BixeLab

Biometrics Identity Experience & Evaluation Laboratory

Letter of Confirmation

Issued to HyperVerge Technologies Private Limited

for the test report issued on the 12th of October 2026 for

CEN/TS 18099-Aligned Injection Attack Detection (IAD) Level Substantial Evaluation of,

HyperKYC SDK with HyperVerge FAS system (Android v2.12.1, iOS 1.6.1, Web v11.0.0) – Target of Evaluation (TOEs)

To whom it may concern,

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.

Between 1st July and 10th September 2026, BixeLab conducted an independent injection attack detection evaluation of HyperKYC SDK with HyperVerge FAS system (Android v2.12.1, iOS 1.6.1, Web v11.0.0). Four Injection attack methods (IAMs) and 10 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.

Testing parameters

- **Platforms:** Android 13 and 16, iOS 26.3 and WebSDK (tested on Google Chrome v153.0.7977.85 and Safari v 26.6.2)
- **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):** Ten 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).
- **Bona fide runs:** 300 total, resulting in a BPCER of 1.33%.
- **Injection Attempts:** 630 IAI transactions delivered through virtual-camera on Mac device (OBS, 300 transactions), USB-camera on windows devices (HDMI capture, 300 transactions) and iOS VCam module (iOS Virtual Camera, 30 transactions). These transactions were rejected by the TOE.
- **Integrity & Environment Controls:** All tests were executed under controlled conditions at BixeLab's Griffith (ACT) laboratory using predefined test devices and toolchains. Root and detection routines were identified and targeted by function hooking and were partially bypassed by function hooking, however, the ToE was unable to capture virtual frames at the capture stage.

Conclusion

Within the scope of executed testing, no successful sensor-level injection bypasses were observed. Across the IAMs and IAIs tested, all 630 injection transactions were rejected by the TOE. Attempts to bypass root detection were successful but the application did not capture the virtual frames from VCam. No IAIs were successfully injected. See full details in the test report (26_BXL027.3_TR_21).

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

Dr. Ted Dunstone
Senior Responsible 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.