**Swiss Biometrics Center (SBC)**
Idiap Research Institute
Rue Marconi 19
CH-1920 Martigny, Switzerland

# Information About Evaluations

| | |
|---|---|
| **Authors** | Dr Sushil Bhattacharjee |
| **Approved by** | Dr Sébastien Marcel |
| **Contributors** | |
| **Doc. Id** | SBC/Doc/D01-CQD |
| **Issue Date** | 2025/09/10 |
| **Version** | 2.1 |

| | |
|---|---|
| **Document Title** | Information About Evaluations |
| **Document Type** | SBC Customer Information Document |
| **Dissemination Level** | Biometrics vendors, Customers |
| **Reviewer(s)** | Dr Sébastien Marcel |

**Disclaimer**: Idiap and the SBC commit to apply their best effort in accomplishing the Services provided.
SBC warrants that to the best of its knowledge, at the delivery date, the Services do not infringe, violate or misappropriate any Intellectual Property Rights or proprietary rights of any third party.
SBC make no warranty that the use of the Services does not infringe, violate or misappropriate any Intellectual Property Rights or proprietary rights of any third party. The Services are provided ”as is” and ”as available”, without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of originality, merchantability, satisfactory quality, fitness for a particular purpose, reasonable care and skill, non-infringement, accuracy, reliability, completeness, or about resulted to be obtained from using the Services.

# 1 Introduction

The Swiss Biometrics Center (SBC)[1] is part of the Biometrics Security and Privacy Group at the Idiap Research Institute. Besides research activities, the SBC also performs independent evaluations of commercial biometrics products. The SBC is Accredited Biometrics Laboratory (ABL) by the FIDO Alliance as well as Google/Android. Specifically, the SBC offers the following kinds of evaluation services to vendors of biometrics products:

1. evaluation for FIDO biometrics certification,
2. evaluation for Android biometrics certification, and
3. independent evaluation.

ABLs for both FIDO Alliance ABLs and Android are bound by confidentiality and impartiality commitments to the respective certification bodies. Moreover, for any evaluation project, the formal contract signed between the vendor and the SBC shall include appropriate and mutually satisfactory confidentiality and non-disclosure agreements.

Evaluations for certification purposes are performed as prescribed by the relevant certification body (FIDO or Android)[2]. The vendor has no influence over how such an evaluation is performed.

This document aims to provide information regarding evaluations for biometric certification, and may start as a starting point for discussions between interested vendors and the SBC. Brief definitions of technical terms and acronyms used in this document are given in Section 2. Information relevant to evaluation for FIDO certification are provided in Section 3, and information for Android certification is included in Section 4. In Section 5 we briefly describe the independent evaluation services offered by the SBC. Additional practical information, aimed to facilitate quick and error-free evaluation, is provided in Section 6. Certain topics pertinent to evaluations are discussed in more detail in the Appendix.

As additional information for vendors, a description of the methodology and metrics involved in the tests are described in the Appendix.

[1] The SBC was formerly named Swiss Center for Biometrics Research and Testing, (SCBRT).

[2] The ABL (the SBC, in this case) is only responsible for performing the evaluation according to the procedures specified by the respective certification body, and for producing an evaluation report. To obtain the actual certification, the vendor must correspond directly with the certification body in question (FIDO or Android), which will take into account the evaluation report from the ABL when making any decision about certification of the vendor's product.

# 2 Glossary of Relevant Terms

- **Accredited Biometrics Laboratory (ABL)**: a testing laboratory (lab) accredited by the FIDO Alliance as having the capability to evaluate biometrics-based authenticators vying for FIDO certification.
- **Allowed Integration Document (AID)**: discussed in Section 3.4.
- **Attack Presentation Classification Error Rate (APCER)**: the proportion of attack presentations classified as *bona fide* by the TOE.
- **Bona-Fide Presentation Classification Error Rate (BPCER)**: the proportion of *bona fide* presentations classified by the TOE as PA.
- **Biometric sample**: biometric data captured by the biometric sensor in the TOE
- **Biometric reference**: a template, created from a biometric sample, that is used for enrolling a specific identity
- **Biometric probe**: a template, created from a biometric sample, that is compared with the biometric reference of the claimed identity, to verify the claimed identity.
- **False Accept Rate (FAR)**: the proportion of zero-effort impostor (ZEI) presentations incorrectly accepted during identity-verification tests
- **False Reject Rate (FRR)**: the proportion of genuine presentations that are incorrectly rejected by the TOE during identity-verification tests
- **Impostor Attack Presentation Accept Rate (IAPAR)**: the proportion of PAs incorrectly accepted by the TOE
- **Presentation Attack (PA)** (informally called spoof attack): a presentation made to a biometric sensor using a fake biometric-sample
- Presentation Attack Instrument (PAI): the object used to create a PA.
- **Software Development Kit (SDK)**: a software library, provided by the vendor, that replicates exactly the biometrics functionalities of the TOE.
- **Spoof Accept Rate (SAR)**: the proportion of PAs that are accepted by the TOE as *bona fide*. Similar to IAPAR.
- **Target of Evaluation (TOE)**: the biometrics-based authentication subsystem under evaluation
- **Test harness**: all the hardware and software necessary to perform live tests on the TOE (see appendix A1.3).

# 3 Evaluation for FIDO Biometrics Certification

The information provided in this section is publicly available, in greater detail, on the FIDO Alliance website[3]. Information specific to FIDO Biometric Certification presented here corresponds to two FIDO documents: (1) the Biometric Component Certification Policy v1.4[4] and (2) the FIDO Biometric Certification Requirements v3.0[5] (updated in January 2023). The present document shall be updated when the FIDO Alliance updates its policies or requirements.

FIDO Biometric Component Certification refers to two characteristics of the TOE: (1) its biometric-recognition (identity-verification) capability, and (2) the vulnerability of the TOE to presentation attacks (PA). The biometric-recognition performance of the TOE is quantified using two figures of merit: FRR, and FAR. The vulnerability of the TOE to PAs is expressed by its IAPAR. To be eligible for FIDO Biometric Certification, all three metrics for the TOE should be lower than a certain threshold.

Evaluation for FIDO Biometrics Certification involves two kinds of tests: *online* and *offline*. FIDO Alliance prescibes specific protocols for both kinds of tests. Online tests refer to 'live' tests performed on the TOE. Offline tests refer to tests performed on a separate computer, not on the TOE. Online tests enable us to estimate the FRR, whereas the FAR and IAPAR are estimated via offline tests based on a SDK provided by the vendor (see Sec. 3.3 for details). To obtain FIDO Biometrics Certification, the TOE should meet the specified performance levels of all three metrics. (Certification requirements for the three performance criteria – FAR, FRR, and IAPAR – are summarized on Table 1. Although the table shows other numbers pertaining only to face-biometrics, the requirements for these performance criteria are the same for all biometrics modalities.)

FIDO Biometric Certification can be achieved at four levels: **BioLevel1**, **BioLevel1+**, **BioLevel2**, and **BioLevel2+**. The difference between **BioLevel1** and **BioLevel2** is that for **BioLevel2** the TOE should achieve an IAPAR of 7% or less, whereas for **BioLevel1** the IAPAR may be as high as 15%. The difference between **BioLevel1** and **BioLevel1+** (and similarly, between **BioLevel2** and **BioLevel2+**) is the number of test subjects invited for the evaluation. For face-biometrics, the differences among the various FIDO Biometrics Certification levels are highlighted in Table 1.

As shown in the table, for **BioLevel1** we need to invite only 25 subjects, whereas for the number of test subjects required for **BioLevel1+** would be 245. The number of test subjects required depends on the biometrics modality used in the TOE. The numbers presented in Table 1 serve only to illustrate the differences among the four FIDO Biometrics Certification levels. Note that, because the number of subjects required for **BioLevel1** is much smaller than for **BioLevel1+**, the FAR and FRR requirements for **BioLevel1** certification are also lower than for **BioLevel1+** certification.

| | **BioLevel1** | **BioLevel1+** | **BioLevel2** | **BioLevel2+** |
|---|---|---|---|---|
| Num. subjects for FAR/FRR | 25 | 245 | 25 | 245 |
| Lab Tested FAR | 1% | **0.01%** | 1% | **0.01%** |
| Lab Tested FRR | 7% | **5%** | 7% | **5%** |
| Num. subjects for IAPAR | 15 | 15 | 15 | 15 |
| Lab Tested IAPAR | 15% | 15% | **7%** | **7%** |
| Num. PAI Species for Level A | 6 | 6 | 6 | 6 |
| Num. PAI Species for Level B | 8 | 8 | 8 | 8 |

Table 1: Some parameters of evaluation for FIDO Face Biometrics Certification.

[3] https://fidoalliance.org

[4] https://fidoalliance.org/specs/biometric/certificationpolicy/Biometric-Component-Certification-Policy-v1.4-fd-20211206.pdf

[5] https://fidoalliance.org/specs/biometric/requirements/Biometrics-Requirements-v3.0-fd-20230111.pdf

For IAPAR estimation, 15 PAIs are used for each PAI species. As indicated in Table 1, six Level A PAI species and eight Level B PAI species are used. For Level B, four PAI species shall be designed by the ABL tailored specifically to attack the kind of technology used in the TOE. The remaining four Level B PAI species, as well as all six Level A PAI species, may be the same for all TOEs of a given biometrics modality. This requirement implies that the vendor (or manufacturer) of the TOE should share relevant information with the ABL (us) to help construct appropriate PAIs of Level B. Such information may be shared on the basis of a non-disclosure agreement, if necessary.

In the remainder of this section we describe the items the vendor is expected to provide the ABL for evaluation related to FIDO Biometrics Certification.

## 3.1 Articles the Vendor Provides to the SBC

According to FIDO requirements, before a FIDO evaluation of the TOE can be performed, the vendor will have to provide the ABL with the following articles:

1. TOE and test-harness, along with the descriptions listed in Section 3.2
2. Software development kit (SDK) for offline tests on a computer
3. FIDO Allowed Integration Document (FAID)
4. Descriptions of previous tests, if applicable
5. Other relevant details

## 3.2 Description of the Target of Evaluation (TOE)

Here, the TOE is the biometric subsystem to be certified. The vendor shall describe the components and functionality of the TOE, including information about the following:

1. **Data capture**: describe the sensors used by the TOE for capturing the input biometric samples. Does the TOE include functionality to allow the ABL-testers to download the raw biometrics samples captured by the TOE? This is helpful when preparing the offline tests.
2. **Signal processing subsystem**: describe the features extracted from each biometric sample, and the feature-extraction process. In case different processes are used during enrolment and probe, please include sufficiently detailed information about both kinds of processes. The TOE shall include functionality to enable the ABL-testers to download the templates (enrolment and probe) to an external computer. This is necessary for the offline tests using the SDK.
3. **Data storage**: what data is recorded/stored on the TOE? In what representation? What is the size of each enrolment or probe template? Are biometric references (also called enrolment templates) stored in encrypted form on the TOE? What is the maximum number of identities that can be enrolled simultaneously?
4. **Comparison**: describe the method used for comparing a biometric probe with a biometric reference.
5. **Decision**: the procedure for converting the matching result into a decision (e.g., the score-threshold used) The FIDO Alliance requires that the vendor provide the testing-lab with the above information. Please include brief, compact, but complete descriptions for the points listed above. Wherever relevant, for example for software and hardware components, please mention the version numbers of the components supplied for tests. In addition, please provide sufficiently detailed instructions on how to operate the TOE.

## 3.3 Software Development Kit (SDK)

Please provide a SDK with the same biometrics functionalities as the TOE. This SDK will be used to perform offline tests, partly based on the data (templates, raw biometric-samples) downloaded from the TOE. The SDK will also be used to validate the results of the online tests. The SDK should be accompanied with adequate documentation for installing and using it. The documentation should include the version number of the SDK, and should specify the computational resources and environments necessary for using the SDK.

## 3.4 FIDO Allowed Integration Document (FAID)

This document should describe, in detail, all hardware and software modifications to the TOE necessary to integrate it into the final commercial product. FIDO Alliance requires the vendor to provide the ABL (SBC) with a complete FAID. The ABL is required to provide FIDO Alliance with an assessment of how the proposed modifications may affect the biometrics performance of the TOE. The FAID shall be shared with the FIDO Alliance, along with the final evaluation report. A template for the FAID can be found on the FIDO Alliance website[6].

## 3.5 Duration of Evaluation Project

The duration of a FIDO evaluation project depends on the biometrics modality being used by the TOE. As explained in Appendix A1.2, the biometrics modality in question dictates the number of subjects to be used for the evaluation. In general, we expect an evaluation of a TOE with face modality to take about 10 weeks for **BioLevel1** or **BioLevel2** and approximately 13 weeks for **BioLevel1+** or **BioLevel2+**. The duration may be different for other biomerics modalities. Precise start and end dates of a specific project are decided after discussion with the vendor.

[6] Version 1.2 of the document, accessed on 2021/04/26, is available via the following link:
`media.fidoalliance.org/wp-content/uploads/2020/02/FIDOAllowedIntegrationDocumentTemplate_v1.2.pdf`
Please note that more recent versions may be available.

# 4 Evaluation for Google/Android

Evaluation for Android biometrics certification is somewhat different from that for FIDO certification. For Android certification the evaluation performed by the ABL focuses on estimating a single PAD metric: SAR (see Section 2).

Although, for Android certification, the ABL only estimates the SAR of the TOE, this does not mean that biometrics recognition performance (as measured using FAR and FRR) is not considered for Android certification. Android/Google expects the vendor to report the FAR and FRR of their product based on evaluations conducted by the vendor itself.

Due to existing non-disclosure agreements, we are not able to discuss details of the tests we perform during an evaluation for Android biometrics certification. We can, however, direct interested readers towards relevant information made publicly available by Android[7]. Further compatibility information may also be found on the Android website[8].

## 4.1 Articles the Vendor Provides to the SBC

According to FIDO requirements, before a FIDO evaluation of the TOE can be performed, the vendor shall provide the ABL with the following:

1. the TOE,
2. the test-harness, and
3. adequate documentation for the TOE and the test-harness.

## 4.2 Allowed Integration

The vendor of a biometrics system typically recommends an *allowed integration* process, to be used for integrating the biometrics system into a commercial product (*e.g.*, for integrating a capacitive fingerprint sensor from vendor X, in a smartphone manufactured by a company Y). Android recommends that integrators follow the allowed integration process defined by the vendor of the biometrics system. However, unlike for FIDO certification, Android does not require vendors to furnish an AID to the ABL for evaluation.

# 5 Independent Evaluations by SBC

The SBC also performs independent evaluations of biometrics products. The evaluation protocols followed for independent evaluations are similar to those designed by official certification bodies (such as FIDO Alliance), and are therefore compliant with the ISO 19795-1 standard, but have a smaller scope. Independent evaluations can be tailored to the requirements of the vendor / manufacturer / commercial-partner. For such evaluation projects, the SBC follows an evaluation protocol agreed in advance with the vendor. Vendors often request independent evaluations for internal R&D purposes, but if necessary, the SBC can also provide formal letters to 'certify' the performance of a given product in such an independent evaluation.

[7] `https://source.android.com/security/biometric/measure` (accessed on 15-April-2021).

[8] `https://source.android.com/compatibility/cdd` (accessed on 15-April-2021).

# 6 TOE Output

During the evaluation the TOE is expected to generate certain outputs, to enable offline analysis of the evaluation results. Evaluation metrics are estimated on the basis of transactions (see Sec. A1.2 for discussion about transactions).

## 6.1 Outputs for FIDO Certification

For an evaluation towards FIDO certification, the TOE should be capable of recording the following information:

1. Biometric samples used to constructing the biometrics references for every identity
2. All biometric probe samples
3. Results of each probe-transaction in a log-file (see Section 6.3)

The TOE should include functionality to enable the testers to downloaded all recorded information to an external computer (via a USB-cable or wireless connection to the computer).

## 6.2 Outputs for Android Certification

For evaluations related to Android certification, the TOE should record the results of probe-transactions in log-files. Again, the TOE should include functionality to enable the testers to download the log-files to an external computer for offline analysis.

In Section 6.3 we propose a log-file format in json.

## 6.3 Log-File Format

For a single transaction, the evaluation results shall be logged in a file, in the following json structure:

```
{
"transactionID": <unique-string or unique-numeric>
"time_stamp": <value>
"input:{
                "subjectID": <value>
                "presentation_type": <"BF" or "PA">
                "rec_score_thresh": <float>
                "pad_score_thresh": <float>
        }
"output": [
                {
                "attemptID": 1
                "final_decision" : <"0" or "1">
                "rec_score": <float>
                "rec_decision": <"0" or "1">
                "pad_score": <float>
                "pad_decision": <"0" or "1">
                },
        ...
                {
                "attemptID": 5
                "final_decision" : <"0" or "1">
                "rec_score": <float>
                "rec_decision": <"0" or "1">
                "pad_score": <float>
                "pad_decision": <"0" or "1">
                }
        ]
}
```

The json-structure proposed above is a hypothetical example. We are happy to discuss with the vendor of the TOE in question, how the proposed structure may be adapted to something more suitable to the evaluation project and to the vendor. For example, for a fingerprint recognition system, the ‘`input`’ section should include additional elements to identify the hand (left or right) and the specific finger in each hand.

The two elements ‘`rec_score_thresh`’ and ‘`pad_score_thresh`’ in the ‘`input`’ section refer to the recognition-score-threshold and PAD-score-threshold used in the TOE. The element ‘`rec_score`’ in this example refers to the recognition-score generated by the TOE for the attempt in question, and ‘`pad_score`’ refers to the PAD-score generated for that attempt. Similarly, ‘`rec_decision`’ and ‘`pad_decision`’ indicate the decision produced by the biometric-recognition subsystem and the PAD-subsystem of the TOE, respectively. These two (decision) elements take binary values. (NOTE: If your TOE does not explicitly generate ‘`rec_decision`’ and ‘`pad_decision`’, then these elements may be left out of the log-file.) The element ‘`final_decision`’ carries a binary value, say, 0 or 1, indicating that the attempted was ‘accepted’ (1) or ‘rejected’ (0).

The vendor may also choose a completely different format for the log-file. However, please note that the proposed json-structure will enable us to analyse the log-files more quickly. In particular, please note that that cost-estimates for evaluation projects are made on the assumption that the log-files will be formatted as suggested in this section. If the vendor chooses a different format (*e.g.*, a free-text format where every line corresponds to a single attempt), this may impact the cost and duration of the evaluation project.

# A1 Appendix

## A1.1 Presentation Attack Instruments

During initial discussions for evaluation projects, vendors often ask us about the PAIs used in such evaluations. We prefer not to discuss this topic in great detail, partly due to confidentiality agreements with certification bodies, and, more generally, in the interests of fairness and neutrality of the evaluation.

The PAIs used in our evaluations are constructed following the guidelines set out in relevant ISO/IEC and Common Criteria documents. PAIs are categorized into three levels – A, B, and C – depending on the complexity of the PAI (skill, cost, and time required to create the PAI). PAIs of level A are the simplest to construct, requiring no special skill, and less than a day to create. Level B PAIs should be more difficult to construct than Level A PAIs. These PAIs may take up to 3 days to make, and may require some special skills, or specialized equipment. PAIs of level C require the most skill, investment and time (more than 3 days) to manufacture. Evaluation projects aimed at certification by industry-bodies typically require PAIs of Levels A and B only.

The PAIs used in our evaluation are prepared, and deployed (for performing attacks), in accordance with the protocols specified by the certification bodies (FIDO Alliance or Android). In particular, PAIs for evaluations aimed at FIDO Alliance certification are created according to the relevant ISO standards. For evaluations oriented towards Android certification, the PAIs are prepared according the specifications provided to us by Google.

## A1.2 Description of Evaluation Metrics

**Transaction**: The various figures of merit – FAR, FRR, IAPAR – are estimated on the basis of *transactions*. A transaction consists of one or more *attempts*, where one attempt is a single presentation captured by the TOE. In real-world situations, when a person is trying to spoof an biometrics system using a PA, if the first PA fails, the person is likely to try again immediately. To prevent a user from repeating attempts for a long time, most biometrics systems also implement a time-out period.

The concept of transactions is designed to enable the simulation of such behavior during evaluations. Specifically, a transaction starts with the first attempt, and ends with any of the following three conditions is satisfied:

1. an attempt is accepted as *bona fide* by the TOE,
2. the predefined maximum number of attempts (typically, five), is reached, or
3. the predefined time-out limit is reached.

The maximum number of attempts per transaction and the time-out limit are not standardized. The vendor (or manufacturer) is free to define these parameters for the TOE in question. For FIDO Biometrics Certification evaluation, however, the time-out limit may not exceed 30 seconds. In general, regardless of the kind of evaluation desired, we recommend that the time-out limit be set to 30 seconds, and the maximum number of attempts in a transaction be set to five.

**False Reject Rate (FRR)**: The FRR is computed based on online tests, that is, with live presentations using the target of evaluation (TOE). For a TOE to be FIDO certified at **BioLevel1**, the FRR must be at most 7% at the upper bound of the 80% confidence interval (and at most 5% at the upper bound of the 8% confidence interval for **BioLevel1+** certification).

For the biometrics modality in question (face, fingerprint, iris, etc., depending on the TOE) of each subject is first enrolled in the TOE. After enrolment, each subject performs a fixed number (typically, five) of probe-transactions the TOE to verify his/her identity with each biometric trait (one face, two irises, and so on). During each probe transaction, the subject is allowed multiple attempts, until the end of the transaction (explained above). If, on the last attempt, the TOE still fails to verify the subject's identity, this is considered a false-reject for that probe transaction. The FRR is the proportion of probe transactions that result in a false-reject, expressed as a percentage.

**False Accept Rate (FAR)**: The FAR is computed based on offline tests, that is, tests on a (linux) computer, conducted using the SDK provided by the vendor. We (the ABL) shall implement a software-app to perform experiments to compute the FAR. For this purpose, we prefer to receive from the vendor a SDK compatible with linux OS. The app will compute the FAR based on the presentations (enrolments and probes) downloaded from the TOE. In other words, the same data shall be used for computing FAR as was used for computing FRR. For each enrolled subject, all biometrics samples of all other subjects shall be used as probes for verification. If a probe is accepted (verified) by the TOE for a given enrolled identity, this is considered a false-accept. The FAR is computed as the proportion of probes that result in a false-accept, expressed as a percentage.
The app shall also perform tests to compute the FRR, and verify that the verification-scores generated during the online tests match those generated by the SDK. This procedure is required by FIDO Alliance, to verify that the provided SDK is identical to the TOE in terms of behavior (*i.e.*, for a given comparison it generates the same score as the TOE). Therefore, the TOE should include functionality to enable the testers to export the raw verification-scores as well as verification decisions (accept or reject) generated during the online tests.

**Impostor Attack Presentation Accept Rate (IAPAR)**: The IAPAR estimates the vulnerability of the TOE to PAs. This is computed using PAIs created for by the ABL according to the biometric-trait being verified by the TOE. PAIs constructed for a predetermined number of subjects/identities shall be used to estimate the IAPAR. (The number of subjects depends of the kind of evaluation requested, and shall be agreed between the ABL and the vendor before the commencement of the evaluation.) Probe PA transactions, using the PAIs, shall be made for the corresponding enrolled identity, as done for FRR estimation. In a given transaction (which may involve several attempts within the time-out limit set in the TOE), if a PA is accepted by the TOE, then this is considered an Impostor Attack Presentation Acceptance. The IAPAR is computed as the proportion of the total number of PAIs that resulted in a Impostor Attack Presentation Acceptance, expressed as a percentage.

## A1.3 Common Test Harness

The following text has been reproduced from FIDO documents, to provide additional information to vendors regarding test harnesses. The FIDO Alliance defines a Common Test Harness as follows:

A. *Configurable Enrollment system which:*
   1. *Selects the operating point(s) to be evaluated.*
   2. *Has enrollment hardware / software as will be executed by the FIDO authenticator.*
   3. *Includes a biometric data capture sensor and enrollment software.*
   4. *Can clear an enrollment.*
   5. *Can store an enrollment from acquired biometric sample(s) for use in on-line verification evaluation.*
   6. *Can provide enrollment templates from acquired biometric sample(s) defined as "user's store reference measure based on features extracted from enrollment samples" for use in off-line verification evaluation.*
   7. *Indicates a failure to enroll ([ISOIEC-19795-1], 4.6.1)*

B. *Configurable Verification on-line system which:*
   1. *Selects the operating point(s) to be evaluated.*
   2. *Has verification hardware / software as will be executed by the FIDO authenticator.*
   3. *Includes a biometric data capture sensor, a biometric matcher, and a decision module.*
   4. *Captures features from an acquired biometric sample to be compared against an enrollment template.*
   5. *Makes accept/reject decision at a specific operating point.*
   6. *Indicates an on-line failure to acquire ([ISOIEC-19795-1], 4.6.2).*
   7. *Indicates an on-line decision(accept or reject).*
   8. *Provides a set of acquired biometric sample(s) from an on-line verification transaction (this is called a stored verification transaction). This will be used for off-line verification.*

C. *Configurable Verification off-line software, which:*
   1. *Selects the operating point(s) to be evaluated.*
   2. *Has verification software as will be executed by the FIDO authenticator.*
   3. *Accepts an enrollment template and the stored verification transaction and performs matching in off-line batch mode.*
   4. *Provides a decision (accept or reject).*

D. *logging capabilities, which:*
   1. *Record every interaction with the TOE.*
   2. *Allow the tester to manually addd interactions (e.g. the fact that a tester just cleaned the sensor device)*