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 Foundation of the Idiap Research Institute. The SCBRT is a FIDO Alliance Accredited Biometrics Laboratory (ABL).[1] Under contract with Mobai[2], the SCBRT has evaluated the efficacy of the Mobai's face presentation attack detection (PAD) solution, in accordance with ISO/IEC 30107-3 evaluation protocols. The PAD performance of the product has been evaluated on two smartphones: iPhone 7 and Samsung S9, using Level A presentation attacks (PA). *The product performed perfectly in this evaluation.* This letter describes the evaluation and summarizes the main outcomes.

Target Of Evaluation (TOE): The evaluated product consists of two separate software components, a client and a server. The following software components have been evaluated in this study: client version 2.0.0 and server version 2.0.0.

Test Harness:
- iPhone 7, running iOS 14.1;
- Samsung S9, running Android 10; and
- łaptop, running Ubuntu version 20.04.

The client runs on each phone, captures face biometric samples, and transmits each sample to the server, running on the laptop, via a wireless connection. The server processes the biometric samples and transmits each decision ('*bona fide*' or 'Presentation Attack') back to the client, which displays the result on the phone-screen. The *bona fide* subjects and the testers interact only with the client on each phone.

Scope of Evaluation: Presentation Attack Detection (PAD), using Level A attacks. The Presentation Attack Instruments (PAI) have been created in accordance with ISO standards used to assess and triage the attack potential of PAs. Level A PAIs are attack instruments that can be created within a day, requiring neither sophisticated equipment nor a high degree of expertise.

PAIs of the six Level A species have been used in this study. They are listed in Table 1. The PAI species have been defined in consultation with Mobai. However, the actual PAIs have been constructed by the SCBRT independently, without any involvement of Mobai.

PAI Species	Description
A1	Face printed on glossy photo paper using inkjet printer
A2	Face printed on matte photo paper using inkjet printer
A3	Face printed on glossy photo paper using laser color printer
A4	Face printed on matte photo paper using laser color printer
A5	Face image displayed on Apple iPad 2 tablet
A6	Face image displayed on an Android smartphone

Table 1: List of Level A PAI species used in this evaluation.

The TOE has been evaluated using *bona fide* and PA transactions, where each transaction may consist of up to five attempts (each attempt being a single presentation) performed within a period of 30 seconds. The TOE records the result of each attempt of each transaction in a logfile.

---

[1]The evaluation discussed in this letter is not related to FIDO certification.
[2]www.mobai.bio

Ten PAIs per species have been used. For each species, five PAIs have been used to evaluate the TOE on the iPhone 7 and the remaining five have been used for PAs on the Samsung S9.

A reference *bona fide* score-distribution has been constructed based on 10 subjects (five women and five men). Each subject performed five transactions on each phone. Thus, a total of 50 *bona fide* transactions and 150 Level A PA transactions (25 per PAI species) have been made on each phone. Note, that a given transaction may include several (up to five) attempts. Table 2 shows the total number of transactions and attempts for each phone. In particular, the table indicates that a single attempt was sufficient for each *bona fide* transaction.

Phone	Bona fide		Level A Presentation Attacks	
	Transactions	**Attempts**	**Transactions**	**Attempts**
iPhone 7	50	50	150	750
Samsung S9	50	50	150	749

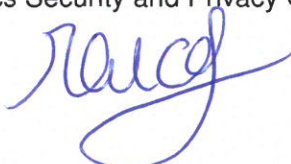Table 2: Number of transactions and attempts in this evaluation.

Evaluation Results: The performance of the TOE in this evaluation is quantified using several ISO metrics. On both phones the TOE achieved perfect results for all Level A PAIs. The performance-metrics of the TOE are summarized in Table 3.

Metric		iPhone 7	Samsung S9
BPCER	Bona-fide Presentation Classification Error Rate (%): the proportion of *bona fide* transactions incorrectly classified as PA	0	0
APCER	Attack Presentation Classification Error Rate (%): the proportion of PA transactions incorrectly classified as *bona fide*	0	0
BPNRR	*Bona fide* Presentation Classification Error Rate (%): proportion of *bona fide* transactions that did not result in a response from the TOE	0	0
APNRR	Attack Presentation Non-Response Rate (%): proportion of PAs of the same PAI species that produced no response from the TOE	0	0
APAR	Attack Presentation Acquisition Rate (%): proportion of PA transactions that did elicit a response from the TOE	100	100

Table 3: Performance metrics estimated for the TOE in this evaluation. See ISO/IEC 30107-3 for definitions of these metrics. The TOE achieved perfect results in this evaluation, for Level A PAIs. For the Level A PAIs used in this evaluation (Table 1), the TOE achieved perfect results on both smartphones.

Sincerely yours,

Dr. Sébastien Marcel
Head
Biometrics Security and Privacy Group

Dr. François Foglia
Deputy Director
Idiap Research Institute