Docusign Envelope ID: 941D9CF5-7C34-8625-81C7-E111517219DD

BixeLab

Biometrics Identity Experience & Evaluation Laboratory

Letter of Confirmation

Issued to **Emirates Face Recognition LLC** for the test report issued on the 2nd of November 2026 for **CEN/TS 18099-Aligned High Level Injection Attack Detection (IAD) Evaluation** of,

EFR-Mobile SDK (Android MFL v5.1.3 and MFL iOS v5.1.3) and **EFR-WebSDK WFL v1.6.5** – Target of Evaluation

To whom it may concern,

Between 14th September and 15th October 2026, BixeLab conducted an independent High level injection attack detection evaluation of Emirates Face Recognitions' EFR-Mobile (Android MFL v5.1.3 and MFL iOS v5.1.3) v5.1.3 and WebSDK WFL v1.6.5. Injection attack methods (IAMs) and injection attack instruments (IAIs) were executed against the Android, iOS and Web environments to assess the system's resilience under controlled laboratory test conditions. This evaluation took place at the BixeLab headquarters located in the Australian Capital Territory, Australia.

BixeLab (NVLAP Lab Code: 600301-0) is accredited by the NIST-administered National Voluntary Laboratory Accreditation Program (NVLAP) to ISO/IEC 17025:2017 for services listed on its published scope. NVLAP does not currently accredit Injection Attack Detection (IAD) to CEN/TS 18099. This evaluation was therefore conducted in close alignment with CEN/TS 18099, but it does not constitute an NVLAP-accredited outcome.

Testing parameters

- **Platforms:** Android 13 and 15, iOS 26.3 and 16.7, and WebSDK WFL v1.6.5 (tested on Google Chrome v153 and Firefox v156)
- **Injection Attack Methods (IAMs):** Virtual-sensor injection (OBS virtual camera and HDMI/USB capture card), Android virtual camera (VCam Xposed module), device emulation, and function hooking of rooted and emulator detection routines.
- **Injection Attack Instruments (IAIs):** Fifteen representative species – Selfie image, passport image, posed photo, video, face morphed image, face swap image, deepfake video (MyHeritage), deepfake video (DeepLiveCam), face reenactment video (LivePortrait), 3D avatar reenactment video (LargeAvatarModel), AI Profile, DeepLiveCam HighQuality Video, AgeSwap Image, Live DeepLiveCam, and Live LivePortrait.
- **Bona fide runs:** 300 total, resulting in a BPCER of 0.67%.
- **Injection Attempts:** 1,350 IAI transactions delivered through virtual-camera (OBS, 450 transactions), USB-camera (HDMI capture, 450 transactions) and VCam module (Android Virtual Camera, 450 transactions). In the final validated configuration of the TOE (Android MFL v5.1.3, MFL iOS v5.1.3 and WFL v1.6.5), all injection transactions were rejected.
- **Integrity & Environment Controls:** All tests were executed under controlled conditions at BixeLab's Griffith (ACT) laboratory, using predefined test devices and toolchains. Android root, iOS jailbreak and emulator detection routines were identified and targeted by function hooking and were partially bypassed by function hooking, however, the application remained uninitialized preventing the capture workflow from starting.

Conclusion

Within the scope of testing, all 1,350 injection transactions across the IAMs and IAIs tested were rejected by the final validated versions of the TOE (Android MFL v5.1.3, MFL iOS v5.1.3 and WFL v1.6.5) and no successful injection bypasses were observed. Attempts to bypass Android root, iOS jailbreak and emulator detection achieved partial bypasses, but the application did not start the capture flow in the emulated environment. See full details in the test report (26_BXL065_TR_11).

Ms. Somya Singh
General Manager
BixeLab Pty Ltd
info@bixelab.com

Dr. Ted Dunstone
Chief Executive Officer
BixeLab Pty Ltd
info@bixelab.com

NOTE: This letter is a validation summary only i.e., this was not a certification, benchmark, or endorsement by NIST, NVLAP, or any government agency. The results apply only to the stated versions, configurations, datasets, and conditions; coverage is limited to the tested IAMs/IAIs, it may be reproduced only in full, and BixeLab accepts no liability for use beyond the stated purpose.