Docusign Envelope ID: A5E3A7C6-81E9-8EBD-831E-A28F9E27DAAB

BixeLab

Biometrics Identity Experience & Evaluation Laboratory

Letter of Conformance

Issued to TWYN T4ISB Do Brasil Tecnologia E Participações LTDA

for the test report issued on the 21st of October 2026 for

CEN/TS 18099-Aligned Injection Attack Detection (IAD) Basic (Level 1) Evaluation of **T4FastID SDK (Android v1.0)** – Target of Evaluation (TOE)

To whom it may concern,

From 6th to 8th October 2026, BixeLab conducted an independent IAD evaluation of the T4FastID SDK (Android v1.0) at its headquarters in the Australian Capital Territory, Australia. The evaluation comprised Basic (Level 1) IAD technical checks, supplementary injection resilience tests, and transport security validation in the Android environment to assess the TOE's resilience and security controls under controlled laboratory test conditions.

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 of accreditation. NVLAP does not currently accredit Injection Attack Detection (IAD) evaluations against CEN/TS 18099. Accordingly, this evaluation was conducted in close alignment with CEN/TS 18099: 2024 and does not constitute an NVLAP-accredited outcome.

Testing parameters

- **Platforms**: Samsung Galaxy S23, Samsung Galaxy S24, Samsung S20 (Magisk-rooted) and ARM64 Android Emulator (Android 16).
- **Scope of Evaluation**: Basic (Level 1) IAD technical checks, supplemented by targeted attack scenarios involving virtual-camera injection, Android emulator manipulation, rooted-device exploitation, SDK manipulation, and runtime API hooking techniques.
- **Positive Functional Check (Bona Fide)**: 20 bona fide transactions were completed across two physical Android devices under multiple lighting conditions. All transactions passed successfully, although some unexpected detector signals were observed.
- **Negative Smoke Check**: 30 negative smoke transactions were conducted across two injection approaches, with all transactions rejected as expected.
    - **Virtual Camera on Android Emulator**: 15 OBS virtual-camera injection transactions were conducted on an ARM64 Android emulator. All were rejected before reaching Sentinel.
    - **VCam on Rooted Android**: 15 VCam injection transactions were conducted on a Magisk-rooted Android device. All were rejected.
- **Integrity & Environment Controls**: Testing was conducted under controlled laboratory conditions at BixeLab's Griffith (ACT) facility using predefined devices and toolchains. Root-detection and integrity-check routines were identified and targeted through function hooking.

Conclusion

Within the scope of executed testing, the TOE demonstrated satisfactory performance in the Basic (Level 1) evaluation. All 20 bona fide transactions were completed successfully, Minor detector signals (SILENTLIGHT_RESPONSE_ABSENT and VIDEOSPOOF) were logged but did not impact final transaction outcomes. All 30 negative smoke transactions were detected and rejected as expected. Transport security checks confirmed the use of HTTPS/TLS usage and certificate pinning, with no cleartext HTTP observed. Some unexpected detector signals were noted during bona fide testing.

Based on the executed evaluation, BixeLab confirms that the T4FastID SDK (Android v1.0) successfully completed a Basic (Level 1) IAD evaluation conducted in alignment with CEN/TS 1809:2024. For further details, refer to the full test report (26_BXL077_TR_00_IAD).

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.