

To whom it may concern:

The Swiss Center for Biometrics Research and Testing (SCBRT) is part of the Biometrics Security and Privacy group at the Idiap Research Institute. The SCBRT is also a FIDO Alliance Accredited Biometrics Laboratory (ABL). On behalf of Identity Inc., the SCBRT has conducted an evaluation of the presentation attack detection (PAD) efficacy of the Identity Face Authentication solution in accordance with ISO/IEC 30107-3 evaluation protocols. This letter summarizes the evaluation and the main outcomes.

Target Of Evaluation (TOE): Identity Face Authentication solution, version 1.9.4.0.

Test Harness: Motorola g7 smartphone, running Android 9. The TOE uses the front camera of the smartphone to capture face biometric-samples.

Scope of Evaluation: PAD, using Level B attacks only. The Presentation Attack Instruments (PAI) have been created in accordance with ISO standards used to assess and triage the attack potential of presentation attacks (PA). Level B PAs are attacks that require some skill to make, and may require more than one day to create. In this case the Level B PAs are constructed by processing high-quality digital face-photographs to enhance the image quality and to mitigate the effects of printing and re-capturing.

PAIs of the following nine Level B species have been used in this study:

- four PAI species of color printed-photo attacks, using face images printed on two kinds of photo-quality paper (matte, glossy) on two kinds of printers (laser, Inkjet),
- one paper-mask PAI species, where each mask is cut out from a color-photograph printed on matte paper, and has holes cut out for eyes and nose,
- two PAI species of replay-attacks, based on still color face-images displayed on two hand-held devices (tablet, and smart-phone), and
- two PAI species of video replay-attacks made using the same two hand-held devices.

The TOE has been evaluated using *bona fide* and PA transactions, where each transaction consists of up to five attempts performed within a period of 30 seconds.

Ten subjects participated in this evaluation (four female and six male). Each subject first enrolled oneself, and then performed five *bona fide* transactions. Subsequently, five PA transactions were made for each PAI (10 PAIs per species).

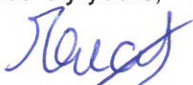
The performance metrics estimated in this evaluation are summarized in Table 1.

Metric	Value	Explanation
BPCER	8%	Bona-fide Presentation Classification Error Rate (BPCER) is the proportion of <i>bona fide</i> transactions that were incorrectly rejected by the PAD subsystem of the TOE.
APCER	0%	Attack Presentation Classification Error Rate (APCER) is the proportion of PAs that were incorrectly classified as <i>bona fide</i> by the PAD subsystem of the TOE.
IAPMR	0%	Impostor Attack Presentation Match Rate (IAPMR) estimates the vulnerability of the TOE to PAs and is computed as the proportion of PAs on a given identity that were accepted by the TOE.

Table 1: Performance metrics estimated for the TOE in this evaluation.

Additional Analysis: The median capture-time per attempt (the time required to capture the biometrics sample) was about 4 seconds. The median processing-time (required to generate a decision based on the captured biometric sample) including PAD and face-recognition, was about 230 milliseconds.

Sincerely yours,



Dr. Sébastien Marcel



Dr. François Foglia
Deputy Director
Idiap Research Institute