TOE.

8. If the TRIAL result is a MATCH, and the number of MATCHES gets higher than MAX_SUBJECT_MATCHES, the TL will jump to step 10, increasing the variable SUBJECTS_FAIL. If SUBJECTS_FAIL gets higher than MAX_SUBJECTS_FAIL, all TRIALS for this test will be finished, resulting in a FAIL for the TEST.
9. The TL returns to step 3, to repeat the process until MIN_TRIALS is reached for that SUBJECT.
10. The SUBJECT is changed, and the TL returns to step 1, until all SUBJECTS have been used for that SETTING.

7.4.3.4 ATTEMPTS

For each TRIAL, a maximum number of ATTEMPTS is given by MAX_ATTEMPTS. ATTEMPTS will be repeated for each TRIAL, until that number is reached, or a result of MATCH or NON_MATCH is returned.

If the number of ATTEMPTS becomes higher than MAX_ATTEMPTS for a TRIAL, then the TRIAL result is declared as an ERROR.

7.4.3.5 Data to be included in the ETR

In addition to all required information, the ETR shall include the following information for this test:

- Number and description (with photographs/videos) of the SETTINGS used.
- Number and type of reference data used. If reference data is obtained through a previously obtained document, images of such documents shall be attached in an anonymized way (except for the photograph included).
- Number and classification (e.g., age, gender, etc.) of the bona-fide users. The similarity values among the USERS, given by the REF_APP, shall be reported.
- Total number of SUBJECTS used in the test.
- Total number of TRIALS executed.
- TIMEOUT used, and whether this TIMEOUT has been specified by the TOE documentation, or by the application profile.
- A table with the information about SUBJECT_ERRORS, MATCHES and NON_MATCHES for each SUBJECT, TRIAL and SETTING. An example of such a table could be the following:

Table 5 — Example of results summary for T2-6

SUBJECT	TRIAL	SETTING 2			TOTALS	
		MATCH	ERROR	NON_MATCH	ERROR	NON_MATCH
S1	1					
S1	2					
S1	n					
S2	1					

...	...					
Sn						
TOTALS						

— Test result after applying the evaluation criteria.

8 Phase 3 – Bona-fide robustness

8.1 Introduction

The main objective of this phase is to verify that the functionality claimed by the TOE manufacturer is robust facing different contextual changes and thus maintained for the application profile defined, within the SETTINGS defined.

This phase is essential to be able to determine, if the product is able to stay functional under different contexts and still suitable for the application profile defined. Otherwise, the TL shall decide to discontinue the rest of the phases of the evaluation.

All tests made during Phase 3 are using bona-fide SUBJECTS.

The following subclauses define each of the possible tests that each application profile may claim to be applied.

8.2 SUBJECT variation tests

8.2.1 Test T3-1-1: Variations of lighting conditions

8.2.1.1 Description

The purpose of this test is to verify if the TOE is robust against the variations of lighting conditions. This test should represent the possible lighting environment linked to the TOE usage (e.g., low lighting of a house, standard lighting of a house, lo lighting of an office, standard lighting of an office, outside in the morning, etc.). Also lighting orientation is of importance for most application profiles.

8.2.1.2 SETTINGS

In addition to the general indications about SETTINGS (see 6.4), SETTINGS in this test shall have specific illuminance value in lux, as well as relevant orientations.

EDITOR'S NOTE: As per LATE comment in March, is has been suggested to add specification on the colour temperature for light sources or if necessary RGB-values, for coloured light. Call for contributions on the topic.

8.2.1.3 Materials

For each of the TRIALS to be executed in this test, the following material is used:

- The TOE including a capture device (in case the capture device is not included in the TOE). If the capture device is not embedded in the TOE, the capture device to be used shall be one at the visible range, and with the lowest values in terms of resolution and auto-focus (from those allowed by the TOE specifications).
- A lux meter for measuring illuminance
- Any required mean to guarantee that the required orientation for the lighting is achieved.
- A repository (in whatever form allowed by the application profile and/or TOE) of the reference data for each of the test crew members.

8.2.1.4 TRIALS

During this test, a set of TRIALS for each SUBJECT and SETTING will be executed. The minimum number of TRIALS is given by MIN_TRIALS, specified in the applicable application profile.

The steps to follow for each TRIAL are:

1. The TL will setup up the SETTING (by adjusting the light if necessary) and will prepare the SUBJECT, telling him/her how to act and where to be placed
2. The SUBJECT will prepare himself/herself to interact with the TOE, and, if needed, will prepare the access to the reference data. This will be done following the operational guide of the TOE.
3. The SUBJECT will perform an ATTEMPT to identify/verify, following the indication of the operational guide of the TOE. The interaction with the TOE while performing an ATTEMPT may include actions that will be used for proof of life.
4. The SUBJECT will wait for the TOE outcome, and the TL will note the result obtained, increasing the number of MATCHES, NON_MATCHES or SUBJECT_ERRORS as applicable.
5. The SUBJECT will get himself/herself totally or partially out of the point of interaction with the TOE (e.g., will stop staring at the capture device, moving himself/herself significantly). This shall be done to ensure that the next TRIAL es a completely new interaction with the TOE.
6. If the TRIAL for such SUBJECT results in an ERROR, the variables SUBJECT_ERRORS and TEST_ERRORS will be incremented, and the following checking is performed by the TL, in the order given:
 - a. If TEST_ERRORS gets higher than MAX_TEST_ERRORS, all TRIALS for this TEST will be finished, and the TEST will result in a FAIL.
 - b. If SUBJECT_ERRORS gets higher than MAX_SUBJECT_ERRORS, the TL will jump to step number 9.
7. If in that TRIAL for that SUBJECT the number of NON_MATCHES is higher than MAX_SUBJECT_NON_MATCHES, the TL will jump to step 9.
8. The TL returns to step 3, to repeat the process until MIN_TRIALS is reached for that SUBJECT.
9. The SUBJECT is changed, and the TL returns to step 1, until all SUBJECTS have been used for that SETTING.

8.2.1.5 ATTEMPTS

For each TRIAL, a maximum number of ATTEMPTS is given by MAX_ATTEMPTS. ATTEMPTS will be repeated for each TRIAL, until that number is reached, or a result of MATCH or NON_MATCH is returned.

If the number of ATTEMPTS becomes higher than MAX_ATTEMPTS for a TRIAL, then the TRIAL result is declared as an ERROR.

8.2.1.6 Data to be included in the ETR

In addition to all required information, the ETR shall include the following information for this test:

- Number and description (with photographs/videos) of the SETTINGS used.
- Number and type of reference data used. If reference data is obtained through a previously obtained document, images of such documents shall be attached in an anonymized way (except for the photograph included).
- Number and classification (e.g., age, gender, etc.) of the bona-fide users. The similarity values among the USERS, given by the REF_APP, shall be reported.
- Total number of SUBJECTS used in the test.
- Total number of TRIALS executed.
- A table with the information about SUBJECT_ERRORS, MATCHES and NON_MATCHES for each SUBJECT, TRIAL and SETTING. An example of such a table could be the one described for the test T2-2.
- Test result after applying the evaluation criteria.

8.2.2 Test T3-1-2: Variations of background

8.2.2.1 Description

Certain facial biometric products may impose a fixed background (i.e., some ABC systems). But many others may not have any restriction, as the product is expected to be used at the own convenience of the user. This means that the background of the facial images taken may differ significantly (e.g., in videoconferencing-related products).

This test intends to verify if the TOE is robust against the variation of background during the image acquisition.

8.2.2.2 SETTINGS

The TL shall have to adapt the background and the environment of the TOE to the target application. As a general rule, the following three scenario SETTINGS are defined:

- SETTING 1 – Fixed background. This will be the case of, for example, a photo booth, where the background is a plain colour (typically white), and no alteration to that background is expected during the test.
- SETTING 2 – Dynamic background without other faces. In this SETTING, the background may be a video sequence with a moving scenery with the equipment discussed in 6.4. Examples of those sceneries could be a panoramic view of an office (without workers in it), or a nature landscape. The video shall not be a still image, and objects shall be moving within the whole duration of the video. The video could be of an

indoors scenery or an outdoors one, whatever is more probable to be found during the regular use of the TOE. The video shall be as long as the longest TRIAL to be executed.

- SETTING 3 – Dynamic background with other faces included. In this SETTING, the background is also a video, as in SETTING 2. But in this case, the video shall include other people appearing in the background, looking at different directions, but temporarily facing the camera. Some of those people appearing in the video shall be those members of the bona-fide users test crew. The rest of the requirements are the same as in SETTING 2.

The application profile shall define which SETTINGS are included in this test.

8.2.2.3 Materials

For each of the TRIALS to be executed in this test, the following material is used:

- The TOE including a capture device (in case the capture device is not included in the TOE). If the capture device is not embedded in the TOE, the capture device to be used shall be one at the visible range, and with the lowest values in terms of resolution and auto-focus (from those allowed by the TOE specifications).
- A repository (in whatever form allowed by the application profile and/or TOE) of the reference data for each of the test crew members.
- The relevant equipment to be able to implement each of the defined SETTINGS. Some guidance can be found in clause 6.4.

8.2.2.4 TRIALS

During this test, a set of TRIALS for each SUBJECT and SETTING will be executed. The minimum number of TRIALS is given by MIN_TRIALS, specified in the applicable application profile.

The steps to follow for each TRIAL are:

1. The TL will setup up the SETTING (by adjusting the light if necessary) and will prepare the SUBJECT, telling him/her how to act and where to be placed
2. The SUBJECT will prepare himself/herself to interact with the TOE, and, if needed, will prepare the access to the reference data. This will be done following the operational guide of the TOE.
3. The SUBJECT will perform an ATTEMPT to identify/verify, following the indication of the operational guide of the TOE. The interaction with the TOE while performing an ATTEMPT may include actions that will be used for proof of life.
4. The SUBJECT will wait for the TOE outcome, and the TL will note the result obtained, increasing the number of MATCHES, NON_MATCHES or SUBJECT_ERRORS as applicable.
5. The SUBJECT will get himself/herself totally or partially out of the point of interaction with the TOE (e.g., will stop staring at the capture device, moving himself/herself significantly). This shall be done to ensure that the next TRIAL es a completely new interaction with the TOE.
6. If the TRIAL for such SUBJECT results in an ERROR, the variables SUBJECT_ERRORS and TEST_ERRORS will be incremented, and the following checking is performed by the TL, in the order given:
 - a. If TEST_ERRORS gets higher than MAX_TEST_ERRORS, all TRIALS for this TEST will be finished, and the TEST will result in a FAIL.

- b. If SUBJECT_ERRORS gets higher than MAX_SUBJECT_ERRORS, the TL will jump to step number 9.
7. If in that TRIAL for that SUBJECT the number of NON_MATCHES is higher than MAX_SUBJECT_NON_MATCHES, the TL will jump to step 9.
8. The TL returns to step 3, to repeat the process until MIN_TRIALS is reached for that SUBJECT.
9. The SUBJECT is changed, and the TL returns to step 1, until all SUBJECTS have been used for that SETTING.

8.2.2.5 ATTEMPTS

For each TRIAL, a maximum number of ATTEMPTS is given by MAX_ATTEMPTS. ATTEMPTS will be repeated for each TRIAL, until that number is reached, or a result of MATCH or NON_MATCH is returned.

If the number of ATTEMPTS becomes higher than MAX_ATTEMPTS for a TRIAL, then the TRIAL result is declared as an ERROR.

8.2.2.6 Data to be included in the ETR

In addition to all required information, the ETR shall include the following information for this test:

- Number and description (with photographs/videos) of the SETTINGS used.
- Number and type of reference data used. If reference data is obtained through a previously obtained document, images of such documents shall be attached in an anonymized way (except for the photograph included).
- Number and classification (e.g., age, gender, etc.) of the bona-fide users. The similarity values among the USERS, given by the REF_APP, shall be reported.
- Total number of SUBJECTS used in the test.
- Total number of TRIALS executed.
- A table with the information about SUBJECT_ERRORS, MATCHES and NON_MATCHES for each SUBJECT, TRIAL and SETTING. An example of such a table could be the one described for the test T2-2.
- Test result after applying the evaluation criteria.

8.3 Scenario variation tests

8.3.1 Test T3-2-1: Variations in facial expressions

8.3.1.1 Description

The purpose of this test is to verify if the TOE is robust against the variations in facial expressions. This test should represent the most common emotions. The application profile shall define the facial expressions that are relevant. If nothing is specified in the application profile, the following expressions shall be considered:

- Strong smile
- Laughing
- Extreme sadness, close to crying

- Extreme anger
- Sleepiness

EDITOR'S NOTE: It may be interesting to add a description (may be as a NOTE or EXAMPLE) of each of the expressions. Some figures may be of help, in comparison with neutral expression.

8.3.1.2 Materials

For each of the TRIALS to be executed in this test, the following material is used:

- The TOE including a capture device (in case the capture device is not included in the TOE). If the capture device is not embedded in the TOE, the capture device to be used shall be one at the visible range, and with the lowest values in terms of resolution and auto-focus (from those allowed by the TOE specifications).
- A repository (in whatever form allowed by the application profile and/or TOE) of the reference data for each of the test crew members.

8.3.1.3 TRIALS

During this test, a set of TRIALS for each SUBJECT and SETTING will be executed. The minimum number of TRIALS is given by MIN_TRIALS, specified in the applicable application profile.

The steps to follow for each TRIAL are:

1. The TL will prepare the SUBJECT according to the specific SETTING, telling him/her how to act and where to be placed
2. The SUBJECT will prepare himself/herself to interact with the TOE, and, if needed, will prepare the access to the reference data. This will be done following the operational guide of the TOE.
3. The SUBJECT will perform an ATTEMPT to identify/verify, following the indication of the operational guide of the TOE. The interaction with the TOE while performing an ATTEMPT may include actions that will be used for proof of life.
4. The SUBJECT will wait for the TOE outcome, and the TL will note the result obtained, increasing the number of MATCHES, NON_MATCHES or SUBJECT_ERRORS as applicable.
5. The SUBJECT will get himself/herself totally or partially out of the point of interaction with the TOE (e.g., will stop staring at the capture device, moving himself/herself significantly). This shall be done to ensure that the next TRIAL is a completely new interaction with the TOE.
6. If the TRIAL for such SUBJECT results in an ERROR, the variables SUBJECT_ERRORS and TEST_ERRORS will be incremented, and the following checking is performed by the TL, in the order given:
 - a. If TEST_ERRORS gets higher than MAX_TEST_ERRORS, all TRIALS for this TEST will be finished, and the TEST will result in a FAIL.
 - b. If SUBJECT_ERRORS gets higher than MAX_SUBJECT_ERRORS, the TL will jump to step number 9.
7. If in that TRIAL for that SUBJECT the number of NON_MATCHES is higher than MAX_SUBJECT_NON_MATCHES, the TL will jump to step 9.
8. The TL returns to step 3, to repeat the process until MIN_TRIALS is reached for that SUBJECT.

9. The SUBJECT is changed, and the TL returns to step 1, until all SUBJECTS have been used for that SETTING.

8.3.1.4 ATTEMPTS

For each TRIAL, a maximum number of ATTEMPTS is given by MAX_ATTEMPTS. ATTEMPTS will be repeated for each TRIAL, until that number is reached, or a result of MATCH or NON_MATCH is returned.

If the number of ATTEMPTS becomes higher than MAX_ATTEMPTS for a TRIAL, then the TRIAL result is declared as an ERROR.

8.3.1.5 Data to be included in the ETR

In addition to all required information, the ETR shall include the following information for this test:

- Number and description (with photographs/videos) of the SETTINGS used.
- Number and type of reference data used. If reference data is obtained through a previously obtained document, images of such documents shall be attached in an anonymized way (except for the photograph included).
- Number and classification (e.g., age, gender, etc.) of the bona-fide users. The similarity values among the USERS, given by the REF_APP, shall be reported.
- Total number of SUBJECTS used in the test.
- Total number of TRIALS executed.
- A table with the information about SUBJECT_ERRORS, MATCHES and NON_MATCHES for each SUBJECT, TRIAL and SETTING. An example of such a table could be the one described for the test T2-2.
- Test result after applying the evaluation criteria.

8.3.2 Test T3-2-2: Variation in face orientation towards the TOE

8.3.2.1 Description

The purpose of this test is to verify if the TOE is robust against the variations in face orientations towards the TOE. This test will give an overview of the range of angle values which is accepted by the TOE. The application profile shall define the face orientations that are relevant.

EDITOR'S NOTE 1: Some figures may be of help, in comparison with the frontal orientation.

EDITOR'S NOTE 2: Some examples may be of help. Call for contributions on these examples.

EDITOR'S NOTE 3: The definition of the base-line orientation shall be given (e.g., frontal orientation)

8.3.2.2 Materials

For each of the TRIALS to be executed in this test, the following material is used:

- The TOE including a capture device (in case the capture device is not included in the TOE). If the capture device is not embedded in the TOE, the capture device to be used shall be one at the visible range, and with the lowest values in terms of resolution and auto-focus (from those allowed by the TOE specifications).

- Any mean to help the SUBJECT to reach the desired orientation (e.g., may be a mark in the background to know where to face).
- A repository (in whatever form allowed by the application profile and/or TOE) of the reference data for each of the test crew members.

8.3.2.3 TRIALS

During this test, a set of TRIALS for each SUBJECT and SETTING will be executed. The minimum number of TRIALS is given by MIN_TRIALS, specified in the applicable application profile.

The steps to follow for each TRIAL are:

1. The TL will prepare the SUBJECT according to the specific SETTING, telling him/her how to act and where to be placed
2. The SUBJECT will prepare himself/herself to interact with the TOE, and, if needed, will prepare the access to the reference data. This will be done following the operational guide of the TOE.
3. The SUBJECT will perform an ATTEMPT to identify/verify, following the indication of the operational guide of the TOE. The interaction with the TOE while performing an ATTEMPT may include actions that will be used for proof of life.
4. The SUBJECT will wait for the TOE outcome, and the TL will note the result obtained, increasing the number of MATCHES, NON_MATCHES or SUBJECT_ERRORS as applicable.
5. The SUBJECT will get himself/herself totally or partially out of the point of interaction with the TOE (e.g., will stop staring at the capture device, moving himself/herself significantly). This shall be done to ensure that the next TRIAL es a completely new interaction with the TOE.
6. If the TRIAL for such SUBJECT results in an ERROR, the variables SUBJECT_ERRORS and TEST_ERRORS will be incremented, and the following checking is performed by the TL, in the order given:
 - a. If TEST_ERRORS gets higher than MAX_TEST_ERRORS, all TRIALS for this TEST will be finished, and the TEST will result in a FAIL.
 - b. If SUBJECT_ERRORS gets higher than MAX_SUBJECT_ERRORS, the TL will jump to step number 9.
7. If in that TRIAL for that SUBJECT the number of NON_MATCHES is higher than MAX_SUBJECT_NON_MATCHES, the TL will jump to step 9.
8. The TL returns to step 3, to repeat the process until MIN_TRIALS is reached for that SUBJECT.
9. The SUBJECT is changed, and the TL returns to step 1, until all SUBJECTS have been used for that SETTING.

8.3.2.4 ATTEMPTS

For each TRIAL, a maximum number of ATTEMPTS is given by MAX_ATTEMPTS. ATTEMPTS will be repeated for each TRIAL, until that number is reached, or a result of MATCH or NON_MATCH is returned.

If the number of ATTEMPTS becomes higher than MAX_ATTEMPTS for a TRIAL, then the TRIAL result is declared as an ERROR.

8.3.2.5 Data to be included in the ETR

In addition to all required information, the ETR shall include the following information for this test:

- Number and description (with photographs/videos) of the SETTINGS used.
- Number and type of reference data used. If reference data is obtained through a previously obtained document, images of such documents shall be attached in an anonymized way (except for the photograph included).
- Number and classification (e.g., age, gender, etc.) of the bona-fide users. The similarity values among the USERS, given by the REF_APP, shall be reported.
- Total number of SUBJECTS used in the test.
- Total number of TRIALS executed.
- A table with the information about SUBJECT_ERRORS, MATCHES and NON_MATCHES for each SUBJECT, TRIAL and SETTING. An example of such a table could be the one described for the test T2-2.
- Test result after applying the evaluation criteria.

8.3.3 Test T3-2-3: Significant SUBJECT esthetical variations

8.3.3.1 Description

The purpose of this test is to detect if the TOE is able to identify a bona-fide SUBJECT even with some traditional esthetical changes (e.g., with or without beard, with or without make up, with or without piercings, with different hair styles, etc.), all of them with the test SUBJECT acting as a bona-fide one. The application profile shall define the esthetical changes that are relevant.

EXAMPLE the following cases can be considered:

- With and without glasses (no sunglasses)
- With and without moustache
- With and without beard
- With and without "office-like" make-up
- With and without "party-time" make-up (but not as radical as for a costume-party)
- With and without piercings (EDITOR'S NOTE: it has to be defined which kind of piercings)
- With long and short hair

In each of those cases, one of the options shall be used for the biometric reference, while the other shall be used for the verification.

EDITOR'S NOTE: Some figures may be of help.

8.3.3.2 Materials

For each of the TRIALS to be executed in this test, the following material is used:

- The TOE including a capture device (in case the capture device is not included in the TOE). If the capture device is not embedded in the TOE, the capture device to be used shall be one at the visible range, and with the lowest values in terms of resolution and auto-focus (from those allowed by the TOE specifications).
- Specific equipment depending on the SETTINGS if needed (e.g., wigs, fake beards, glasses, etc.).

- A repository (in whatever form allowed by the application profile and/or TOE) of the reference data for each of the test crew members.

8.3.3.3 TRIALS

During this test, a set of TRIALS for each SUBJECT and SETTING will be executed. The minimum number of TRIALS is given by MIN_TRIALS, specified in the applicable application profile.

The steps to follow for each TRIAL are:

1. The TL will setup up the SETTING (by adjusting the light if necessary) and will prepare the SUBJECT, telling him/her how to act and where to be placed
2. The SUBJECT will prepare himself/herself to interact with the TOE, and, if needed, will prepare the access to the reference data. This will be done following the operational guide of the TOE.
3. The SUBJECT will perform an ATTEMPT to identify/verify, following the indication of the operational guide of the TOE. The interaction with the TOE while performing an ATTEMPT may include actions that will be used for proof of life.
4. The SUBJECT will wait for the TOE outcome, and the TL will note the result obtained, increasing the number of MATCHES, NON_MATCHES or SUBJECT_ERRORS as applicable.
5. The SUBJECT will get himself/herself totally or partially out of the point of interaction with the TOE (e.g., will stop staring at the capture device, moving himself/herself significantly). This shall be done to ensure that the next TRIAL es a completely new interaction with the TOE.
6. If the TRIAL for such SUBJECT results in an ERROR, the variables SUBJECT_ERRORS and TEST_ERRORS will be incremented, and the following checking is performed by the TL, in the order given:
 - a. If TEST_ERRORS gets higher than MAX_TEST_ERRORS, all TRIALS for this TEST will be finished, and the TEST will result in a FAIL.
 - b. If SUBJECT_ERRORS gets higher than MAX_SUBJECT_ERRORS, the TL will jump to step number 9.
7. If in that TRIAL for that SUBJECT the number of NON_MATCHES is higher than MAX_SUBJECT_NON_MATCHES, the TL will jump to step 9.
8. The TL returns to step 3, to repeat the process until MIN_TRIALS is reached for that SUBJECT.
9. The SUBJECT is changed, and the TL returns to step 1, until all SUBJECTS have been used for that SETTING.

8.3.3.4 ATTEMPTS

For each TRIAL, a maximum number of ATTEMPTS is given by MAX_ATTEMPTS. ATTEMPTS will be repeated for each TRIAL, until that number is reached, or a result of MATCH or NON_MATCH is returned.

If the number of ATTEMPTS becomes higher than MAX_ATTEMPTS for a TRIAL, then the TRIAL result is declared as an ERROR.

8.3.3.5 Data to be included in the ETR

In addition to all required information, the ETR shall include the following information for this test:

- Number and description (with photographs/videos) of the SETTINGS used.
- Number and type of reference data used. If reference data is obtained through a previously obtained document, images of such documents shall be attached in an anonymized way (except for the photograph included).
- Number and classification (e.g., age, gender, etc.) of the bona-fide users. The similarity values among the USERS, given by the REF_APP, shall be reported.
- Total number of SUBJECTS used in the test.
- Total number of TRIALS executed.
- A table with the information about SUBJECT_ERRORS, MATCHES and NON_MATCHES for each SUBJECT, TRIAL and SETTING. An example of such a table could be the one described for the test T2-2.
- Test result after applying the evaluation criteria.

9 Phase 4 –Attack Detection

9.1 Introduction

The main goal of the Phase 4 tests is to check if the TOE is susceptible to be attacked during the process of presenting the biometric trait. The attacks executed in this Phase may be oriented to obfuscation or to impersonation.

EDITOR'S NOTE: This initial proposal is focussed on impersonation attacks, subject to be enhanced/improved/etc.

Tests are divided in groups, attending to the kind of artefact used.

ATTACKERS shall have the attack ready before starting the recognition process, and if needed, to be able to access the bona-fide user biometric reference (e.g., in case the reference is in a document, to be able to use that document).

In order to calculate the total number of biometric comparisons, the number of bona-fide users involved in the text, multiplied by the number of artefacts used, shall be considered.

For each of the described tests, the application profile shall indicate the maximum number of TRIALS per test.

Within a test, the maximum number of TRIALS per TEST and SUBJECT shall be defined by the application profile. But for the first time that an attack has led to a PASS, evaluation may result in a FAIL, according to the rules defined in the appropriate application profile at the appropriate LoA. If that is the case, the rest of the TRIALS shall not be executed.

For those products that allow several ATTEMPTS per recognition process, in case that SUBJECT_ERRORS are found, further attempts shall be included in the TRIAL, until the limit given by MAX_ATTEMPTS is reached.

As defined in Part 3, a PASS in any of the tests included in Phase 4, will indicate that the TOE is not robust against presentation attacks.

9.2 Common parameters for Phase 4 tests

9.2.1 Introduction

The descriptions of the tests for Phase 4 have many common parts. This subclause is describing those common parameters, so that each test will focus on its specifics. Therefore, all what is described here is mandatory to all Phase 4 tests, unless anything specific described in each test.

9.2.2 Materials

For each of the TRIALS to be executed in Phase 4 tests, the following material is used, in addition to any other material described in the relevant test:

- The TOE including a capture device (in case the capture device is not included in the TOE). If the capture device is not embedded in the TOE, the capture device to be used shall be one at the visible range, and with the lowest values in terms of resolution (from those allowed by the TOE specifications). It is important to note that if the TOE allows the use of visible-range cameras, a near-infrared (NIR) camera does not have to be used during the TRIALS, as such kind of cameras could intrinsically remove some of the artefacts used for the attacks. In other words, depending on the TOE biometric acquisition and PAD technology, only PAIs visible to the specific technology can be used.
- A repository (in whatever form allowed by the application profile and/or TOE) of the reference data for each of the test crew members.

9.2.3 ATTEMPTS

For each TRIAL, a maximum number of ATTEMPTS is given by MAX_ATTEMPTS. ATTEMPTS will be repeated for each TRIAL, until that number is reached, or a result of MATCH or NON_MATCH is returned by the TOE.

If the number of ATTEMPTS becomes higher than MAX_ATTEMPTS for a TRIAL, then the TRIAL result is declared as an ERROR.

9.2.4 Data to be included in the ETR

In addition to all required information, the ETR shall include the following information for this test:

- Number and description (with photographs/videos) of the SETTINGS used.
- Number and type of reference data used. If reference data is obtained through a previously obtained document, images of such documents shall be attached in an anonymized way (except for the photograph included).
- Number and classification (e.g., age, gender, etc.) of the bona-fide users. The similarity values among the USERS, given by the REF_APP, shall be reported.
- Total number of SUBJECTS used in the test.
- Total number of TRIALS executed.
- TIMEOUT used, and whether this TIMEOUT has been specified by the TOE documentation, or by the application profile.
- In case artefacts are used for the attacks, the following information shall be provided:

- Description about how the artifact has been developed and prepared
- Effort required to obtain the artefact. Effort will be given in terms of technical knowledge, manufacturing time, cost, preparation of instruments needed, etc.
- Description of the source of the biometric traits. For example, if the artifact has been obtained using direct presentations of the biometric trait (e.g., through a collaborative approach), or using indirect presentations (e.g., a latent trait), or using modified representations, or synthetic biometric traits.
- Time needed for the training and habituation. In other words, it has to be reported the time needed for the TRIAL when using and presenting the artifact, as well as the time needed for the ATTACKER to habituate himself/herself to the use of the artifact.
- Duration of the artifact. Some kind of artifacts (e.g., depending on the material used) might have a limited time of application, as time may impact in its efficiency in the attack. Depending on the application profile, the analysis of the viability of the attack may be impacted by the time the artifact can be used, or the number of presentations used.
- Description on how the artifact has been used. This shall be provided in a way that it is clear for how long the artifact has been used, and the number of previous presentations in which it has been used.
- Evidence of the artifact used (image, video, etc.)
- For each of the artifacts used, the calculation of the attack potential shall be provided.
- If the test requires to check the level of similarity between the bona-fide user and the ATTACKER and/or artifact, the similarities values using REF_APP shall be reported. The similarity will have to be measured with the ATTACKER just before the interaction with the TOE is executed. This is to measure the goodness of the attack.
- A table with the information about SUBJECT_ERRORS, MATCHES and NON_MATCHES for each SUBJECT, TRIAL and SETTING. An example of such a table could be the following:

Table 6 — Example of results summary for Phase 4 tests

SUBJECT	TRIAL	SETTING 3			TOTALS	
		MATCH	ERROR	NON_MATCH	ERROR	NON_MATCH
S1	1					
S1	2					
S1	n					
S2	1					
...	...					
Sn						
TOTALS						

- Test result after applying the evaluation criteria.

9.3 Zero-Effort attacks

9.3.1 Test T4-1: Zero-effort imposter attack

POSTPONED COMMENT TO BE RESOLVED IN THE NEXT CYCLE:

Comment: This section deals with FMR evaluation, it is strange to have it here and not included in Phase 2 tests.

Proposed change: Suggest to include FALSE_MATCH before

Disposition:

This test is intended to be scenario-based, not technology evaluation (i.e., no databases are to be used).

From the conceptual point of view, this is an attack test. The test subjects will interact with the intention of being accepted by the TOE, meaning a PASS in the test, and therefore, a FAIL of the TOE.

A request has been made to tell the TL to analyse if the PASS has happened because of a threshold problem, or any other kind of problem.

9.3.1.1 Description

The main goal of this test is to check if the TOE is vulnerable to the impersonation of a bona-fide user, by an ATTACKER that looks similar to that bona-fide user, without applying any kind of artifact. Therefore, the ATTACKER shall be one that will reach a comparison value with one bona-fide user, lower than BONAFIDE_SIM_TH using the REF_APP.

It is important to note that the concept of similarity in this test refers to the facial biometric recognition between the ATTACKER and the bona-fide user. Parameters such as height, weight, age, etc, are of no interest for this test.

For the execution of the TRIALS within this test, it is not needed to have the bona-fide user present. Only access to his/her reference data.

Throughout this test, the ATTACKER will behave following the TOE's operation guide, including the proof-of-life mechanism implemented (if applicable). The only deviation to the operation guide, is the use of the reference data from the bona-fide user, instead of the one from the ATTACKER.

In general terms, this test is executed in the same way as T2-2, but in here, the desirable result is a NON_MATCH, instead of a MATCH.

9.3.1.2 Materials

For all TRIALS to be executed in this test, the material to be used will be the specified in 9.2.2. In addition, REF_APP will also be used.

9.3.1.3 TRIALS

During this test, a set of TRIALS for each SUBJECT and SETTING will be executed. The minimum number of TRIALS is given by MIN_TRIALS, specified in the applicable application profile.

The steps to follow for each TRIAL are:

1. The TL will setup up the SETTING and will prepare the SUBJECT (in this test, the SUBJECT is the ATTACKER), telling him/her how to act and where to be placed. The TL will have to make it clear for the ATTACKER, that the interaction shall be as indicated in the TOE operational guide, being as cooperative as possible, and performing the proof-of-life mechanisms (if available).
2. The ATTACKER will prepare himself/herself to interact with the TOE, and, if needed, will prepare the access to the bona-fide user reference data. This will be done following the operational guide of the TOE.
3. The SUBJECT will perform an ATTEMPT to identify/verify, following the indication of the operational guide of the TOE.
4. If the TOE results in a result different from MATCH or NON_MATCH, a new ATTEMPT will be executed. This will be repeated until the limit given by MAX_ATTEMPTS is reached. In such case, the TOE results in an ERROR.
5. The TL will note the result obtained, increasing the number of MATCHES, NON_MATCHES or SUBJECT_ERRORS as applicable.
6. The SUBJECT will get himself/herself totally or partially out of the point of interaction with the TOE (e.g., will stop staring at the capture device, moving himself/herself significantly). This shall be done to ensure that the next TRIAL es a completely new interaction with the TOE.
7. If the TRIAL result is a MATCH, and the number of MATCHES gets higher than MAX_SUBJECT_MATCHES, the TL will jump to step 9, increasing the variable SUBJECTS_PASS. If SUBJECTS_PASS gets higher than MAX_SUBJECTS_PASS, all TRIALS for this test will be finished, resulting in a PASS for the TEST.
8. The TL returns to step 2, to repeat the process until MIN_TRIALS is reached for that SUBJECT.
9. The SUBJECT is changed, and the TL returns to step 1, until all SUBJECTS have been used for that SETTING.

9.3.1.4 Minimum attack level analysis

According to the definitions in part 1, the attack level weights are:

Table 7 —T4-1 attack level analysis

CRITERIA	IDENTIFICATION INTERVAL	IDENTIFICATION WEIGHT	EXPLOITATION INTERVAL	EXPLOITATION WEIGHT
Time effort	< one hour	0	< one day	3
Expertise	Layman	0	Layman	0
Knowledge of product	Public information	0	Public information	0
Equipment	Standard	0	Standard	0
Access to TOE	Easy	0	Easy	0
Access to biometric characteristic	Easy	0	Easy	0
Degree of scrutiny	None	0	None	0
TOTAL WEIGHT		0		3
ASSURANCE LEVEL		0+3 = 3	No rating	N/A

9.4 Enrolment-based attacks

9.4.1 Test T4-2-1: Basic attack to the biometric reference storage

This test is out of the scope of this document. The test shall be considered within the scope of the media that stores the biometric reference.

EXAMPLE If the storage media is a smart card, refer to CEN 419211 family of standards that evaluates the security of secure signature creation devices (SSCD).

9.4.2 Test T4-2-2: Use of morphing techniques during enrolment

EDITOR'S NOTE: There is currently a project on this topic at ISO/IEC JTC1/SC37: ISO/IEC CD 20059 "Vulnerability of Biometric Recognition Systems with Respect to Morphing Attacks". We should make some kind of reference to this standard, and to check if the content is applicable here, or if we should contribute to that project.

Regarding CD 20059: Is it required that a PAD mechanism is implemented to mitigate the attack vector of presenting morphs on prints, display ... **CALL FOR CONTRIBUTIONS ON THIS TEST.**

9.4.2.1 Description

The main goal of this test is to check if the TOE is vulnerable to the impersonation of a bona-fide user, by an ATTACKER that uses morphed images from that bona-fide user face and the attacker's face as reference image. The ATTACKER presents the morphed image as reference image while interacting with the TOE during enrolment.

During this test, the TL will be able to check if the ATTACKER is able to get a MATCH with a morphed image as reference image. Moreover, the TL will also check if the TOE is able to detect morphed image during enrolment.

9.4.2.2 Materials

For each of the TRIALS to be executed in this test, the following material is used:

- The TOE including a capture device (in case the capture device is not included in the TOE). If the capture device is not embedded in the TOE, the capture device to be used shall be one at the visible range, and with the lowest values in terms of resolution and auto-focus (from those allowed by the TOE specifications).
- **The TL shall at least use three different morphing technique (i.e., shall use at least three different tools from independent sources to make the morphed image).**
- A repository (in whatever form allowed by the application profile and/or TOE) of the reference data for each of the test crew members.

9.4.2.3 TRIALS

During this test, a set of TRIALS for each SUBJECT and SETTING will be executed. The minimum number of TRIALS is given by MIN_TRIALS, specified in the applicable application profile.

The steps to follow for each TRIAL are:

1. The TL will setup up the SETTING and will prepare the SUBJECT (in this test, the SUBJECT is the ATTACKER), telling him/her how to act and where to be placed. The TL will have to make it clear for the ATTACKER, that the interaction shall be as indicated in the TOE operational guide, being as cooperative as possible, and performing the proof-of-life mechanisms (if available).
2. The ATTACKER will prepare himself/herself to interact with the TOE, and, if needed, will prepare the access to the bona-fide user reference data. This will be done following the operational guide of the TOE.
3. The SUBJECT will perform an ATTEMPT to identify/verify, following the indication of the operational guide of the TOE.
4. If the TOE results in a result different from MATCH or NON_MATCH, a new ATTEMPT will be executed. This will be repeated until the limit given by MAX_ATTEMPTS is reached. In such case, the TOE results in an ERROR.
5. The TL will note the result obtained, increasing the number of MATCHES, NON_MATCHES or SUBJECT_ERRORS as applicable.
6. The SUBJECT will get himself/herself totally or partially out of the point of interaction with the TOE (e.g., will stop staring at the capture device, moving himself/herself significantly). This shall be done to ensure that the next TRIAL es a completely new interaction with the TOE.
7. If the TRIAL result is a MATCH, and the number of MATCHES gets higher than MAX_SUBJECT_MATCHES, the TL will jump to step 9, increasing the variable SUBJECTS_PASS. If SUBJECTS_PASS gets higher than MAX_SUBJECTS_PASS, all TRIALS for this test will be finished, resulting in a PASS for the TEST.
8. The TL returns to step 2, to repeat the process until MIN_TRIALS is reached for that SUBJECT.
9. The SUBJECT is changed, and the TL returns to step 1, until all SUBJECTS have been used for that SETTING.

9.4.2.4 ATTEMPTS

For each TRIAL, a maximum number of ATTEMPTS is given by MAX_ATTEMPTS. ATTEMPTS will be repeated for each TRIAL, until that number is reached, or a result of MATCH or NON_MATCH is returned.

If the number of ATTEMPTS becomes higher than MAX_ATTEMPTS for a TRIAL, then the TRIAL result is declared as an ERROR.

9.4.2.5 Minimum attack level analysis

Several scenarios can be considered for this test. In the case of an “auto-enrolment” (i.e., the user is enrolling without any control of an officer), the attack level is given in the following table:

Table 8 —T4-2-2 attack level analysis (auto-enrolment)

CRITERIA	IDENTIFICATION INTERVAL	IDENTIFICATION WEIGHT	EXPLOITATION INTERVAL	EXPLOITATION WEIGHT
----------	-------------------------	-----------------------	-----------------------	---------------------

Time effort	< one hour	0	< one hour	0
	< one day	1	< one day	3
	< three days	2	< three days	4
	< 7 days	3	< 7 days	6
	< 25 days	6	< 25 days	8
	> 25 days	10	> 25 days	10
	Not practical	*	Not practical	*
Expertise	Layman	0	Layman	0
	Skilled	2	Skilled	2
	Expert	5	Expert	4
	Multiple experts	7	Multiple experts	6
Knowledge of product	Public information	0	Public information	0
	Restricted information	2	Restricted information	2
	Sensitive information	4	Sensitive information	3
	Critical information	6	Critical information	5
Equipment	Standard	0	Standard	0
	Specialized	2	Specialized	4
	Bespoke	4	Bespoke	6
	Multiple Bespoke	6	Multiple Bespoke	10
	Not Practical	*	Not Practical	*
Access to TOE	Easy	0	Easy	0
	Moderate	2	Moderate	2
	Difficult	4	Difficult	4
Access to biometric characteristic	Not needed	0	Not needed	0
	Easy	0	Easy	0
	Moderate	4	Moderate	4
	Difficult	8	Difficult	8
Degree of scrutiny	None	0	None	0
	Overseen	2	Overseen	3
	Not Practical	*	Not Practical	*
LEVEL / TOTAL WEIGHT		10		4
ASSURANCE LEVEL	0-10 No rating – 11-20 Basic - 1 21-30 Enhanced Basic - 2 31-40 Moderate - 3 >40 High - 4 or 5	10+4 = 14	Basic	AVA_VAN.1

In the case that the enrolment is supervised by an officer, but it is done using a photograph brought by the user, the attack level is given in the following table:

Table 9 — T4-2-2 attack level analysis (photograph)

CRITERIA	IDENTIFICATION INTERVAL	IDENTIFICATION WEIGHT	EXPLOITATION INTERVAL	EXPLOITATION WEIGHT
Time effort	< one hour	0	< one hour	0
	< one day	1	< one day	3
	< three days	2	< three days	4
	< 7 days	3	< 7 days	6
	< 25 days	6	< 25 days	8
	> 25 days	10	> 25 days	10
	Not practical	*	Not practical	*
Expertise	Layman	0	Layman	0
	Skilled	2	Skilled	2
	Expert	5	Expert	4
	Multiple experts	7	Multiple experts	6
Knowledge of product	Public information	0	Public information	0
	Restricted information	2	Restricted information	2

	Sensitive information	4	Sensitive information	3
	Critical information	6	Critical information	5
Equipment	Standard	0	Standard	0
	Specialized	2	Specialized	4
	Bespoke	4	Bespoke	6
	Multiple Bespoke	6	Multiple Bespoke	10
	Not Practical	*	Not Practical	*
Access to TOE	Easy	0	Easy	0
	Moderate	2	Moderate	2
	Difficult	4	Difficult	4
Access to biometric characteristic	Not needed	0	Not needed	0
	Easy	0	Easy	0
	Moderate	4	Moderate	4
Degree of scrutiny	Difficult	8	Difficult	8
	None	0	None	0
	Overseen	2	Overseen	3
	Not Practical	*	Not Practical	*
LEVEL / TOTAL WEIGHT		16		9
ASSURANCE LEVEL	0-10 No rating - 11-20 Basic - 1 21-30 Enhanced Basic - 2 31-40 Moderate - 3 >40 High - 4 or 5	16+9 = 25	Enhanced Basic	AVA_VAN.2

In the case that the enrolment is performed at a supervised office and making a live capture at the office, the attack level is given in the following table:

Table 10 —T4-2-2 attack level analysis (live capture)

CRITERIA	IDENTIFICATION INTERVAL	IDENTIFICATION WEIGHT	EXPLOITATION INTERVAL	EXPLOITATION WEIGHT
Time effort	< one hour	0	< one hour	0
	< one day	1	< one day	3
	< three days	2	< three days	4
	< 7 days	3	< 7 days	6
	< 25 days	6	< 25 days	8
	> 25 days	10	> 25 days	10
	Not practical	*	Not practical	*
Expertise	Layman	0	Layman	0
	Skilled	2	Skilled	2
	Expert	5	Expert	4
	Multiple experts	7	Multiple experts	6
Knowledge of product	Public information	0	Public information	0
	Restricted information	2	Restricted information	2
	Sensitive information	4	Sensitive information	3
Equipment	Critical information	6	Critical information	5
	Standard	0	Standard	0
	Specialized	2	Specialized	4
Access to TOE	Bespoke	4	Bespoke	6
	Multiple Bespoke	6	Multiple Bespoke	10
	Not Practical	*	Not Practical	*
Access to biometric characteristic	Easy	0	Easy	0
	Moderate	2	Moderate	2
	Difficult	4	Difficult	4
Degree of scrutiny	Difficult	8	Difficult	8
	None	0	None	0
	Overseen	2	Overseen	3

	Overseen Not Practical	2 *	Overseen Not Practical	3 *
LEVEL / TOTAL WEIGHT		*		*
ASSURANCE LEVEL	0-10 No rating - 11-20 Basic - 1 21-30 Enhanced Basic - 2 31-40 Moderate - 3 >40 High - 4 or 5	*	Not Practical	Not Practical

9.4.2.6 Data to be included in the ETR

In addition to all what it is specified in 9.2.5, the ETR shall also include the tools used to create the morphed images.

9.5 Attacks during recognition process

9.5.1 Test T4-3-1: Still images as ARTIFACTS

9.5.1.1 Description

The main goal of this test is to check if the TOE is vulnerable to the impersonation of a bona-fide user, by an ATTACKER that uses still images from that bona-fide user. The ATTACKER presents the image while interacting with the TOE for reaching a biometric verification.

Most likely, if the TOE implement any kind of proof-of-life mechanism based on challenge-response, this attack won't be successful, as the presentation of the proof-of-life won't be possible when using only still images (e.g., a printed photograph.).

In general terms, this test is executed in the same way as in T4-1, where the desirable results for the TRIAL is either NON_MATCH or ERROR, while the non-desired result will be a MATCH.

9.5.1.2 Materials

For all TRIALS to be executed in this test, the material to be used will be the specified in 9.2.2.

In addition, the following material is needed:

- The artifacts classified as still images
- The specific material needed to present the artifact to the TOE (e.g., a tablet to display portrait photo of the bona-fide user targeted by the ATTACKER)

9.5.1.3 TRIALS

During this test, a set of TRIALS for each ARTIFACT and SETTING will be executed. The minimum number of TRIALS is given by MIN_TRIALS, specified in the applicable application profile.

The steps to follow for each TRIAL are:

1. The TL will setup up the SETTING and will prepare the ARTIFACT for a proper synchronism between the presentation of the still image and the real interaction with the TOE.

2. The ATTACKER will prepare himself/herself to interact with the TOE, and the video of the bona-fide user to be attacked. Also, if needed, will prepare the access to the bona-fide user reference data.
3. The ATTACKER will perform an ATTEMPT to identify/verify, following the indication of the operational guide of the TOE, except for using the still image to replicate the SUBJECT when interacting with the TOE.
4. If the TOE outputs a result different from MATCH or NON_MATCH, a new ATTEMPT will be executed. This will be repeated until the limit given by MAX_ATTEMPTS is reached. In such case, the TOE results in an ERROR.
5. The TL will note the result obtained, increasing the number of MATCHES, NON_MATCHES or SUBJECT_ERRORS as applicable.
6. The ATTACKER will get himself/herself totally or partially out of the point of interaction with the TOE (e.g., will stop staring at the capture device, moving himself/herself significantly). This shall be done to ensure that the next TRIAL is a completely new interaction with the TOE.
7. If the result is an ERROR or a NON_MATCH, the ATTACKER will analyse how the TRIAL has been carried out, and will decide whatever modification that might be suitable in order to reach a MATCH in the next ATTEMPT.
8. If the TRIAL result is a MATCH, and the number of MATCHES gets higher than MAX_SUBJECT_MATCHES, the TL will jump to step 10, increasing the variable SUBJECTS_PASS. If SUBJECTS_PASS gets higher than MAX_SUBJECTS_PASS, all TRIALS for this test will be finished, resulting in a PASS for the TEST.
9. The TL returns to step 2, to repeat the process until MIN_TRIALS is reached for that ARTIFACT.
10. The ARTIFACT is changed, and the TL returns to step 1, until all ARTIFACTS have been used for that SETTING.

9.5.1.4 ATTEMPTS

For each TRIAL, a maximum number of MAX_ATTEMPTS is specified, in order to be able to obtain a proper biometric trait capture. That capture shall result in either a MATCH or a NON_MATCH.

If the TOE uses different types of proof-of-life mechanisms, and the proof-of-life mechanisms requested by the TOE during the ATTEMPT does not correspond to the one presented using the still image, the ATTEMPT will be considered invalid, not incrementing any counter. In such case, the ATTEMPT will be repeated, expecting that this time the proof-of-life mechanism will be the one that corresponds to the video.

If the number of ATTEMPTS gets higher than MAX_ATTEMPTS, the TRIAL will result in an ERROR.

9.5.1.5 Minimum attack level analysis

According to the definitions in part 1, the attack level is given in the following table:

Table 11 — T4-3-1 attack level analysis

CRITERIA	IDENTIFICATION INTERVAL	IDENTIFICATION WEIGHT	EXPLOITATION INTERVAL	EXPLOITATION WEIGHT
Time effort	< one hour	0	< one hour	0
	< one day	1	< one day	3
	< three days	2	< three days	4

	< 7 days	3	< 7 days	6
	< 25 days	6	< 25 days	8
	> 25 days	10	> 25 days	10
	Not practical	*	Not practical	*
Expertise	Layman	0	Layman	0
	Skilled	2	Skilled	2
	Expert	5	Expert	4
	Multiple experts	7	Multiple experts	6
Knowledge of product	Public information	0	Public information	0
	Restricted information	2	Restricted information	2
	Sensitive information	4	Sensitive information	3
	Critical information	6	Critical information	5
Equipment	Standard	0	Standard	0
	Specialized	2	Specialized	4
	Bespoke	4	Bespoke	6
	Multiple Bespoke	6	Multiple Bespoke	10
	Not Practical	*	Not Practical	*
Access to TOE	Easy	0	Easy	0
	Moderate	2	Moderate	2
	Difficult	4	Difficult	4
Access to biometric characteristic	Not needed	0	Not needed	0
	Easy	0	Easy	0
	Moderate	4	Moderate	4
	Difficult	8	Difficult	8
Degree of scrutiny	None	0	None	0
	Overseen	2	Overseen	3
	Not Practical	*	Not Practical	*
LEVEL / TOTAL WEIGHT		0		0
ASSURANCE LEVEL	0-10 No rating - 11-20 Basic - 1 21-30 Enhanced Basic - 2 31-40 Moderate - 3 >40 High - 4 or 5	0	No rating	N/A

9.5.1.6 Data to be included in the ETR

In addition to all what it is specified in 9.2.4, the ETR shall also include:

- The still images generated for the ATTACKS
- Depending on the application profile:
 - The appropriate metrics value as defined in the ISO/IEC 30107-3 for each PAI species used. Or;
 - The quotation of the ATTACK performed with an ARTIFACT which has been classified as vulnerability (identified and exploited) according to the attack rating methodology as defined in (WI=00224273).

9.5.2 Test T4-3-2: Videos as ARTIFACTS

9.5.2.1 Description

The main goal of this test is to check if the TOE is vulnerable to the impersonation of a bona-fide user, by an ATTACKER that uses a video from that bona-fide user's face. The ATTACKER presents the video while interacting with the TOE for reaching a biometric verification.

It is important to reach a proper synchronization between the video and the TOE interaction, so that the proof-of-life (if available), will be contextual meaningful in the use of the TOE.

In general terms, this test is executed in the same way as in T4-1, where the desirable results for the TRIAL is either NON_MATCH or ERROR, while the non-desired result will be a MATCH.

9.5.2.2 Materials

For all TRIALS to be executed in this test, the material to be used will be the specified in 9.2.2.

In addition, the following material is needed:

- The artifacts classified as videos
- The specific material needed to present the artifact to the TOE (e.g., a tablet to display portrait video of the bona-fide user targeted by the ATTACKER)

NOTE These videos can be recorded while the bona-fide user interacts with the TOE during the Phase 2 tests in the use case of replay attacks.

9.5.2.3 TRIALS

During this test, a set of TRIALS for each ARTIFACT and SETTING will be executed. The minimum number of TRIALS is given by MIN_TRIALS, specified in the applicable application profile.

The steps to follow for each TRIAL are:

1. The TL will setup up the SETTING and will prepare the ARTIFACT for a proper synchronism between the presentation of the video artifact and the real interaction with the TOE.
2. The ATTACKER will prepare himself/herself to interact with the TOE, and the video of the bona-fide user to be attacked. Also, if needed, will prepare the access to the bona-fide user reference data.
3. The ATTACKER will perform an ATTEMPT to identify/verify, following the indication of the operational guide of the TOE, except for using the video to replicate the SUBJECT interaction with the TOE.
4. If the TOE outputs a result different from MATCH or NON_MATCH, a new ATTEMPT will be executed. This will be repeated until the limit given by MAX_ATTEMPTS is reached. In such case, the TOE results in an ERROR.
5. The TL will note the result obtained, increasing the number of MATCHES, NON_MATCHES or SUBJECT_ERRORS as applicable.
6. The ATTACKER will get himself/herself totally or partially out of the point of interaction with the TOE (e.g., will stop staring at the capture device, moving himself/herself significantly). This shall be done to ensure that the next TRIAL es a completely new interaction with the TOE.
7. If the result is an ERROR or a NON_MATCH, the ATTACKER will analyse how the TRIAL has been carried out, and will decide whatever modification that might be suitable in order to reach a MATCH in the next ATTEMPT.
8. If the TRIAL result is a MATCH, and the number of MATCHES gets higher than MAX_SUBJECT_MATCHES, the TL will jump to step 10, increasing the variable SUBJECTS_PASS. If SUBJECTS_PASS gets higher than MAX_SUBJECTS_PASS, all TRIALS for this test will be finished, resulting in a PASS for the TEST.
9. The TL returns to step 2, to repeat the process until MIN_TRIALS is reached for that ARTIFACT.

10. The ARTIFACT is changed, and the TL returns to step 1, until all ARTIFACTS have been used for that SETTING.

9.5.2.4 ATTEMPTS

For each TRIAL, a maximum number of MAX_ATTEMPTS is specified, in order to be able to obtain a proper biometric trait capture. That capture shall result in either a MATCH or a NON_MATCH.

If the TOE uses different types of proof-of-life mechanisms, and the proof-of-life mechanisms requested by the TOE during the ATTEMPT does not correspond to the one represented in the video, the ATTEMPT will be considered invalid, not incrementing any counter. In such case, the ATTEMPT will be repeated, expecting that this time the proof-of-life mechanism will be the one that corresponds to the video.

If the number of ATTEMPTS gets higher than MAX_ATTEMPTS, the TRIAL will result in an ERROR.

9.5.2.5 Minimum attack level analysis

Several scenarios can be considered for this test. In the case of the attacker using a large TV playing a regular video of the bona-fide user, the attack level is given in the following table:

Table 12 — T4-3-2 attack level analysis (large TV with regular video)

CRITERIA	IDENTIFICATION INTERVAL	IDENTIFICATION WEIGHT	EXPLOITATION INTERVAL	EXPLOITATION WEIGHT
Time effort	< one hour	0	< one hour	0
	< one day	1	< one day	3
	< three days	2	< three days	4
	< 7 days	3	< 7 days	6
	< 25 days	6	< 25 days	8
	> 25 days	10	> 25 days	10
	Not practical	*	Not practical	*
Expertise	Layman	0	Layman	0
	Skilled	2	Skilled	2
	Expert	5	Expert	4
	Multiple experts	7	Multiple experts	6
	Public information	0	Public information	0
Knowledge of product	Restricted information	2	Restricted information	2
	Sensitive information	4	Sensitive information	3
	Critical information	6	Critical information	5
	Standard	0	Standard	0
Equipment	Specialized	2	Specialized	4
	Bespoke	4	Bespoke	6
	Multiple Bespoke	6	Multiple Bespoke	10
	Not Practical	*	Not Practical	*
	Easy	0	Easy	0
Access to TOE	Moderate	2	Moderate	2
	Difficult	4	Difficult	4
	Not needed	0	Not needed	0
Access to biometric characteristic	Easy	0	Easy	0
	Moderate	4	Moderate	4
	Difficult	8	Difficult	8
	None	0	None	0
Degree of scrutiny	Overseen	2	Overseen	3

	Not Practical	*	Not Practical	*
LEVEL / TOTAL WEIGHT		1		0
ASSURANCE LEVEL	0-10 No rating – 11-20 Basic - 1 21-30 Enhanced Basic – 2 31-40 Moderate – 3 >40 High – 4 or 5	1+0 = 1	No rating	N/A

In the case of the attacker using a portable device playing a regular video of the bona-fide user, the attack level is given in the following table:

Table 13 —T4-3-2 attack level analysis (portable device and regular video)

CRITERIA	IDENTIFICATION INTERVAL	IDENTIFICATION WEIGHT	EXPLOITATION INTERVAL	EXPLOITATION WEIGHT
Time effort	< one hour	0	< one hour	0
	< one day	1	< one day	3
	< three days	2	< three days	4
	< 7 days	3	< 7 days	6
	< 25 days	6	< 25 days	8
	> 25 days	10	> 25 days	10
	Not practical	*	Not practical	*
Expertise	Layman	0	Layman	0
	Skilled	2	Skilled	2
	Expert	5	Expert	4
	Multiple experts	7	Multiple experts	6
Knowledge of product	Public information	0	Public information	0
	Restricted information	2	Restricted information	2
	Sensitive information	4	Sensitive information	3
	Critical information	6	Critical information	5
Equipment	Standard	0	Standard	0
	Specialized	2	Specialized	4
	Bespoke	4	Bespoke	6
	Multiple Bespoke	6	Multiple Bespoke	10
	Not Practical	*	Not Practical	*
Access to TOE	Easy	0	Easy	0
	Moderate	2	Moderate	2
	Difficult	4	Difficult	4
Access to biometric characteristic	Not needed	0	Not needed	0
	Easy	0	Easy	0
	Moderate	4	Moderate	4
	Difficult	8	Difficult	8
Degree of scrutiny	None	0	None	0
	Overseen	2	Overseen	3
	Not Practical	*	Not Practical	*
LEVEL / TOTAL WEIGHT		1		0
ASSURANCE LEVEL	0-10 No rating – 11-20 Basic - 1 21-30 Enhanced Basic – 2 31-40 Moderate – 3 >40 High – 4 or 5	1+0 = 1	No rating	N/A

In the case of the attacker using a large TV playing a video of the bona-fide user that shows the response to the proof-of-life mechanism requested by the TOE, the attack level is given in the following table:

Table 14 —T4-3-2 attack level analysis (large TV with proof-of-life request video)

CRITERIA	IDENTIFICATION INTERVAL	IDENTIFICATION WEIGHT	EXPLOITATION INTERVAL	EXPLOITATION WEIGHT
Time effort	< one hour	0	< one hour	0
	< one day	1	< one day	3
	< three days	2	< three days	4
	< 7 days	3	< 7 days	6
	< 25 days	6	< 25 days	8
	> 25 days	10	> 25 days	10
	Not practical	*	Not practical	*
Expertise	Layman	0	Layman	0
	Skilled	2	Skilled	2
	Expert	5	Expert	4
	Multiple experts	7	Multiple experts	6
Knowledge of product	Public information	0	Public information	0
	Restricted information	2	Restricted information	2
	Sensitive information	4	Sensitive information	3
	Critical information	6	Critical information	5
Equipment	Standard	0	Standard	0
	Specialized	2	Specialized	4
	Bespoke	4	Bespoke	6
	Multiple Bespoke	6	Multiple Bespoke	10
	Not Practical	*	Not Practical	*
Access to TOE	Easy	0	Easy	0
	Moderate	2	Moderate	2
	Difficult	4	Difficult	4
Access to biometric characteristic	Not needed	0	Not needed	0
	Easy	0	Easy	0
	Moderate	4	Moderate	4
	Difficult	8	Difficult	8
Degree of scrutiny	None	0	None	0
	Overseen	2	Overseen	3
	Not Practical	*	Not Practical	*
LEVEL / TOTAL WEIGHT		11		4
ASSURANCE LEVEL	0-10 No rating - 11-20 Basic - 1 21-30 Enhanced Basic - 2 31-40 Moderate - 3 >40 High - 4 or 5	11+4 = 15	Basic	AVA_VAN.1

9.5.2.6 Data to be included in the ETR

In addition to all what it is specified in 9.2.4, the ETR shall also include:

- The videos generated for the ATTACKS.
- Depending on the application profile:
 - The appropriate metrics value as defined in the ISO/IEC 30107-3 for each PAI species used. Or;
 - The quotation of the ATTACK performed with an ARTIFACT which has been classified as vulnerability (identified and exploited) according to the attack rating methodology as defined in (WI=00224273).

9.5.3 Test T4-3-3: Low-cost masks as ARTIFACTS

9.5.3.1 Description

The main goal of this test is to check that the TOE is not vulnerable to the impersonation of a bona-fide user, by the use of low-cost masks as an artifact.

In general terms, this test is executed in the same way as T4-1, where the desirable result for each TRIAL is either a NON_MATCH or an ERROR, while the non-desired result is a MATCH.

9.5.3.2 Materials

For all TRIALS to be executed in this test, the material to be used will be the specified in 9.2.2.

In addition, the TL shall provide at least two kinds of low-cost mask that will represent the face of the bona-fide users (i.e., at least two masks per users).

These masks can be, for example:

- A printed-paper, with the material out of the face chopped out, and the eyes being cut as to allow the eyes of the ATTACKER to be seen. The material with which the printed copy is made, shall allow the most natural feeling possible, avoiding, for example, light reflections from the TOE or the scenery. Depending on the TOE, the ink with which the paper is printed, could lead to NON_MATCHES results, so it is recommended that half of the masks are printed with a laser printer, and the other half with ink-injection printers.
- A personalized second skin. This is a piece of cloth, as some kind of stockings, with the face of the bona-fide user printed. Such second skin is placed over the face of the ATTACKER. The cloth shall have holes for the eyes and the mouth. It shall be placed in a way that wrinkles are not visible, and shall be completed with the use of wigs and any other kind of cosmetic apparel that may lead the ATTACKER to look more similar to the bona-fide user. Figure 1 shows some examples of second-skins.

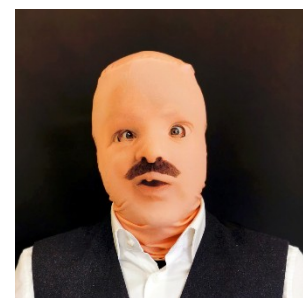
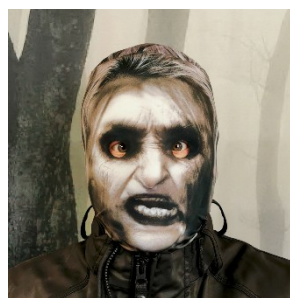


Figure 1 — Examples of second-skin products¹

- A face photograph printed on a t-shirt or textile support. This will allow the ATTACKER give a 3D shape to the face thanks to the flexible aspect of the textile.
- A mask of the targeted bona-fide user printed in 3D thanks to a low-cost 3D printer (a PLA 3D printer or a resin 3D printer for instance). These masks will be realised from a face model created from photographs of the victim.

EDITOR'S NOTE: insert a photo of the 3D printed masks. Contributions are welcomed.

¹ Images taken from <https://www.britishmade.gifts>

9.5.3.3 TRIALS

During this test, a set of TRIALS for each ARTIFACT and SETTING will be executed. The minimum number of TRIALS is given by MIN_TRIALS, specified in the applicable application profile.

The steps to follow for each TRIAL are:

1. The TL will setup up the SETTING and will prepare the SUBJECT (i.e., the ATTACKER) and the ARTIFACT. The ATTACKER is reminded to be as cooperative as possible with the TOE, including the proof-of-life mechanisms (if available).
2. The ATTACKER will prepare himself/herself to interact with the TOE, and wears the mask properly. Also, if needed, will prepare the access to the bona-fide user reference data.
3. The ATTACKER will perform an ATTEMPT to identify/verify, following the indication of the operational guide of the TOE, except for using mask to impersonate the bona-fide user.
4. If the TOE outputs a result different from MATCH or NON_MATCH, a new ATTEMPT will be executed. This will be repeated until the limit given by MAX_ATTEMPTS is reached. In such case, the TOE results in an ERROR.
5. The TL will note the result obtained, increasing the number of MATCHES, NON_MATCHES or SUBJECT_ERRORS as applicable.
6. The ATTACKER will get himself/herself totally or partially out of the point of interaction with the TOE (e.g., will stop staring at the capture device, moving himself/herself significantly). This shall be done to ensure that the next TRIAL es a completely new interaction with the TOE.
7. If the result is an ERROR or a NON_MATCH, the ATTACKER will analyse how the TRIAL has been carried out, and will decide whatever modification that might be suitable in order to reach a MATCH in the next ATTEMPT.
8. If the TRIAL result is a MATCH, and the number of MATCHES gets higher than MAX_SUBJECT_MATCHES, the TL will jump to step 10, increasing the variable SUBJECTS_PASS. If SUBJECTS_PASS gets higher than MAX_SUBJECTS_PASS, all TRIALS for this test will be finished, resulting in a PASS for the TEST.
9. The TL returns to step 2, to repeat the process until MIN_TRIALS is reached for that ARTIFACT.
10. The ARTIFACT is changed, and the TL returns to step 1, until all ARTIFACTS have been used for that SETTING.

9.5.3.4 Minimum attack level analysis

Several scenarios can be considered for this test. In the case of the attacker uses a home-made paper mask, the attack level is given in the following table:

Table 15 —T4-3-3 attack level analysis (paper mask)

CRITERIA	IDENTIFICATION INTERVAL	IDENTIFICATION WEIGHT	EXPLOITATION INTERVAL	EXPLOITATION WEIGHT
Time effort	< one hour	0	< one hour	0
	< one day	1	< one day	3
	< three days	2	< three days	4
	< 7 days	3	< 7 days	6
	< 25 days	6	< 25 days	8

	> 25 days Not practical	10 *	> 25 days Not practical	10 *
Expertise	Layman	0	Layman	0
	Skilled	2	Skilled	2
	Expert	5	Expert	4
	Multiple experts	7	Multiple experts	6
Knowledge of product	Public information	0	Public information	0
	Restricted information	2	Restricted information	2
	Sensitive information	4	Sensitive information	3
	Critical information	6	Critical information	5
Equipment	Standard	0	Standard	0
	Specialized	2	Specialized	4
	Bespoke	4	Bespoke	6
	Multiple Bespoke	6	Multiple Bespoke	10
	Not Practical	*	Not Practical	*
Access to TOE	Easy	0	Easy	0
	Moderate	2	Moderate	2
	Difficult	4	Difficult	4
Access to biometric characteristic	Not needed	0	Not needed	0
	Easy	0	Easy	0
	Moderate	4	Moderate	4
	Difficult	8	Difficult	8
Degree of scrutiny	None	0	None	0
	Overseen	2	Overseen	3
	Not Practical	*	Not Practical	*
LEVEL / TOTAL WEIGHT		3 / 5		2 / 0
ASSURANCE LEVEL	0-10 No rating – 11-20 Basic - 1 21-30 Enhanced Basic – 2 31-40 Moderate – 3 >40 High – 4 or 5	3+2 = 5	No rating	N/A

In the case that the attacker uses a painted 2nd skin material, with holes for eyes and mouth, the attack level is given in the following table:

Table 16 —T4-3-3 attack level analysis (painted 2nd skin)

CRITERIA	IDENTIFICATION INTERVAL	IDENTIFICATION WEIGHT	EXPLOITATION INTERVAL	EXPLOITATION WEIGHT
Time effort	< one hour	0	< one hour	0
	< one day	1	< one day	3
	< three days	2	< three days	4
	< 7 days	3	< 7 days	6
	< 25 days	6	< 25 days	8
	> 25 days	10	> 25 days	10
	Not practical	*	Not practical	*
Expertise	Layman	0	Layman	0
	Skilled	2	Skilled	2
	Expert	5	Expert	4
	Multiple experts	7	Multiple experts	6
Knowledge of product	Public information	0	Public information	0
	Restricted information	2	Restricted information	2
	Sensitive information	4	Sensitive information	3
	Critical information	6	Critical information	5
Equipment	Standard	0	Standard	0
	Specialized	2	Specialized	4
	Bespoke	4	Bespoke	6

	Multiple Bespoke Not Practical	6 *	Multiple Bespoke Not Practical	10 *
Access to TOE	Easy Moderate Difficult	0 2 4	Easy Moderate Difficult	0 2 4
Access to biometric characteristic	Not needed Easy Moderate Difficult	0 0 4 8	Not needed Easy Moderate Difficult	0 0 4 8
Degree of scrutiny	None Overseen Not Practical	0 2 *	None Overseen Not Practical	0 3 *
LEVEL / TOTAL WEIGHT		3 / 5		2 / 0
ASSURANCE LEVEL	0-10 No rating - 11-20 Basic - 1 21-30 Enhanced Basic - 2 31-40 Moderate - 3 >40 High - 4 or 5	5+0 = 5	No rating	N/A

9.5.3.5 Data to be included in the ETR

In addition to all what it is specified in 9.2.4, the ETR shall also include:

- The number and types (with evidences, such as photographs or videos) of the artifacts used (i.e., the low-cost masks).
- Depending on the application profile:
 - The appropriate metrics value as defined in the ISO/IEC 30107-3 for each PAI species used. Or;
 - The quotation of the ATTACK performed with an ARTIFACT which has been classified as vulnerability (identified and exploited) according to the attack rating methodology as defined in (WI=00224273).

9.5.4 Test T4-3-4: Advanced masks as ARTIFACTS

9.5.4.1 Description

The main goal of this test is to check that the TOE is not vulnerable to the impersonation of a bona-fide user, by the use of advanced masks as an artifact.

In general terms, this test is executed in the same way as T4-1, where the desirable result for each TRIAL is either a NON_MATCH or an ERROR, while the non-desired result is a MATCH.

9.5.4.2 Materials

For all TRIALS to be executed in this test, the material to be used will be the specified in 9.2.2.

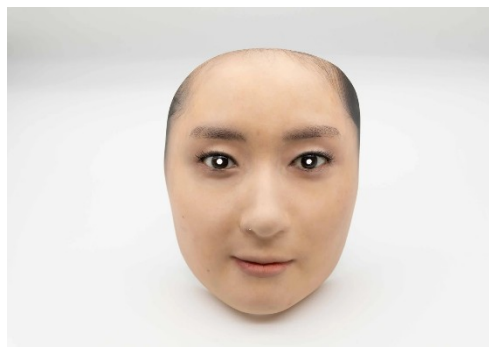
In addition, the TL shall provide at least three kinds of advanced mask, which shall follow the following requirements:

- Three kinds of advanced masks, that will represent the face of at least two bona-fide users. This will fulfil the following specifications:

- The mask shall represent one of the following two options:
 - The face of, at least, 2 bona-fide users.
 - The face of, at least, 2 generic users, for which the reference data is also available. In this case, those generic users will be considered as bona-fide users. This option is available to allow cost reduction in case the advanced mask may increase the budget significantly.
- An advanced mask is that kind of mask that will show with all detail the facial look of the bona-fide user, including the skin tone and the 3D structure. Some examples of these kind of masks can be seen in the Figure 2. As an example, these masks can be:
 - 3D-coloured printed masks
 - 3D latex masks
 - 3D silicone masks



a)



b)

Figure 2 — Some examples of advanced masks²

9.5.4.3 TRIALS

During this test, a set of TRIALS for each ARTIFACT and SETTING will be executed. The minimum number of TRIALS is given by MIN_TRIALS, specified in the applicable application profile.

The steps to follow for each TRIAL are:

1. The TL will setup up the SETTING and will prepare the SUBJECT (i.e., the ATTACKER). The ATTACKER is reminded to be as cooperative as possible with the TOE, including the proof-of-life mechanisms (if available).
2. The ATTACKER will prepare himself/herself to interact with the TOE, and wears the mask properly. Also, if needed, will prepare the access to the bona-fide user reference data.
3. The ATTACKER will perform an ATTEMPT to identify/verify, following the indication of the operational guide of the TOE, except for using mask to impersonate the bona-fide user.
4. If the TOE outputs a result different from MATCH or NON_MATCH, a new ATTEMPT will be executed. This will be repeated until the limit given by MAX_ATTEMPTS is reached. In such case, the TOE results in an ERROR.

² Images taken from: a) http://real-f.jp/en_news.html; b) <https://www.etsy.com/es/shop/maskshopOMOTE>

5. The TL will note the result obtained, increasing the number of MATCHES, NON_MATCHES or SUBJECT_ERRORS as applicable.
6. The ATTACKER will get himself/herself totally or partially out of the point of interaction with the TOE (e.g., will stop staring at the capture device, moving himself/herself significantly). This shall be done to ensure that the next TRIAL is a completely new interaction with the TOE.
7. If the result is an ERROR or a NON_MATCH, the ATTACKER will analyse how the TRIAL has been carried out, and will decide whatever modification that might be suitable in order to reach a MATCH in the next ATTEMPT.
8. If the TRIAL result is a MATCH, and the number of MATCHES gets higher than MAX_SUBJECT_MATCHES, the TL will jump to step 10, increasing the variable SUBJECTS_PASS. If SUBJECTS_PASS gets higher than MAX_SUBJECTS_PASS, all TRIALS for this test will be finished, resulting in a PASS for the TEST.
9. The TL returns to step 2, to repeat the process until MIN_TRIALS is reached for that SUBJECT.
10. The ARTIFACT is changed, and the TL returns to step 1, until all ARTIFACTS have been used for that SETTING.

9.5.4.4 Minimum attack level analysis

According to the definitions in part 1, the attack level is given in the following table:

Table 17 — T4-3-4 attack level analysis

CRITERIA	IDENTIFICATION INTERVAL	IDENTIFICATION WEIGHT	EXPLOITATION INTERVAL	EXPLOITATION WEIGHT
Time effort	< one hour	0	< one hour	0
	< one day	1	< one day	3
	< three days	2	< three days	4
	< 7 days	3	< 7 days	6
	< 25 days	6	< 25 days	8
	> 25 days	10	> 25 days	10
	Not practical	*	Not practical	*
Expertise	Layman	0	Layman	0
	Skilled	2	Skilled	2
	Expert	5	Expert	4
	Multiple experts	7	Multiple experts	6
Knowledge of product	Public information	0	Public information	0
	Restricted information	2	Restricted information	2
	Sensitive information	4	Sensitive information	3
	Critical information	6	Critical information	5
Equipment	Standard	0	Standard	0
	Specialized	2	Specialized	4
	Bespoke	4	Bespoke	6
	Multiple Bespoke	6	Multiple Bespoke	10
	Not Practical	*	Not Practical	*
Access to TOE	Easy	0	Easy	0
	Moderate	2	Moderate	2
	Difficult	4	Difficult	4
Access to biometric characteristic	Not needed	0	Not needed	0
	Easy	0	Easy	0
	Moderate	4	Moderate	4

	Difficult	8	Difficult	8
Degree of scrutiny	None	0	None	0
	Overseen	2	Overseen	3
	Not Practical	*	Not Practical	*
LEVEL / TOTAL WEIGHT		12		9
ASSURANCE LEVEL	0-10 No rating - 11-20 Basic - 1 21-30 Enhanced Basic - 2 31-40 Moderate - 3 >40 High - 4 or 5	12+9 = 21	Enhanced Basic	AVA_VAN.2

9.5.4.5 Data to be included in the ETR

In addition to all what it is specified in 9.2.4, the ETR shall also include:

- The number and types (with evidences, such as photographs or videos) of the artifacts used (i.e., the advanced masks).
- Depending on the application profile:
 - The appropriate metrics value as defined in the ISO/IEC 30107-3 for each PAI species used. Or;
 - The quotation of the ATTACK performed with an ARTIFACT which has been classified as vulnerability (identified and exploited) according to the attack rating methodology as defined in (WI=00224273).

9.5.5 Test T4-3-5: Make-up-based attacks

9.5.5.1 Description

The main goal of this test is to check that the TOE is not vulnerable to the impersonation of a bona-fide user, by the use of make-up as an artifact.

In general terms, this test is executed in the same way as T4-1, where the desirable result for each TRIAL is either a NON_MATCH or an ERROR, while the non-desired result is a MATCH.

9.5.5.2 Materials

For all TRIALS to be executed in this test, the material to be used will be the specified in 9.2.2.

In addition, the following resources are needed:

- A make-up professional with more than 5-year experience
- Make-up material
- It is allowed to use volume-modifier-prosthesis, to create, increment or modify face volumes

The make-up professional shall try to get a facial look of the ATTACKER that will be similar to the bona-fide user. Similarity will be achieved if the result of comparing both images with REF_APP provides a score lower or equal to BONAFIDE_SIM_TH.

The make-up technique used might any available. An example could be using *contouring*, such as it can be seen in Figure 3:



Figure 3 — Examples of make-up using contouring³

9.5.5.3 TRIALS

During this test, a set of TRIALS for each SUBJECT and SETTING will be executed. The minimum number of TRIALS is given by MIN_TRIALS, specified in the applicable application profile.

The steps to follow for each TRIAL are:

1. The TL will setup up the SETTING and will prepare the SUBJECT (i.e., the ATTACKER). The ATTACKER is reminded to be as cooperative as possible with the TOE, including the proof-of-life mechanisms (if available).
2. The ATTACKER will prepare himself/herself to interact with the TOE, and wears the mask properly. Also, if needed, will prepare the access to the bona-fide user reference data.
3. The SUBJECT will perform an ATTEMPT to identify/verify, following the indication of the operational guide of the TOE, except for using the makeup to resemble to the bona-fide user.
4. If the TOE outputs a result different from MATCH or NON_MATCH, a new ATTEMPT will be executed. This will be repeated until the limit given by MAX_ATTEMPTS is reached. In such case, the TOE results in an ERROR.
5. The TL will note the result obtained, increasing the number of MATCHES, NON_MATCHES or SUBJECT_ERRORS as applicable.
6. The SUBJECT will get himself/herself totally or partially out of the point of interaction with the TOE (e.g., will stop staring at the capture device, moving himself/herself significantly). This shall be done to ensure that the next TRIAL es a completely new interaction with the TOE.

³ Images taken from: a) <https://www.demilked.com/celebrity-makeup-artist-face-paint-contouring-lucia-pittalis/> y b) <https://celebrity.land/maquilladora-talentosa-se-transforma-en-celebridades/>

7. If the result is an ERROR or a NON_MATCH, the ATTACKER will analyse how the TRIAL has been carried out, and will decide whatever modification that might be suitable in order to reach a MATCH in the next ATTEMPT.
8. If the TRIAL result is a MATCH, and the number of MATCHES gets higher than MAX_SUBJECT_MATCHES, the TL will jump to step 10, increasing the variable SUBJECTS_PASS. If SUBJECTS_PASS gets higher than MAX_SUBJECTS_PASS, all TRIALS for this test will be finished, resulting in a PASS for the TEST.
9. The TL returns to step 2, to repeat the process until MIN_TRIALS is reached for that SUBJECT.
10. The SUBJECT is changed, and the TL returns to step 1, until all SUBJECTS have been used for that SETTING.

9.5.5.4 Minimum attack level analysis

Several scenarios can be considered for this test. In the case that the make-up is done by a regular person which is able to properly make up himself/herself or another person, the attack level is given in the following table:

Table 18 — T4-3-5 attack level analysis (regular person)

CRITERIA	IDENTIFICATION INTERVAL	IDENTIFICATION WEIGHT	EXPLOITATION INTERVAL	EXPLOITATION WEIGHT
Time effort	< one hour	0	< one hour	0
	< one day	1	< one day	3
	< three days	2	< three days	4
	< 7 days	3	< 7 days	6
	< 25 days	6	< 25 days	8
	> 25 days	10	> 25 days	10
	Not practical	*	Not practical	*
Expertise	Layman	0	Layman	0
	Skilled	2	Skilled	2
	Expert	5	Expert	4
	Multiple experts	7	Multiple experts	6
Knowledge of product	Public information	0	Public information	0
	Restricted information	2	Restricted information	2
	Sensitive information	4	Sensitive information	3
	Critical information	6	Critical information	5
Equipment	Standard	0	Standard	0
	Specialized	2	Specialized	4
	Bespoke	4	Bespoke	6
	Multiple Bespoke	6	Multiple Bespoke	10
	Not Practical	*	Not Practical	*
Access to TOE	Easy	0	Easy	0
	Moderate	2	Moderate	2
	Difficult	4	Difficult	4
Access to biometric characteristic	Not needed	0	Not needed	0
	Easy	0	Easy	0
	Moderate	4	Moderate	4
Degree of scrutiny	Difficult	8	Difficult	8
	None	0	None	0
	Overseen	2	Overseen	3
	Not Practical	*	Not Practical	*
LEVEL / TOTAL WEIGHT		2		2
ASSURANCE LEVEL	0-10 No rating -	2+2 = 4	No rating	N/A

	11-20 Basic - 1 21-30 Enhanced Basic - 2 31-40 Moderate - 3 >40 High - 4 or 5			
--	--	--	--	--

In the case that the make-up is done by professional make-up artist, the attack level is given in the following table:

Table 19 —T4-3-5 attack level analysis (professional make-up artist)

CRITERIA	IDENTIFICATION INTERVAL	IDENTIFICATION WEIGHT	EXPLOITATION INTERVAL	EXPLOITATION WEIGHT
Time effort	< one hour	0	< one hour	0
	< one day	1	< one day	3
	< three days	2	< three days	4
	< 7 days	3	< 7 days	6
	< 25 days	6	< 25 days	8
	> 25 days	10	> 25 days	10
	Not practical	*	Not practical	*
Expertise	Layman	0	Layman	0
	Skilled	2	Skilled	2
	Expert	5	Expert	4
	Multiple experts	7	Multiple experts	6
Knowledge of product	Public information	0	Public information	0
	Restricted information	2	Restricted information	2
	Sensitive information	4	Sensitive information	3
Equipment	Critical information	6	Critical information	5
	Standard	0	Standard	0
	Specialized	2	Specialized	4
	Bespoke	4	Bespoke	6
Access to TOE	Multiple Bespoke	6	Multiple Bespoke	10
	Not Practical	*	Not Practical	*
	Easy	0	Easy	0
Access to biometric characteristic	Moderate	2	Moderate	2
	Difficult	4	Difficult	4
	Not needed	0	Not needed	0
Degree of scrutiny	Easy	0	Easy	0
	Moderate	4	Moderate	4
	Difficult	8	Difficult	8
LEVEL / TOTAL WEIGHT	None	0	None	0
	Overseen	2	Overseen	3
	Not Practical	*	Not Practical	*
LEVEL / TOTAL WEIGHT		7		13
ASSURANCE LEVEL	0-10 No rating - 11-20 Basic - 1 21-30 Enhanced Basic - 2 31-40 Moderate - 3 >40 High - 4 or 5	7+13 = 20	Enhanced Basic	AVA_VAN.2

9.5.5.5 Data to be included in the ETR

In addition to all what it is specified in 9.2.4, the ETR shall also include evidences of the make-up attacks (e.g., photographs or videos).

9.5.6 Test T4-3-6: Biometric data injection attacks

EDITOR'S NOTE: The content of this section has been proposed for the TS on Digital Injection and removed from here. This section shall refer to the work done in the TS on Digital Injection Attacks.

For the time being, the number is left as **(WI=00224273)**, as this is the work item number assigned to "Digital Presentation Attack in biometric systems" project. The number will be changed as soon as the real one is available.

9.5.6.1 Description

The main goal of this test is to check that the TOE is not vulnerable to the impersonation of a bona-fide user, by the use of biometric data injection attacks.

In general terms, this test is executed in the same way as T4-1, where the desirable result for each TRIAL is either a NON_MATCH or an ERROR, while the non-desired result is a MATCH.

This test shall follow the requirements described in **(WI=00224273). The passing criteria of this test described in the application profile shall be based on the rules defined in the Clause 9 and the Annex A of **(WI=00224273)**.**

9.5.6.2 Materials

For all TRIALS to be executed in this test, the material to be used will be the specified in 9.2.2.

In addition, the following materials are needed:

- The equipment to create the IAI used during the test
- The equipment to execute the different IAMs.

The TL shall use at least:

- **10 different attack types as defined in **(WI=00224273)****
- **2 different IAM as defined in **(WI=00224273)****

9.5.6.3 TRIALS

During this test, a set of TRIALS for each INJECTION_ATTACK and SETTING will be executed. The minimum number of TRIALS is given by MIN_TRIALS, specified in the applicable application profile.

The steps to follow for each TRIAL are:

1. The TL will setup up the SETTING and will prepare the INJECTION_ATTACK.
2. The ATTACKER will perform an ATTEMPT to identify/verify, following the indication of the operational guide of the TOE.

3. If the TOE outputs a result different from MATCH or NON_MATCH, a new ATTEMPT will be executed. This will be repeated until the limit given by MAX_ATTEMPTS is reached. In such case, the TOE results in an ERROR.
4. The TL will note the result obtained, increasing the number of MATCHES, NON_MATCHES or SUBJECT_ERRORS as applicable.
5. The ATTACKER will stop the injection. This shall be done to ensure that the next TRIAL is a completely new interaction with the TOE.
6. If the result is an ERROR or a NON_MATCH, the ATTACKER will analyse how the TRIAL has been carried out, and will decide whatever modification that might be suitable in order to reach a MATCH in the next ATTEMPT.
7. If the TRIAL result is a MATCH, and the number of MATCHES gets higher than MAX_SUBJECT_MATCHES, the TL will jump to step 10, increasing the variable SUBJECTS_PASS. If SUBJECTS_PASS gets higher than MAX_SUBJECTS_PASS, all TRIALS for this test will be finished, resulting in a PASS for the TEST.
8. The TL returns to step 2, to repeat the process until MIN_TRIALS is reached for that INJECTION_ATTACK.
9. The INJECTION_ATTACK is changed, and the TL returns to step 1, until all INJECTION_ATTACKS have been used for that SETTING.

9.5.6.4 Data to be included in the ETR

In addition to all what it is specified in 9.2.4, the ETR shall also include:

- Images of the attack types used during the tests
- Attack quotation following the attack rating methodology defined in clause 12 of the (WI=00224273) if an attack has been classified as vulnerability (identified and exploited).

EDITOR'S NOTE: Double check the clause number whenever the TS will go to publication, or better refer to the clause by its title, to avoid the need of using dated references in this standard.

Annex A (normative)1204

Profile 1: Remote identity verification using video-conferencing tools and pre-issued documents, with human supervision before final decision

EDITOR'S NOTE: One example of this application profile is the case of Spanish STIC 140 F11 and IT-14

EDITOR'S NOTE: The current text is taken from IT-14, which corresponds to this annex, but with also the constraint of being tested under a "Common Criteria Light" scheme, such as the one called in Spain as LINCE (limited time for the evaluation, limited budget for the evaluation). The security level is, therefore, considered as HIGH, but in future version of this annex, it may be possible to generalize this specification to also allow security level SUBSTANTIAL, as a subset.

EDITOR'S NOTE: These annexes are not compliant at this moment with the definition of application profile in Part 1. This will be corrected in future cycles, as soon as Part 1 becomes stable enough.

EDITOR'S NOTE: The passing criteria, the tests and the associated settings will be rebuilt to take into account two different LoA: Substantial and High. This will help to get a conformity with the French PVID in addition to the Spanish STIC 140 F11.

A.1 Introduction

This Annex describes the application profile for a product that used facial biometrics for verifying the identity of a citizen against the photograph previously enrolled in an ID document (e.g., National Identity Card, Passport, etc.). Therefore, the enrolment is not part of the application (i.e., is not part of the TOE).

In addition, this application performs this biometric verification using videoconferencing tools (e.g., a webcam through a webpage, a mobile app with the own mobile camera, etc.).

Last, but not least, this application does not take a final decision in an automatic manner. The final decision is taken by a human operator, who uses the output of this application as input data for taking that decision.

As it is detailed, this application enforces certain tests, while dismiss others due to the non-applicability/non-viability in this context.

This application profile can be taken by any certification body, government and/or sector, to define and evaluate the requirements for their biometric products. This may be used in coordination with other current National initiatives. Governments may decide to give a higher preference to other National specifications.

A.2 TOE description

The TOE of this application profile is a product that is able to perform biometric verification using facial biometrics, with the following characteristics:

- The biometric verification is carried out using video-conferencing tools.
- No platform is required, neither recommended. In other words, this can be executed using a workstation, or using any kind of mobile device. Also, operating system used is not specified, so

anyone in the market might be applicable (e.g., Microsoft Windows, MacOS, iOS, Android, Linux, etc.)

- The capture device is also not fixed, so it will be at the choice of the citizen, and related with the platform used by the citizen. It could be a webcam, the embedded camera in their mobile device (either rear or front), etc.
- The remote video-identification is supervised by a human operator, who is the one taking the final decision. This will be done in an asynchronous manner.
- The verification is done between the live image of the citizen, and the one captured from an accepted document (e.g., any official document, such as a National Identity Card, or a Passport). The TOE might allow the user to read the information of the facial image electronically (e.g., through the NFC interface), or by performing a live scanning of the surface of the document, to detect the printed image of the face. Therefore, the reference data will be the one obtained from that document.
- The TOE shall be compliant with "Common Criteria Light" certification (e.g., LINCE scheme in Spain).
- The TOE shall send the human operator, or relevant evidences that will allow the operator to take the final decision.
- The citizen may perform this operation anywhere and at any time. Therefore, the context and background of the facial verification is not controlled.
- The TOE shall implement proof-of-life mechanisms, to detect that the citizen at the other end of the videoconference, is a living person.

TOE's operation shall follow this sequence, where steps 2 and 3 can be exchanged in order:

1. An application requests a biometric verification through videoconference to the TOE.
2. The TOE asks the SUBJECT to acquire a living image/video of his/her face in an official identity document. This acquisition could be done by electronic means (e.g., reading the information stored in a contactless card), or by scanning the printed facial imaged in the document.
 - a. The TOE decides if the acquisition has been successful. If that is not the case, the TOE may cancel the whole process, or ask to repeat the process a certain number of times (i.e., a certain number of ATTEMPTS).
 - b. The TOE may decide to cancel the acquisition, after a certain time has passed (i.e., a timeout)
3. The TOE asks the SUBJECT to perform a live capture of his face (image or video), using the device camera (e.g., uploading a photograph is not allowed).
 - a. The TOE decides if the acquisition has been successful. If that is not the case, the TOE may cancel the whole process, or ask to repeat the process a certain number of times (i.e., a certain number of ATTEMPTS).
 - b. The TOE may decide to cancel the acquisition, after a certain time has passed (i.e., a timeout)
4. The TOE performs the biometric comparison between the document info acquired, and the live acquisition of the face, and gets a result.
5. The TOE will send all the evidences to a SERVER, including the comparison result, the captured images, a trace of the video in the process of acquiring the images.
6. If the biometric comparison is a FAIL, the TOE may decide to cancel the whole process, or require a repetition to the SUBJECT, until a certain number of ATTEMPTS is reached (i.e., NUM_MAX_INT_VERIF)

7. A human operator checks all evidences received, and will ratify the biometric comparison, or deny it.

The following figure summarizes the context of the TOE.

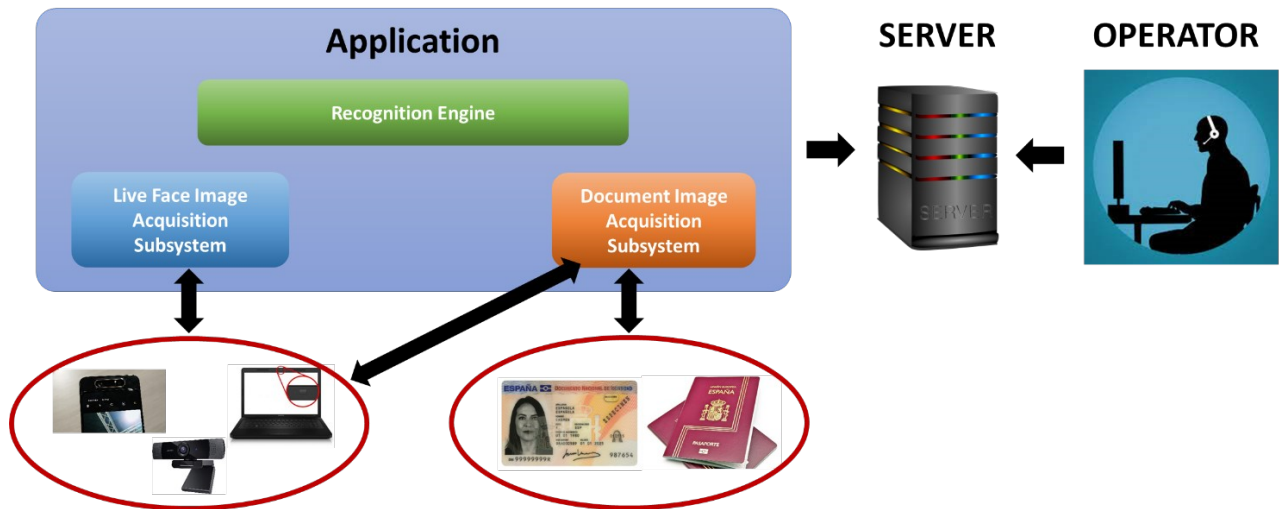


Figure 5 — TOE's Block Diagram

Important details from the TOE to highlight are:

- The TOE is not a simple biometric algorithm, but what can be called as a biometric engine.
- The performance of the biometric engine might differ significantly from the biometric algorithm performance, as it will be dependent on the quality of the face images captured, and use for the comparison.
- As the one acquiring the images is the SUBJECT himself, and the capture device is also chosen by the SUBJECT, there could be a significant difference among the performance achieved by all SUBJECTS. This could lead to high acquisition failures (FTA), or that the manufacturer decides to lower the decision criteria, in order reduce the number of FTAs or improve the performance.
- Capture devices:
 - At the own choice of the SUBJECT, unless the TOE manufacturer establishes some kind of limitation on the capture devices to be used.
 - If the manufacturer does not impose any limitation related to the quality of the camera, the minimum camera to be used will be a visible-range camera, with 0,9 megapixels, and 50Hz refresh rate.
 - If the manufacturer imposes some limits on the capture device to be used, the worst ones from those allowed by the TOE will be used as the one for the tests.
- Environment:
 - There is no restriction about the environment, unless the TOE shows some limitations. This means that is totally feasible for the user to perform the evaluation with a moving outdoors environment including some other people that may be, even, looking at the camera.
 - Also, lighting conditions are not fixed by default, neither face pose, nor cosmetics artefact, such as glasses, make-up, tattoos, etc.
 - The TOE manufacturer or the Customer shall define what it is considered for them the SETTING of the typical use case. That shall be detailed in the SD_TOE, and shall also be included into the ETR.

A.3 Levels of assurance

This application profile is defined under the condition of LoA “High”, as specified in part 1 of this family of standards.

For the calculation of the attack level of each of the tests defined for Phase 4, the following intervals excel the minimum ones defined in each of the Tests:

- Knowledge of the product: In this application profile, the TOE is expected to be used by any citizen, with basic knowledge of IT products at user level. Therefore, the attacker only needs public information. The only piece of information that might be considered differently, is the way the product performs the proof-of-life. But in those products where the proof-of-life is achieved by using a challenge-response strategy, the attacker, by just using the TOE several times before, is able to learn how it works, without accessing restricted information. So, by default, the interval shall be “Public Information”. In those cases where the proof-of-life is implicit, then the attacker may need restricted information to attempt a successful attack. So, in such a case the interval chosen for both Identification and Exploitation phases shall be “Restricted information”.
- Access to TOE: In this application profile, the TOE is available to the attacker at any moment, as it can even be his/her own mobile device. Therefore, the interval shall be fixed to “Easy”.
- Access to biometric characteristic: The biometric characteristic is an image (or video) of the face, which is extremely easy to acquire. On the other hand, the biometric reference is also acquired from a document that may not have electronic means for supplying the photograph of the face. Therefore, the interval shall be fixed to “Easy”
- Degree of scrutiny: The TOE is expected to be used by the citizen at any place, including those in which there is no possibility of being overseen. Therefore, the interval shall be fixed to “None”.

With these parameters, the attack potential for each of the relevant Phase 4 tests is equal to the basic attack potential calculated in clause 9.

A.4 Phase 1: Interoperability requirements

This application is not exchanging information with other systems, so interoperability requirements are not applicable.

A.5 Decision criteria for functional tests (Phases 2 and 3)

A.5.1 Phase 2 parameters and passing criteria

A.5.1.1 Overall requirements

With the description of the TOE given, and considering a limitation on the time and cost available for the evaluation, the only test that are applicable are the following:

- T2-1-1: Technology evaluation
- T2-2-1: Check correct behaviour under different SETTINGS
- T2-3-3: Proof-of-life detection

The following subclauses define the specifics for those tests.

By default, the SETTING to be used in all these tests shall be the one defined as SETTING 1 in clause 8.2.2.2.

A.5.1.2 T2-1-1: Technology evaluation

In order to simplify the evaluation in time and cost, the technology evaluation of the product will be substituted by a technology evaluation of the biometric algorithm included in the TOE. For that case, such biometric algorithm should have obtained a FNR (False Negative Rate) equal or lower to 0.5%, for a FPR (False Positive Rate) lower or equal to 1/1 000 000. This data shall have to be obtained in a third-party evaluation.

EXAMPLE At time of publication, the NIST Facial Recognition Vendor Test (FRVT), under the VISABORDER category, is an appropriate example of third-party evaluation.

EDITOR'S NOTE: At meetings with ETSI/ESI it is being considered to get a FPR or 1/100 000. Call for comments on considering this, as to revisit the numbers for FNR in case this is finally applied.

A.5.1.3 T2-2-1: Check correct behaviour under different SETTINGS

Test crew

- Number of bona-fide users: 6
- Each bona-fide user will have 1 official document, allowed by the TOE
- Number of SUBJECTS: 6

Parameters

According to the following parameters, the total number of TRIALS in this test are 120:

- MAX_SETTING_NON_MATCHES = 3
- MAX_TEST_NON_MATCHES = 6
- MAX_SUBJECT_NON_MATCHES = 3
- MAX_TEST_ERRORS = 6
- MAX_SUBJECT_ERRORS = 3
- MAX_SUBJECTS_FAIL = 2
- MAX_ATTEMPTS = 3 (if the TOE allows a lower number of ATTEMPTS, the TOE limit will be the one used)
- MIN_TRIALS = 10
- MIN_SETTINGS = 2
- MIN_SUBJECTS = 6

Passing Criteria

The following table shows the criteria to get a FAIL in the test. If none of those cases are given, the test results with a PASS.

Table A.1 — Decision criteria for T2-2

VARIABLE	OP.	THRESHOLD	VERDICT
----------	-----	-----------	---------

Number of TEST_ERRORS	>	MAX_TEST_ERRORS	FAIL
Number of SUBJECTS_FAIL	>	MAX_SUBJECTS_FAIL	FAIL
Number of TEST_NON_MATCHES	>	MAX_TEST_NON_MATCHES	FAIL
Number of SETTING_NON_MATCHES	>	MAX_SETTING_NON_MATCHES	FAIL

A.5.1.4 T2-3-3: Proof-of-life detection

Test crew

- Number of bona-fide users: 2
- Each bona-fide user will have 1 official document, allowed by the TOE
- Number of SUBJECTS: 2

Parameters

According to the following parameters, the total number of TRIALS in this test are 10:

- MAX_SETTING_NON_MATCHES = Not applicable
- MAX_TEST_NON_MATCHES = Not applicable
- MAX_SUBJECT_NON_MATCHES = Not applicable
- MAX_TEST_MATCHES = 1
- MAX_SUBJECT_MATCHES = 1
- MAX_TEST_ERRORS = Not applicable
- MAX_SUBJECT_ERRORS = Not applicable
- MAX_SUBJECTS_FAIL = 1
- MAX_ATTEMPTS = 3
- MIN_TRIALS = 5
- MIN_SETTINGS = 1
- MIN_SUBJECTS = 2
- TIMEOUT = 20 seconds (unless the TOE's documentation specify a higher value)

Passing Criteria

The following table shows the criteria to get a FAIL in the test. If none of those cases are given, the test results with a PASS.

Table A.2 — Decision criteria for T2-6

VARIABLE	OP.	THRESHOLD	VEREDICT
Number of SUBJECTS_FAIL	>	MAX_SUBJECTS_FAIL	FAIL

Number of TEST_MATCHES	>	MAX_TEST_MATCHES	FAIL

A.5.2 Phase 3 parameters and passing criteria

A.5.2.1 Overall requirements

With the description of the TOE given, and considering a limitation on the time and cost available for the evaluation, the only test that are applicable are the following:

— T3-1-2: Variations of background

The following subclause define the specifics for this test.

By default, the SETTING to be used in all these tests shall be the one defined as SETTING 1 in clause 8.2.2.2.

A.5.2.2 T3-1-2: Variations of background

TBD

A.6 Phase 4 parameters and passing criteria

A.6.1 Overall requirements

For this application profile, most of the test in Phase 4 has common parameters and criteria. Therefore, this subclause is specifying them. Unless something different is declared in an individual Phase 4 test, the following applies.

Applicable tests

The applicable test in Phase 4 for this application profile are:

- T4-1: Zero-effort imposter attack
- T4-3-2: Videos as ARTIFACTS
- T4-3-3: Low-cost masks as ARTIFACTS
- T4-3-4: Advanced masks as ARTIFACTS
- T4-3-5: Make-up based attacks
- T4-3-6: Biometric data injection attacks

They are detailed in following subclauses.

By default, the SETTING to be used in all these tests shall be the one defined as SETTING 1 in clause 8.2.2.2.

Parameters

- MAX_SETTING_MATCHES = 0, i.e., any successful verification will result in a PASS for the test.
- MAX_TEST_MATCHES = 0, i.e., any successful verification will result in a PASS for the test.
- MAX_SUBJECT_MATCHES = 0, i.e., any successful verification will result in a PASS for the test.

- MAX_SUBJECTS_PASS = 0, i.e., any SUBJECT for which a successful verification is found, will result in a PASS for the test.
- MAX_ATTEMPTS = 3
- MIN_TRIALS = 10
- MIN_SETTINGS = 1

Passing Criteria

The following table shows the criteria to get a PASS in the test. If none of those cases are given, the test results with a FAIL.

Table A.3 — Decision criteria for all tests in Phase 4

VARIABLE	OP.	THRESHOLD	VEREDICT
Number of SUBJECTS_PASS	>	MAX_SUBJECTS_PASS	PASS
Number of TEST_MATCHES	>	MAX_TEST_MATCHES	PASS
Number of SETTING_MATCHES	>	MAX_SETTING_MATCHES	PASS

According to the defined parameters, and in few words, it can be said that if a TRIAL results in a MATCH, the TEST will result directly a PASS, so the TOE was proven to be vulnerable.

A.6.2 T4-1: Zero-effort imposter attack

POSTPONED COMMENT (jointly with the one in 9.3):

Comment:

The SUBJECTS to take part in this TEST are:

- A minimum of 2 ID documents, from the bona-fide users involved in the evaluation.
- 2 ATTACKERS, one per bona-fide user
- Therefore, the number of SUBJECTS is 2.

As this is the section about zero-impostor test, this reads as if we are evaluating FMR with 2 subjects, while in A.5.1.2 we are requiring accuracy of FPR of 1/1000000.

This does not seem to add up, unless I missed something

Proposal: Clarify why this would be a relevant test.

Disposition:

Postponed

This test is thought for evaluating the TOE as a whole, in a scenario-based evaluation, not the biometric engine.

The TOE might use a biometric engine with high accuracy, but then using a very relaxed threshold, as to improve convenience.

Test crew

The SUBJECTS to take part in this TEST are:

- A minimum of 2 ID documents, from the bona-fide users involved in the evaluation.
- 2 ATTACKERS, one per bona-fide user
- Therefore, the number of SUBJECTS is 2.

Parameters

In addition to all parameters specified in A.6.1, the following parameters shall be added:

- MIN_SUBJECTS = 2

With all these data the total number of TRIALS to execute, is 20.

Attack potential

Considering the specifications of the criteria for this application profile, the attack potential for this test is changed as follows:

- Knowledge of the product = 0 in identification and 0 in exploitation (unless there is implicit proof-of-life, where it will raise to 2 in identification)
- Access to TOE = 0 in identification and 0 in exploitation
- Access to biometric characteristic = 0 in identification and 0 in exploitation
- Degree of scrutiny = 0 in identification and 0 in exploitation

The total weight will reach 3, which means an attack potential Basic. This will assign an assurance level of NOT AVAILABLE.

A.6.3 T4-3-2: Videos as ARTIFACTS

Test crew

The SUBJECTS to take part in this TEST are:

- 1 ID document for each of the 6 bona-fide users involved in the evaluation.
- 2 ATTACKERS. Each of them will attack to the half of the bona-fide users. The assignment of bona-fide users to attackers is done by the TL under its own criteria.
- Therefore, the number of SUBJECTS is 6, considering each pair "ATTACKER – bona-fide user".

Parameters

In addition to all parameters specified in A.6.1, the following parameters shall be added:

- MIN_SUBJECTS = 6

With all these data the total number of TRIALS to execute, is 60.

Attack potential

Considering the specifications of the criteria for this application profile, the attack potential for this test is changed as follows:

- Knowledge of the product = 0 in identification and 0 in exploitation (unless there is implicit proof-of-life, where it will raise to 2 in identification)
- Access to TOE = 0 in identification and 0 in exploitation
- Access to biometric characteristic = 0 in identification and 0 in exploitation
- Degree of scrutiny = 0 in identification and 0 in exploitation

Therefore, for the worst-case attack context, the total weight will reach 15, which means an attack potential Basic. This will assign an assurance level of AVA_VAN.1.

A.6.4 T4-3-3: Low-cost masks as ARTIFACTS**Test crew**

The SUBJECTS to take part in this TEST are:

- 1 ID document for 4 bona-fide users involved in the evaluation.
- 2 ATTACKERS. Each of them will attack to the half of the bona-fide users. The assignment of bona-fide users to attackers is done by the TL under its own criteria.
- 2 artifacts for each of the bona-fide users, according to the masks described in 9.5.3.2
- Therefore, the number of SUBJECTS is 8, considering each pair "ATTACKER – bona-fide user – artifact".

Parameters

In addition to all parameters specified in A.6.1, the following parameters shall be added:

- MIN_SUBJECTS = 8

With all these data, the total number of TRIALS to execute is 80.

Attack potential

Considering the specifications of the criteria for this application profile, the attack potential for this test is changed as follows:

- Knowledge of the product = 0 in identification and 0 in exploitation (unless there is implicit proof-of-life, where it will raise to 2 in identification)
- Access to TOE = 0 in identification and 0 in exploitation
- Access to biometric characteristic = 0 in identification and 0 in exploitation
- Degree of scrutiny = 0 in identification and 0 in exploitation

Therefore, for the worst-case attack context, the total weight will reach 5, which means an attack potential Basic. This will assign an assurance level of NOT AVAILABLE.

A.6.5 T4-3-4: Advanced masks as ARTIFACTS

Test crew

The SUBJECTS to take part in this TEST are:

- 1 ID document for 2 bona-fide users involved in the evaluation.
- 2 ATTACKERS. Each of them will attack one of the bona-fide users. The assignment of bona-fide users to attackers is done by the TL under its own criteria.
- If for any of the bona-fide users, more than one artifact (i.e., mask) is prepared, then it will be considered as an additional SUBJECT.
- Therefore, the number of SUBJECTS is 2, considering each pair "ATTACKER – bona-fide user – artifact".

Parameters

In addition to all parameters specified in A.6.1, the following parameters shall be added:

- MIN_SUBJECTS = 2

With all these data, the total number of TRIALS to execute is 20.

Attack potential

Considering the specifications of the criteria for this application profile, the attack potential for this test is changed as follows:

- Knowledge of the product = 0 in identification and 0 in exploitation (unless there is implicit proof-of-life, where it will raise to 2 in identification)
- Access to TOE = 0 in identification and 0 in exploitation
- Access to biometric characteristic = 0 in identification and 0 in exploitation
- Degree of scrutiny = 0 in identification and 0 in exploitation

The total weight will reach 21, which means an attack potential Basic. This will assign an assurance level of AVA_VAN.2.

A.6.6 T4-3-5: Make-up based attacks

Test crew

The SUBJECTS to take part in this TEST are:

- 1 ID document for 3 bona-fide users involved in the evaluation.
- 1 or several ATTACKERS, depending whether it is possible to fulfil the following requirements:
 - A score of BONAFIDE_SIM_TH or lower has to be reached between the bona-fide user and the ATTACKER with the make-up applied. REF_APP will be used to get such score.
 - A score of ATTACKER_SIM_TH or higher has to be reached between the bona-fide user, and the ATTACKER without any make-up. REF_APP will be used to get such score.
- Each bona-fide user shall be attacked by an ATTACKER.
- Therefore, the number of SUBJECTS is 3, considering each pair "ATTACKER – bona-fide use".

Parameters

In addition to all parameters specified in A.6.1, the following parameters shall be added:

- MIN_SUBJECTS = 3

With all these data, the total number of TRIALS to execute is 30.

Attack potential

Considering the specifications of the criteria for this application profile, the attack potential for this test is changed as follows:

- Knowledge of the product = 0 in identification and 0 in exploitation (unless there is implicit proof-of-life, where it will raise to 2 in identification)
- Access to TOE = 0 in identification and 0 in exploitation
- Access to biometric characteristic = 0 in identification and 0 in exploitation
- Degree of scrutiny = 0 in identification and 0 in exploitation

Therefore, for the worst-case attack context, the total weight will reach 20, which means an attack potential Basic. This will assign an assurance level of AVA_VAN.2.

A.6.7 T4-3-6: Biometric data injection attacks

Test crew

The SUBJECTS to take part in this TEST are:

- Images/videos of, at least, 4 bona-fide users, according to the training needs of the system used for generating the models and the deepfake videos.
- 1 ID document for each of the bona-fide users involved in the test.
- 1 or 2 ATTACKERS, depending on the availability and easiness to impersonate the bona-fide users. The decision will be taken by the TL, following justified (and documented) criteria. Each ATTACKER can attack one or several bona-fide users.
- Therefore, the number of SUBJECTS is 4, considering each bona-fide user attacked.

Parameters

In addition to all parameters specified in A.6.1, the following parameters shall be added:

- MIN_SUBJECTS = 4

With all these data, the total number of TRIALS to execute is 40.

Attack potential

The attack potential for this test is calculated according to CEN TS XXXX on "Digital Injection Attacks".

A.7 Overall assessment criteria

For a product applying for this application profile, a PASS will only be given if all applicable Phase 2 and Phase 3 tests result in PASS, and all Phase 4 tests result in FAIL.

Annex B **(normative)2216**

Profile 2: Face recognition for the on-boarding of credentials in and Identity Digital Wallet (eIDAS)

EDITOR'S NOTE: This will be defined according to the outcomes of the EU Expert Group on the revision of eIDAS, and the definition of the Toolbox, as well as the works in CEN TC224 WG20.

B.1 Introduction

TBD

This application profile can be taken by any certification body, government and/or sector, to define and evaluate the requirements for their biometric products. This may be used in coordination with other current National initiatives. Governments may decide to give a higher preference to other National specifications.

B.2 TOE description

TBD

B.3 Levels of assurance

TBD

The LoA for this application profile shall be “High” with an attack potential of “high” according to ISO/IEC 19989-1.

B.4 Phase 1: Interoperability requirements

TBD

B.5 Decision criteria for functional tests (Phases 1 and 2)

B.5.1 Phase 2 parameters and passing criteria

B.5.1.1 Overall requirements

TBD

B.5.1.2 T2.x

TBD

EDITOR'S NOTE: As many of these sections as TESTs to be required.

Test crew

TBD

Parameters

TBD

Passing Criteria

TBD

B.5.2 Phase 3 parameters and passing criteria

TBD

B.5.2.1 Overall requirements

TBD

B.5.2.2 T3.x

TBD

EDITOR'S NOTE: As many of these sections as TESTs to be required.

Test crew

TBD

Parameters

TBD

Passing Criteria

TBD

B.6 Phase 4: Decision criteria for security requirements

TBD

B.6.1 Overall requirements

TBD

B.6.2 T4.x

TBD

EDITOR'S NOTE: As many of these sections as TESTs to be required.

Test crew

TBD

Parameters

TBD

Passing Criteria

TBD

B.7 Requirements for the overall decision

TBD

Annex C **(normative)3227**

Profile 3: Face recognition for the use of Identity Digital Wallet (eIDAS)

EDITOR'S NOTE: This will be defined according to the outcomes of the EU Expert Group on the revision of eIDAS, and the definition of the Toolbox

C.1 Introduction

TBD

This application profile can be taken by any certification body, government and/or sector, to define and evaluate the requirements for their biometric products. This may be used in coordination with other current National initiatives. Governments may decide to give a higher preference to other National specifications.

C.2 TOE description

TBD

C.3 Levels of assurance

TBD

C.4 Phase 1: Interoperability requirements

TBD

C.5 Decision criteria for functional tests (Phases 1 and 2)

C.5.1 Phase 2 parameters and passing criteria

C.5.1.1 Overall requirements

TBD

C.5.1.2 T2.x

TBD

EDITOR'S NOTE: As many of these sections as TESTs to be required.

Test crew

TBD

Parameters

TBD

Passing Criteria

TBD

C.5.2 Phase 3 parameters and passing criteria

TBD

C.5.2.1 Overall requirements

TBD

C.5.2.2 T3.x

TBD

EDITOR'S NOTE: As many of these sections as TESTs to be required.

Test crew

TBD

Parameters

TBD

Passing Criteria

TBD

C.6 Phase 4: Decision criteria for security requirements

TBD

C.6.1 Overall requirements

TBD

C.6.2 T4.x

TBD

EDITOR'S NOTE: As many of these sections as TESTs to be required.

prEN XXXX:XXXX (E) (ERBP-5 WD7)

Test crew

TBD

Parameters

TBD

Passing Criteria

TBD

C.7 Requirements for the overall decision

TBD

Annex D (normative) 4238

Profile 4: Face biometrics under constrained and supervised recognition systems / Face recognition for Automated Border Control - eGates

EDITOR'S NOTES:

An example of this kind of system are the ABC systems

The current title was drafted as to provide an application-agnostic title, just in the case that this application profile can be applied to any other application (e.g. access to stadiums). But it is true that the title proposed by Kevin is much clearer.

We may discuss about the title once the application profile is finished to really consider if other applications are relevant.

Another AP could be "biometrics on mobile devices" but that can create a collision with BIO-iTC. We should talk to them first for this.

Check also BSI work:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03166/TR-03166_node.html

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03166/BSI-TR-03166.pdf?__blob=publicationFile&v=4

Don't really know if using the term "ABC eGate" is redundant.

D.1 Introduction

This Annex describes the application profile of an ABC eGate that uses facial recognition for verifying the identity of a citizen against the photograph of its electronic passport.

This application profile is only targeting the biometric part of the ABC eGate, i.e. the face recognition algorithm and the Presentation Attack Detection system, and don't take into account any other usability or security aspect.

As it is detailed, this application enforces certain tests, while dismiss others due to the non-applicability/non-viability in this context.

This application profile can be taken by any certification body, government and/or sector, to define and evaluate the requirements for their biometric products. This may be used in coordination with other current National initiatives. Governments may decide to give a higher preference to other National specifications.

D.2 TOE description

The TOE of this application profile is the face recognition component of the ABC eGate. It concerns:

- The capture device of the ABC eGate and its lighting components
- The Presentation Attack Detection system
- The Face recognition algorithm and the quality analysis modules.

The following figure summarizes the context of the TOE.

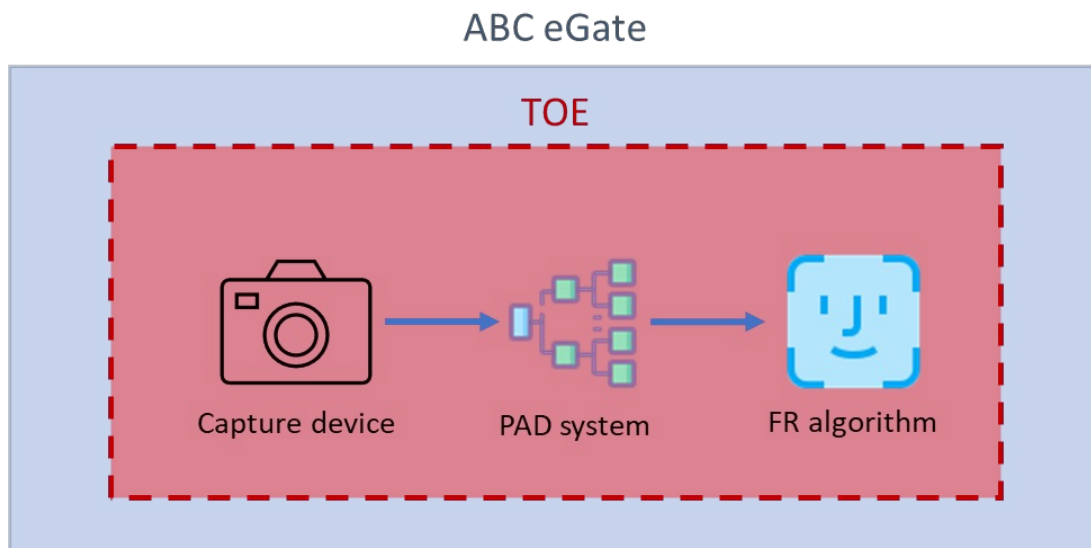


Figure 1: TOE's Block Diagram

Important details from the TOE to highlight are:

- The TOE only concerns the biometric component of the ABC eGate..
- Capture device:
 - The considered capture device for the evaluation is the camera integrated in the eGate
 - The associated lighting components around the camera are taken into account in the TOE
- Environment:
 - The normal lighting environment shall be described in the security target document (in lux)
 - The distance of capture of the user's face shall be described in the security target document (in cm)
 - The TOE is installed in a supervised environment and under restricted conditions

D.3 Levels of assurance

EDITOR'S NOTE: I think that this kind of system shall always be LoA "High", due to the National Security importance. Furthermore, when a LoA "Substantial" might be just AVA-VAN.1, as indicated in the Implementation Act of EUCC. As a comment aside, due to the fact the the EUCC considers that anything is Basic (there is not a security requirement for them), it is not possible to define more than 2 levels of security

Only two possible evaluation levels of assurance are defined for this application profile:

Evaluation levels of assurance	Knowledge of the TOE	Time elapsed to perform the evaluation
Substantial	Target of security	25 days
High	At least the target of security.	30 days.

Table D.24 Evaluation levels of assurance

This application profile is defined under the condition of LoA “High”, as specified in part 1 of this family of standards.

For the calculation of the attack level of each of the tests defined for Phase 4, the following intervals excel the minimum ones defined in each of the Tests:

- Knowledge of the product: This product is used by the general public, but designed and deployed by experts. Therefore, this criterion shall be “Restricted information” for the identification phase, and “Public information” for the exploitation phase.
- Access to TOE: The TOE is designed, developed and deployed in restricted environments. Even using the TOE in order to exploit the attack is done at a very specific moments, and with only a couple of attempts allowed each time the attacker crosses a border. Therefore, this criterion shall be “Difficult” at the Identification phase, and “Moderate” during the Exploitation phase.
- Access to biometric characteristic: The biometric characteristic is an image (or video) of the face, which is extremely easy to acquire. But the biometric reference is either stored in a ePassport or ID card with contactless communication, or in an internal database with very restricted access (e.g., a black list of potential travellers). Under these conditions, the interval during identification shall be “Easy”, but during the exploitation shall be “Moderate”.
- Degree of scrutiny: The TOE is installed in a supervised environment, so in all phases the interval shall be “Overseen”.

D.4 Phase 1: Interoperability requirements

This application profile shall read information from a Machine Readable Travel Document (MRTD). Therefore, the applicable tests are:

EDITOR’S NOTE: Names for each of the tests have to be added to the numbers. Also the numbers shall be with hyphens (e.g., T1-1-1-1, instead of T1.1.1.1)

- T1.1.1.1
- T1.1.1.2
- T1.1.1.3
- T1.1.1.4

- T1.1.1.5
- T1.1.1.6
- T1.1.1.7

Also, the TOE shall be able to detect bad user presentations, so the following tests are also applicable:

- T1.1.2.1
- T1.1.2.2

D.5 Decision criteria for functional tests (Phases 1 and 2)

D.5.1 Phase 2 parameters and passing criteria

D.5.1.1 Overall requirements

With the description of the TOE given, and considering a limitation on the time and cost available for the evaluation, the only test that are applicable are the following:

- T2-1-1: Technology evaluation
- T2-3-2: Differentiation among twins
- T2-3-3: Proof-of-life detection

It is important to note that the deployment may fix the SETTING, including the background and lighting, and there is no possibility to have different capture devices. Therefore, tests T2-2-1 and T2-2-2 are not applicable.

Also, the reference data shall come from a MRTD following ICAO rules and read using electronic means, so, there is no variation of reference data (i.e., T2-3-1 is not applicable).

The following subclauses define the specifics for those tests.

By default, the SETTING to be used is a scenario where the SUBJECT is in front of the ABC eGate camera, at a distance of 70cm and a lighting environment in the range of 300lux and 1000lux. If the TOE's user guide defines other usage conditions, these ones shall be taken as SETTING.

D.5.1.2 T2-1-1: Technology evaluation

In order to simplify the evaluation in time and cost, the technology evaluation of the product will be substituted by a technology evaluation of the biometric algorithm included in the TOE. For that case, such biometric algorithm should have obtained a FNR (False Negative Rate) equal or lower to 0.5%, for a FPR (False Positive Rate) lower or equal to 1/100 000. This data shall have to be obtained in a third-party evaluation.

D.5.1.3 T2-3-2: Differentiation among twins

TBD

D.5.1.4 T2-3-3: Proof-of-life detection

Test crew

- Number of bona-fide users: 20

- Each bona-fide user will have 1 official document allowed by the TOE
- Number of SUBJECTS: 20

Parameters

According to the following parameters, the total number of TRIALS in this test are 200:

- MAX_SETTING_NON_MATCHES = 10
- MAX_TEST_NON_MATCHES = 10
- MAX_SUBJECT_NON_MATCHES = Not applicable
- MAX_TEST_MATCHES = 1
- MAX_SUBJECT_MATCHES = 1
- MAX_TEST_ERRORS = Not applicable
- MAX_SUBJECT_ERRORS = 3
- MAX_SUBJECTS_FAIL = 5
- MAX_ATTEMPTS = 1
- MIN_TRIALS = 10
- MIN_SETTINGS = 1
- MIN_SUBJECTS = 20
- TIMEOUT = 20 seconds (unless the TOE's documentation specify a higher value)

Passing Criteria

The following table shows the criteria to get a FAIL in the test. If none of those cases are given, the test results with a PASS.

Table D.25 - Decision criteria for T2-2

VARIABLE	OP.	THRESHOLD	VERDICT
Number of TEST_ERRORS	>	MAX_TEST_ERRORS	FAIL
Number of SUBJECTS_FAIL	>	MAX_SUBJECT_FAIL	FAIL
Number of TEST_NON_MATCHES	>	MAX_TEST_NON_MATCHES	FAIL
Number of SETTING_NON_MATCHES	>	MAX_SETTING_NON_MATCHES	FAIL

D.5.2 Phase 3 parameters and passing criteria

D.5.2.1 Overall requirements

With the description of the TOE given, and considering a limitation on the time and cost available for the evaluation, the only test that are applicable are the following:

- T3-1-1: Variations of lighting conditions

The following subclauses define the specifics for those tests.

Three SETTINGS shall be considered for this test:

- SETTING 1: Light coming from behind the camera with a lighting of around 300 lux (measure is done for the light coming from the camera at the SUBJECT position).
- SETTING 2: Light coming from behind the camera with a lighting of around 900 lux (measure is done for the light coming from the camera at the SUBJECT position).
- SETTING 3: Light coming from behind the camera AND from one side (left or right) with a lighting of around 300 lux (measure is done for the light coming from the camera at the SUBJECT position).

By default, the distance between the SUBJECT and the camera will be fixed at 70cm. If the TOE's user guide defines another distance, the TOE's user guide distance shall be used.

In addition, the following tests are applicable:

- T3-2-1: Variations in facial expressions
- T3-2-2: Variation in face orientation towards the TOE
- T3-2-3: Significant SUBJECT esthetical variations

D.5.3 T3-1-1: Variations of lighting conditions

Test crew

- Number of bona-fide users: 5
- Each bona-fide user will have 1 official document allowed by the TOE
- Number of SUBJECTS: 5

Parameters

- MAX_SETTING_NON_MATCHES = 10
- MAX_TEST_NON_MATCHES = 10
- MAX_SUBJECT_NON_MATCHES = Not applicable
- MAX_TEST_MATCHES = 1
- MAX_SUBJECT_MATCHES = 1
- MAX_TEST_ERRORS = Not applicable
- MAX_SUBJECT_ERRORS = 1
- MAX_SUBJECTS_FAIL = 1
- MAX_ATTEMPTS = 1
- MIN_TRIALS = 10
- MIN_SETTINGS = 3
- MIN_SUBJECTS = 5
- TIMEOUT = 20 seconds (unless the TOE's documentation specify a higher value)

Passing Criteria

Table D.26 - Decision criteria for T3-1-1

VARIABLE	OP.	THRESHOLD	VEREDICT
Number of TEST_ERRORS	>	MAX_TEST_ERRORS	FAIL
Number of SUBJECTS_FAIL	>	MAX_SUBJECT_FAIL	FAIL
Number of TEST_NON_MATCHES	>	MAX_TEST_NON_MATCHES	FAIL
Number of SETTING_NON_MATCHES	>	MAX_SETTING_NON_MATCHES	FAIL

D.5.3.1 T3-2-1: Variations in facial expressions

TBD

D.5.3.2 T3-2-2: Variations in face orientation towards the TOE

TBD

D.5.3.3 T3-2-3: Significant SUBJECT esthetical variations

TBD

D.6 Phase 4: Decision criteria for security requirements

D.6.1 Overall requirements

With the description of the TOE given, and considering a limitation on the time and cost available for the evaluation, the only test that are applicable are the following:

- T4-1: Zero-effort imposter attack
- T4-2-2: Use of morphing techniques during enrolment
- T4-3-4: Advanced masks as ARTIFACTS
- T4-3-5: Make-up based attacks

It is important to note that, as this is a supervised system, it is considered not practical to have attacks that may lead to a significant misbehaviour of the attacker. Therefore, presenting a still image (T4-3-1), a video (T4-3-2) or wearing a low-quality mask (T4-3-3) are not applicable. And it is not practical to consider a digital injection attack (i.e., T4-3-6).

KEVIN'S NOTE: it might be possible to execute those attacks if surveillance is not so strong. So it is worth to perform T-3-1 2 and 3.

The following subclauses define the specifics for those tests.

By default, the SETTING to be used is a scenario where the SUBJECT is in front of the ABC eGate camera, at a distance of 70cm and a lighting environment in the range of 300lux and 1000lux. If the TOE's user guide defines other usage conditions, these ones shall be taken as SETTING.

Parameters

- MAX_SETTING_MATCHES = 0, i.e. any successful verification will result in a PASS for the test.
- MAX_TEST_MATCHES = 0, i.e. any successful verification will result in a PASS for the test.
- MAX_SUBJECT_MATCHES = 0, i.e. any successful verification will result in a PASS for the test.
- MAX_SUBJECTS_PASS = 0, i.e. any SUBJECT for which a successful verification is found will result in a PASS for the test.
- MAX_SUBJECT_MATCHES = 1
- MAX_TEST_ERRORS = Not applicable
- MAX_ATTEMPTS = 3
- MIN_TRIALS = 10
- MIN_SETTINGS = 1
- TIMEOUT = 20 seconds (unless the TOE's documentation specify a higher value)

Passing Criteria

The following table shows the criteria to get a PASS in the test. If none of those cases are given, the test results with a FAIL.

Table D.27 - Decision criteria for all tests in Phase 4

VARIABLE	OP.	THRESHOLD	VEREDICT
Number of SUBJECT_PASS	>	MAX_SUBJECTS_PASS	FAIL
Number of TEST_MATCHES	>	MAX_TEST_MATCHES	FAIL
Number of SETTING_MATCHES	>	MAX_SETTING_MATCHES	FAIL

According to the defined parameters, and in few words, it can be said that if a TRIAL results in a MATCH, the TEST will result directly a FAIL, so the TOE was proven to be vulnerable.

D.6.2 T4-1: Zero-effort imposter attack

Test crew

The SUBJECTS to take part in this TEST are:

- A minimum of 2 ID documents, from the bona-fide users involved in the evaluation.
- 2 ATTACKERS, one per bona-fide user
- Therefore, the number of SUBJECTS is 2.

Parameters

In addition to all parameters specified in D.6.1, the following parameters shall be added:

- MIN_SUBJECTS = 2

With all these data the total number of TRIALS to execute, is 20.

Attack potential

Considering the specifications of the criteria for this application profile, the attack potential for this test is changed as follows:

- Knowledge of the product = 2 in identification and 0 in exploitation (+2)
- Access to TOE = 4 in identification and 2 in exploitation (+6)
- Access to biometric characteristic = 0 in identification and 4 in exploitation (+4)
- Degree of scrutiny = 2 in identification and 3 in exploitation (+5)

The total weight will reach 20, which means an attack potential Enhanced Basic. This will assign an assurance level of AVA_VAN.2.

D.6.3 T4-2-2: Use of morphing techniques during enrolment

TBD

D.6.4 T4-3-1: Still images as ARTIFACTS

Test crew

- The number of SUBJECTS is 10
- No need to have real ID documents. The TOE shall provide a mean to import ID portrait images of the targeted SUBJECT in order to perform the face recognition process.
- The goal is to vary the printed support between each SUBJECT (e.g., color of paper, type of support, image in B&W, etc.)

Parameters

In addition to all parameters specified in D.6.1, the following parameters shall be added:

- MIN_SUBJECTS = 10
- Realisation of half static attacks (PAI are presented statically in front of the camera) and half dynamic attacks (PAI are presented with light movements – vertically, horizontally or rotation with small angles) during the TRIALS

With all these data the total number of TRIALS to execute, is 100

Attack potential

Considering the specifications of the criteria for this application profile, the attack potential for this test is changed as follows:

- Knowledge of the product = 2 in identification and 0 in exploitation
- Access to TOE = 4 in identification and 2 in exploitation
- Access to biometric characteristic = 0 in identification and 4 in exploitation

- Degree of scrutiny = 2 in identification and 3 in exploitation

The total weight will reach 17, which means an attack potential Basic. This will assign an assurance level of AVA_VAN.1.

D.6.5 T4-3-2: Videos as ARTIFACTS

Test crew

- The number of SUBJECTS is 6
- No need to have real ID documents. The TOE shall provide a mean to import ID portrait images of the targeted SUBJECT in order to perform the face recognition process.
- The goal is to vary the support for display between each SUBJECT (e.g., type of screen, screen with filters, etc.)

Parameters

In addition to all parameters specified in D.6.1, the following parameters shall be added:

- MIN_SUBJECTS = 6
- Realisation of half static attacks (PAI are presented statically in front of the camera) and half dynamic attacks (PAI are presented with light movements – vertically, horizontally or rotation with small angles) during the TRIALS

With all these data the total number of TRIALS to execute, is 60

Attack potential

The use of a large TV is not viable in this attack, so only the “portable device and regular video” attack is applicable. Considering the specifications of the criteria for this application profile, the attack potential for this test is changed as follows:

- Knowledge of the product = 2 in identification and 0 in exploitation (+2)
- Access to TOE = 4 in identification and 2 in exploitation (+6)
- Access to biometric characteristic = 0 in identification and 4 in exploitation (+4)
- Degree of scrutiny = 2 in identification and 3 in exploitation (+2)

The total weight will reach 18, which means an attack potential Basic. This will assign an assurance level of AVA_VAN.1.

D.6.6 T4-3-3: Low-cost masks as ARTIFACTS

Test crew

- The number of SUBJECTS is 30
- No need to have real ID documents. The TOE shall provide a mean to import ID portrait images of the targeted SUBJECT in order to perform the face recognition process.
- The masks used shall include at least (each mask is considered as a SUBJECT):
 - Curved paper masks

- Fantasy masks
- Head dummy (in silicone, polystyrene, etc.)
- 3D printed masks



Figure D.9 - Examples of two paper masks (left) and three fantasy masks (right)



Figure D.10 - Examples of four head dummies (left) and one 3D printed mask (right)

Parameters

In addition to all parameters specified in D.6.1, the following parameters shall be added:

- MIN_SUBJECTS = 30
- Realisation of half static attacks (PAI are presented statically in front of the camera) and half dynamic attacks (PAI are presented with light movements – vertically, horizontally or rotation with small angles) during the TRIALS

With all these data the total number of TRIALS to execute, is 300.

Attack potential

Considering the specifications of the criteria for this application profile, the attack potential for this test is changed as follows:

- Knowledge of the product = 2 in identification and 0 in exploitation (+2)
- Access to TOE = 4 in identification and 2 in exploitation (+6)
- Access to biometric characteristic = 0 in identification and 4 in exploitation (+4)
- Degree of scrutiny = 2 in identification and 3 in exploitation (+2)

The total weight will reach 22, which means an attack potential Enhanced Basic. This will assign an assurance level of AVA_VAN.2.

D.6.7 T4-3-4: Advanced masks as ARTIFACTS

Test crew

- The number of SUBJECTS is 20
- No need to have real ID documents. The TOE shall provide a mean to import ID portrait images of the targeted SUBJECT in order to perform the face recognition process.
- The masks used shall include at least (each mask is considered as a SUBJECT):
 - 3D rigid mask
 - Latex mask
 - High quality latex mask (price over 300€) – except for evaluation at substantial level
 - Silicone mask – except for evaluation at substantial level



Figure D.11 - Exemples of two 3D rigid mask attacks (left) and two latex mask attacks (right)



Figure D.12 - Exemples of one high quality latex mask attack (left) and three silicone mask attacks (right)

Parameters

In addition to all parameters specified in D.6.1, the following parameters shall be added:

- MIN_SUBJECTS = 20
- Realisation of half static attacks (PAI are presented statically in front of the camera) and half dynamic attacks (PAI are presented with light movements – vertically, horizontally or rotation with small angles) during the TRIALS

With all these data the total number of TRIALS to execute, is 200.

Evaluation Level of Assurance

- Evaluation at substantial level: High quality latex mask and silicone mask are not covered for this level of evaluation
- Evaluation at high level: all masks are covered for this level of evaluation.

Attack potential

Considering the specifications of the criteria for this application profile, the attack potential for this test is changed as follows:

- Knowledge of the product = 2 in identification and 0 in exploitation (+2)
- Access to TOE = 4 in identification and 2 in exploitation (+6)
- Access to biometric characteristic = 0 in identification and 4 in exploitation (+4)
- Degree of scrutiny = 2 in identification and 3 in exploitation (+5)

The total weight will reach 37, which means an attack potential Moderate. This will assign an assurance level of AVA_VAN.3.

D.6.8 T4-3-5: Make-up-based attacks

TBD

D.7 Requirements for the overall decision

For a product applying for this application profile, a PASS will only be given if all applicable Phase 2, Phase 3 and Phase 4 tests result in PASS.

Annex E (normative) 52813

Profile 5: Presentation Attack Detection systems

E.1 Introduction

This Annex describes the application profile for Presentation Attack Detection (PAD) systems using face biometric characteristic.

This application profile is only targeting the automated detection systems for presentation attacks targeting a facial recognition system.

This application profile can be applied for two using modes of PAD systems:

- PAD subsystem mode: A PAD subsystem is a hardware and/or software that implements a PAD mechanism and makes an explicit declaration regarding the detection of presentation attacks [1]. **In PAD subsystem mode, the decision to be considered by the evaluator (if the presentation is classified as an attack or a genuine transaction) is the decision from the PAD subsystem.**
- Full system mode: A full system adds biometric comparison to the PAD, comprising a full end-to-end system [1]. **In Full-system mode, the decision to be considered by the evaluator (if the presentation is classified as an attack or a genuine transaction) is the global decision, i.e. the combination of the decisions taken by the PAD subsystem and the facial recognition system.**

The mode of the evaluation shall appear in the evaluation's report and in the certificate's name (if applicable).

The requirements described in this application profile will depend on the evaluation mode and on the different Levels of Assurance (LoA).

As it is detailed, this application enforces certain tests, while dismiss others due to the non-applicability/non-viability in this context.

This application profile can be taken by any certification body, government and/or sector, to define and evaluate the requirements for their biometric products. This may be used in coordination with other current National initiatives. Governments may decide to give a higher preference to other National specifications.

E.2 TOE description

The TOE of this application profile corresponds to all components involved in the detection of a presentation attack. It concerns:

- The capture device and its lighting components (if there are lighting components)
- The Presentation Attack Detection system
- The Facial recognition algorithm (for Full-system mode only)

The scope of the Annex E is highlighted in Figure 1 which summarizes the possible attack paths on a biometric system, as demonstrated in [2].

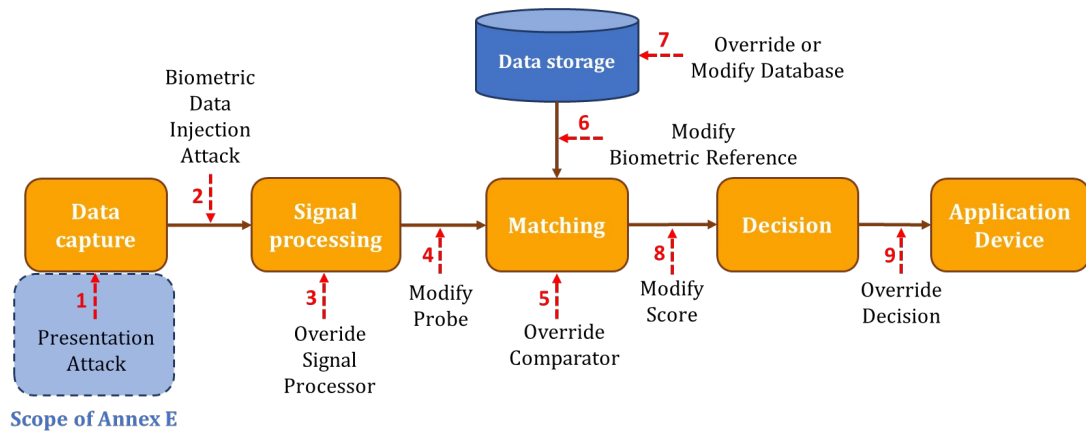


Figure E.14 Possible attack paths on a biometric system

E.3 Levels of assurance

Here are the evaluation levels of assurance defined for this application profile:

Evaluation Levels of Assurance	Knowledge of the TOE	Time elapsed to perform the evaluation
Basic	User guide	5 days
Substantial	Target of security	25 days
High	At least the target of security.	At least 30 days.

Table E.29 Evaluation levels of assurance

E.4 Phase 1: Interoperability requirements

This application is not exchanging information with other systems (the PAD system only shares a Boolean result to the facial recognition system), so interoperability requirements are not applicable.

E.5 Decision criteria for functional tests (Phases 1 and 2)

E.5.1 Phase 2 parameters and passing criteria

E.5.1.1 Overall requirements

With the description of the TOE given, and considering a limitation on the time and cost available for the evaluation, the only test that are applicable are the following:

- T2-1-1 - **only for “Full-system” mode evaluations**
- T2-2-2 (if applicable) – **only for LoA Substantial and High**

The following subclauses define the specifics for those tests.

By default, the SETTING to be used is a scenario where the SUBJECT is in front of a camera, at a distance of around 50cm. If the TOE’s user guide defines other usage conditions, these ones shall be taken as SETTING.

E.5.1.2 T2.1.1

This requirement is only applicable for evaluation in “Full-system” mode (see clause E.1).

In order to simplify the evaluation in time and cost, the technology evaluation of the product will be substituted by a technology evaluation of the biometric algorithm included in the TOE. For that case, such biometric algorithm should have obtained a FNR (False Negative Rate) equal or lower to 5%, for a FPR (False Positive Rate) lower or equal to 1/100 000. This data shall have to be obtained in a third-party evaluation.

E.5.1.3 T2.2.2

This requirement is only applicable for evaluation at LoA “Substantial” and “High” (see Table E.1).

Test crew

- Number of bona-fide users: 5
- Number of SUBJECTS: 5
- Number of different capture devices to be tested: 4 (will be considered as 4 different SETTINGS)

Parameters

According to the following parameters, the total number of TRIALS in this test are 100:

- MAX_SETTING_NON_MATCHES = 5
- MAX_SUBJECT_NON_MATCHES = 5
- MAX_TEST_NON_MATCHES = 15
- MAX_TEST_ERRORS = 15
- MAX_SUBJECTS_FAIL = 1
- MAX_ATTEMPTS = 1
- MIN_TRIALS = 5
- MIN_SETTINGS = 4
- MIN_SUBJECTS = 5
- TIMEOUT = 20 seconds (unless the TOE's documentation specify a higher value)

Passing Criteria

The following table shows the criteria to get a FAIL in the test. If none of those cases are given, the test results with a PASS.

Table E.30 - Decision criteria for T2-2-2

VARIABLE	OP.	THRESHOLD	VEREDICT
Number of TEST_ERRORS	>	MAX_TEST_ERRORS	FAIL
Number of TEST_NON_MATCHES	>	MAX_TEST_NON_MATCHES	FAIL
Number of SUBJECT_NON_MATCHES	>	MAX_SUBJECT_NON_MATCHES	FAIL
Number of SETTING_NON_MATCHES	>	MAX_SETTING_NON_MATCHES	FAIL

E.5.2 Phase 3 parameters and passing criteria

E.5.2.1 Overall requirements

With the description of the TOE given, and considering a limitation on the time and cost available for the evaluation, the only test that are applicable are the following:

- T3-1-1
- T3-1-2 – **only for LoA Substantial and High**

The following subclauses define the specifics for those tests.

E.5.3 T3.1.1

Test crew

- Number of bona-fide users: 5
- Number of SUBJECTS: 5
- Number of different lighting conditions to be tested: 4 (will be considered as 4 different SETTINGS). The 4 different lighting conditions shall be measured in lux.

Parameters

According to the following parameters, the total number of TRIALS in this test are 100:

- MAX_SETTING_NON_MATCHES = 5
- MAX_SUBJECT_NON_MATCHES = 5
- MAX_TEST_NON_MATCHES = 15
- MAX_TEST_ERRORS = 15
- MAX_SUBJECTS_FAIL = 1
- MAX_ATTEMPTS = 1
- MIN_TRIALS = 5
- MIN_SETTINGS = 4
- MIN_SUBJECTS = 5

- TIMEOUT = 20 seconds (unless the TOE's documentation specify a higher value)

Passing Criteria

The following table shows the criteria to get a FAIL in the test. If none of those cases are given, the test results with a PASS.

Table E.31 - Decision criteria for T3-1-1

VARIABLE	OP.	THRESHOLD	VEREDICT
Number of TEST_ERRORS	>	MAX_TEST_ERRORS	FAIL
Number of TEST_NON_MATCHES	>	MAX_TEST_NON_MATCHES	FAIL
Number of SUBJECT_NON_MATCHES	>	MAX_SUBJECT_NON_MATCHES	FAIL
Number of SETTING_NON_MATCHES	>	MAX_SETTING_NON_MATCHES	FAIL

E.5.4 T3.1.2

This requirement is only applicable for evaluation at LoA “Substantial” and “High” (see Table E.1).

Test crew

- Number of bona-fide users: 2
- Number of SUBJECTS: 2
- Number of different backgrounds to be tested: 3 (will be considered as 3 different SETTINGS). At least 1 background shall be a dynamic background.

Parameters

According to the following parameters, the total number of TRIALS in this test are 30:

- MAX_SETTING_NON_MATCHES = 3
- MAX_SUBJECT_NON_MATCHES = 3
- MAX_TEST_NON_MATCHES = 5
- MAX_TEST_ERRORS = 5
- MAX_SUBJECTS_FAIL = 1
- MAX_ATTEMPTS = 1
- MIN_TRIALS = 5
- MIN_SETTINGS = 3
- MIN_SUBJECTS = 5
- TIMEOUT = 20 seconds (unless the TOE's documentation specify a higher value)

Passing Criteria

The following table shows the criteria to get a FAIL in the test. If none of those cases are given, the test results with a PASS.

Table E.32 - Decision criteria for T3-1-2

VARIABLE	OP.	THRESHOLD	VERDICT
Number of TEST_ERRORS	>	MAX_TEST_ERRORS	FAIL
Number of TEST_NON_MATCHES	>	MAX_TEST_NON_MATCHES	FAIL
Number of SUBJECT_NON_MATCHES	>	MAX_SUBJECT_NON_MATCHES	FAIL
Number of SETTING_NON_MATCHES	>	MAX_SETTING_NON_MATCHES	FAIL

E.6 Phase 4: Decision criteria for security requirements

E.6.1 Overall requirements

With the description of the TOE given, and considering a limitation on the time and cost available for the evaluation, the only test that are applicable are the following:

- T4-1 - **only for “Full-system” mode evaluations**
- T4-3-1
- T4-3-2
- T4-3-3
- T4-3-4 - **only for LoA Substantial and High**

The following subclauses define the specifics for those tests.

Parameters

- MAX_SETTING_MATCHES = 0, i.e. any successful verification will result in a PASS for the test.
- MAX_TEST_MATCHES = 0, i.e. any successful verification will result in a PASS for the test.
- MAX_SUBJECT_MATCHES = 0, i.e. any successful verification will result in a PASS for the test.
- MAX_SUBJECTS_PASS = 0, i.e. any SUBJECT for which a successful verification is found will result in a PASS for the test.
- MAX_SUBJECT_MATCHES = 1
- MAX_TEST_ERRORS = Not applicable
- MAX_ATTEMPTS = 3
- MIN_TRIALS = 10
- MIN_SETTINGS = 1
- TIMEOUT = 20 seconds (unless the TOE's documentation specify a higher value)

If applicable, the evaluator shall vary the lighting conditions and the capture devices during the phase 4 tests. The evaluator shall use at least (spread over ALL phase 4 tests):

- 4 different capture devices
- 4 different lighting environments.

For the phase 4 tests, a PAI, as defined in [1], is considered as a SUBJECT. If the a PAI is designed with accessories, the PAI + the accessories will be considered as a different SUBJECT.

Passing Criteria

The following table shows the criteria to get a PASS in the test. If none of those cases are given, the test results with a FAIL.

Table E.33 - Decision criteria for all tests in Phase 4

VARIABLE	OP.	THRESHOLD	VEREDICT
Number of SUBJECT_PASS	>	MAX_SUBJECTS_PASS	FAIL
Number of TEST_MATCHES	>	MAX_TEST_MATCHES	FAIL
Number of SETTING_MATCHES	>	MAX_SETTING_MATCHES	FAIL

According to the defined parameters, and in few words, it can be said that if a TRIAL results in a MATCH, the TEST will result directly a FAIL, so the TOE was proven to be vulnerable.

E.6.2 T4.1

This requirement is only applicable for evaluation in “Full-system” mode (see clause E.1).

Test crew

The SUBJECTS to take part in this TEST are:

- A minimum of 2 ID documents or other biometric reference, from the bona-fide users involved in the evaluation.
- 2 ATTACKERS, one per bona-fide user
- Therefore, the number of SUBJECTS is 2.

Parameters

In addition to all parameters specified in E.6.1, the following parameters shall be added:

- MIN_SUBJECTS = 2

With all these data the total number of TRIALS to execute, is 20.

E.6.3 T4.3.1

Test crew

- The goal is to vary the printed support between each SUBJECT (e.g., color of paper, type of support, image in B&W, etc.)
- The number of SUBJECTS will depend on the LoA, see parameters for T4.3.1.
- For “Full system” evaluation mode, no need to have real ID documents. The TOE shall provide a mean to import ID portrait images of the targeted SUBJECT in order to perform the face recognition process.

Parameters

In addition to all parameters specified in D.6.1, the following parameters shall be added:

Table E.34 - Parameters for T4.3.1 according to LoAs

LoA	Basic	Substantial	High
MIN_SUBJECTS	100	200	250
Total number of TRIALS	1000	2000	2500

E.6.4 T4.3.2

Test crew

- The goal is to vary the support for display between each SUBJECT (e.g., type of screen, screen with filters, etc.)
- The number of SUBJECTS will depend on the LoA, see parameters for T4.3.2.
- For “Full system” evaluation mode, no need to have real ID documents. The TOE shall provide a mean to import ID portrait images of the targeted SUBJECT in order to perform the face recognition process.

Parameters

In addition to all parameters specified in E.6.1, the following parameters shall be added:

Table E.35 - Parameters for T4.3.2 according to LoAs

LoA	Basic	Substantial	High
MIN_SUBJECTS	50	75	75
Total number of TRIALS	500	750	750

E.6.5 T4.3.3

Test crew

- The number of SUBJECTS will depend on the LoA, see parameters for T4.3.3.
- For “Full system” evaluation mode, no need to have real ID documents. The TOE shall provide a mean to import ID portrait images of the targeted SUBJECT in order to perform the face recognition process.
- The masks used shall include at least (each mask is considered as a SUBJECT):
 - o Curved paper masks

- o Fantasy masks
- o Head dummy (in silicone, polystyrene, etc.)
- o 3D printed masks



Figure E.15 - Examples of two paper masks (left) and three fantasy masks (right)



Figure E.16 - Examples of four head dummies (left) and one 3D printed mask (right)

Parameters

In addition to all parameters specified in E.6.1, the following parameters shall be added:

Table E.36 - Parameters for T4.3.3 according to LoAs

LoA	Basic	Substantial	High
MIN_SUBJECTS	50	75	75
Total number of TRIALS	500	750	750

E.6.6 T4.3.4

This requirement is only applicable for evaluation at LoA “Substantial” and “High” (see Table E.1).

Test crew

- The number of SUBJECTS will depend on the LoA, see parameters for T4.3.4.
- For “Full system” evaluation mode, no need to have real ID documents. The TOE shall provide a mean to import ID portrait images of the targeted SUBJECT in order to perform the face recognition process.
- The masks used shall include at least (each mask is considered as a SUBJECT):
 - o 3D rigid mask

- o Latex mask
- o High-quality latex mask (price over 300€) – **except for evaluation at substantial level**
- o Silicone mask – **except for evaluation at substantial level**



Figure E.17 – Examples of two 3D rigid mask attacks (left) and two latex mask attacks (right)



Figure E.18 – Examples of one high-quality latex mask attack (left) and three silicone mask attacks (right)

Parameters

In addition to all parameters specified in E.6.1, the following parameters shall be added:

Table E.37 - Parameters for T4.3.4 according to LoAs

LoA	Basic	Substantial	High
MIN_SUBJECTS	N.A.	50 (no High-quality latex mask and no Silicone masks)	100
Total number of TRIALS	N.A.	500	1000

E.7 Requirements for the overall decision

For a product applying for this application profile, a PASS will only be given if all applicable Phase 2, Phase 3 and Phase 4 tests result in PASS.

Biblio:

[1] ISO/IEC 30107-3 (2023)

[2] Ratha N.K., Connell J.H., Bolle R. M., Enhancing security and privacy in biometrics-based authentication systems. IBM Syst. J. 2001, 40 (3)

Bibliography

- BIO-iTC. (n.d.). *Face Toolbox*. (BIO-iTC) Retrieved 12 01, 2023, from <https://github.com/biometricITC/Face-Toolbox>
- ISO/IEC_JTC1/SC37_WG3. (s.f.). ISO/IEC 19794 (all parts), Information technology — Biometric data interchange formats.