

## LETTER OF CONFIRMATION

## Fortface SDK — Web

UNE CEN/TS 18099:2024 — Biometric data injection attack detection

HIGH LEVEL · LEVEL 3

Antisec Serviços de Informática Ltda. confirms that the product **Fortface SDK — Web**, owned by Payface, was evaluated under the methodology established by **UNE CEN/TS 18099:2024 — Biometric data injection attack detection**, at the **High (Level 3)** conformance level — **the highest of the three evaluation levels defined by the standard** — on the basis of a formally documented Security Target analysed in depth. The evaluation covered **15 distinct species of Injection Attack Instrument (IAI)** and **3 distinct Injection Attack Methods (IAM)**, as required by Clause 8.6 (Table 4) of the standard.

The product **met both Annex A criteria** of the standard for the High level: it resisted all 18 injection attack runs **with no bypass**, and returned a legitimate-user rejection rate (BPCR) of **2.00%**, against a target value of 15%. The full account of the method, test environment and results is set out in the letter on the following page.

## FINAL VERDICT

**PASS — High Level (Level 3)****18**

ATTACK RUNS

**0**

BYPASSES

**2.00%**

BPCR · TARGET ≤ 15%

ISSUED TO

**Payface / Fortface**

PRODUCT (TOE)

**Fortface SDK — Web**

VERSIONS EVALUATED

SDK Web 2.6.0 · Web Demo APP v3.56.0 · Backend v3.56.0

TYPE OF EVALUATION

IAD subsystem evaluation — injection detection

ENGAGEMENT PERIOD

30 July to 18 August 2026

TECHNICAL REPORT

**ANTISEC-IAD-FORTFACE-WEB-2026-af222402db**

DATE OF ISSUE

**18 August 2026****Victor Henrique Dias Matuk**

CEO — Antisec Serviços de Informática Ltda. · 18 August 2026

+55 (11) 91899-4624 · matuk@antisec.com.br



AS-IAD-2026-0001

VERIFY

EVALUATION

**CEN/TS****18099**High Level  
2026

18 August 2026

## To whom it may concern,

Antisec Serviços de Informática Ltda. conducted **Biometric Injection Attack Detection (IAD)** testing in accordance with **UNE CEN/TS 18099:2024 — Biometric data injection attack detection**, at the **High (Level 3)** conformance level, the most demanding of the three levels defined by the standard.

This testing was conducted with Payface's **Fortface SDK Web 2.6.0**, together with **Web Demo APP v3.56.0** and **Backend v3.56.0**, running on the isolated staging instance <https://app-demo-lab.fortface.ai/>. The build remained frozen — in both version and configuration — from 10 August 2026, 11:30 BRT until the close of the collection window. The engagement ran from **30 July to 18 August 2026**.

Testing was carried out from two independent attack workstations: a **Linux** station running the Chrome browser, with physical cameras disabled and an **operating-system-level virtual camera** fed by pre-produced video; and a **Windows 11** station running Chrome driven through **browser automation**, with a dedicated GPU for real-time synthetic generation. On both stations, TLS traffic was intercepted using a testing proxy.

Testing was conducted in accordance with the contract for a **High-level** attacker profile, which assumes: full control of the client execution environment — the TOE operates in an **unsupervised** setting, with the end user completing the process alone from their own browser; **cooperative subjects**, meaning volunteers willing and able to provide any and all facial biometric samples, including high-quality video; and access to state-of-the-art synthetic generation tooling (GPU deepfake, GAN, *face reenactment*, *morphing*). Privileged access to Payface's backend and insider cooperation were **not** assumed.

The test method, for each Injection Attack Instrument (IAI) species, was: build the artefact; verify environment integrity against the day's *baseline*; execute a **legitimate control transaction** using the physical camera within the same session, to establish a baseline; and then execute the attack, with successive variants until the vector was exhausted. **18 attack runs** were executed, covering **15 distinct IAI species** across the **3 distinct Injection Attack Methods (IAM)** required by Clause 8.6 (Table 4) of the standard. Elapsed time was measured during each run, split into identification and exploitation phases. All runs were executed by Victor Matuk (Antisec).

Results were displayed to the tester on the application screen itself — "**Olá, [name]! Autenticação concluída com sucesso.**" ("Hello, [name]! Authentication completed successfully.") for a successful attempt, and "**Imagem reprovada**" ("Image rejected") or "**Ambiente Suspeito**" ("Suspicious environment") for an unsuccessful attempt — and confirmed in the intercepted HTTP traffic (200 for acceptance; 500 with the corresponding reason code for rejection).

Antisec **was not able to gain a legitimate classification for any injected sample** with Payface's Fortface SDK Web 2.6.0 and its Backend v3.56.0. With 18 runs covering 15 IAI species across the 3 IAM, the number of **bypasses was zero**. The Bona Fide Presentation Classification Error Rate (**BPCER**), calculated over **302 bona fide transactions** from **42 distinct volunteers** — with an effective denominator of **300**, after two discards for non-bona-fide attempts — was **2.00%**, against the 15% target value of Annex A.

Payface's **Fortface SDK Web 2.6.0** and its **Backend v3.56.0** were tested by Antisec to the **UNE CEN/TS 18099:2024** biometric data injection attack detection standard and **met both Annex A criteria for the High (Level 3) conformance level**.

Best regards,

---

**Victor Henrique Dias Matuk**

CEO — Antisec Serviços de Informática Ltda.  
+55 (11) 91899-4624 · [matuk@antisec.com.br](mailto:matuk@antisec.com.br)

## Scope of the evaluation

- **Platform:** Web.
- **Environment evaluated:** Production — SDK Web 2.6.0 (Web Demo APP v3.56.0, Backend v3.56.0), with testing conducted on the isolated staging instance made available for the evaluation.
- **Type of evaluation:** IAD subsystem evaluation (injection detection; facial matching not evaluated).
- **Security Target:** *Security Target — Fortface Web (CEN/TS 18099), v1.1*, signed by both parties on 5 August 2026.
- **Coverage executed:** 15 species of Injection Attack Instrument (IAI) across the 3 Injection Attack Methods (IAM), totalling **18 attack types** with evidence. Full listing in the **Appendix** (page 5).
- **Bona fide metric reported:** BPCER (§9.2), target value  $\leq 15\%$ .
- **Engagement period:** 30 July to 18 August 2026.

## Results — Annex A criteria

| Criterion (Annex A)                                              | Result                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BPCER $\leq 15\%$ , with a minimum of 300 bona fide transactions | ✓ Met — <b>BPCER of 2.00%</b> . Collection of <b>302 transactions</b> from 42 distinct volunteers, all executed within the evaluated version; effective denominator of <b>300</b> after two discards for non-bona-fide attempts. The result is <b>13.00 percentage points</b> below the target value of the standard. |
| Resistance to all attacks classified at High level or below      | ✓ Met — 18 attack runs, covering 15 IAI species across the 3 IAM, <b>with no bypass</b> . There was no successful attack to be rated at any level.                                                                                                                                                                    |
| <b>Final verdict</b>                                             | <b>PASS — High Level (Level 3)</b>                                                                                                                                                                                                                                                                                    |

Both Annex A criteria of the standard were met. The listing of the runs that make up the 18 attack types is set out in the **Appendix**, on page 5. The detailed BPCER calculation and the full attack matrix are set out in the associated Technical Report (§7.4 and §7.2), with the consolidated verdict in §8.6.

## Scope and validity

- This Letter is valid exclusively for the **TOE version identified above**.
- The verdict is **final, not provisional**: no test in the matrix resulted in a failure and, consequently, **no remediation window is open** (Technical Report, §8.7). No result in this Letter is pending re-execution.
- The full Technical Report (internal/confidential use) contains the detail of every attack type tested, the vectors exercised and not exercised against each threat in the model, the treatment given to the attack rating methodology — which produces no classification in this cycle, as there was no bypass — and the evidence. Available upon request from Payface/Fortface.

### AUTHENTICITY

|                                 |                                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Letter reference                | <b>AS-IAD-2026-0001</b>                                                                                                                                                                                                      |
| Published version (EN)          | <a href="https://antisec.com.br/cartas/AS-IAD-2026-0001-en.pdf">antisec.com.br/cartas/AS-IAD-2026-0001-en.pdf</a>                                                                                                            |
| Portuguese version              | <a href="https://antisec.com.br/cartas/AS-IAD-2026-0001-pt.pdf">antisec.com.br/cartas/AS-IAD-2026-0001-pt.pdf</a>                                                                                                            |
| Associated technical report     | ANTISEC-IAD-FORTFACE-WEB-2026-af222402db, v1.0                                                                                                                                                                               |
| SHA-256 of the Technical Report | <b>fbf2238937262b521f8b9386e1ba6ffa356e9b13a0ca707eb68a6948b88deb91</b><br>Computed over the signed PDF of the Technical Report, version 1.0, issued on 18 August 2026.<br>Any change to the Report yields a different hash. |
| Digital signature               | PDF signed with the e-CNPJ (ICP-Brasil) certificate of Antisec Serviços de Informática Ltda. — verifiable in Adobe Acrobat Reader and at <a href="https://validar.it.gov.br">validar.it.gov.br</a>                           |

## Appendix — Attack coverage executed

One line per species of Injection Attack Instrument. The numbering follows the execution matrix of the Technical Report (§7.2); species exercised through more than one IAM appear once, with the methods executed shown in the corresponding column. Identification and exploitation times, variants exercised and evidence are set out exclusively in the Technical Report.

| #               | Species of Injection Attack Instrument (IAI)                                | IAM executed                      | Result  |
|-----------------|-----------------------------------------------------------------------------|-----------------------------------|---------|
| 1               | Static photograph (single portrait)                                         | A — virtual camera<br>B — hooking | Blocked |
| 2               | Pre-recorded video of the subject, unaltered                                | A — virtual camera                | Blocked |
| 3               | Video of the subject with synthetic variation (noise, exposure, frame rate) | A — virtual camera                | Blocked |
| 4               | Combination of multiple videos/frames of the subject                        | A — virtual camera                | Blocked |
| 5               | Morphed image (blend of two identities)                                     | A — virtual camera                | Blocked |
| 6               | Edited/cropped video                                                        | A — virtual camera                | Blocked |
| 7               | Face reenactment (animation of a static photograph)                         | A — virtual camera                | Blocked |
| 8               | Video deepfake, low quality                                                 | A — virtual camera                | Blocked |
| 9               | Video deepfake, high quality                                                | A — virtual camera                | Blocked |
| 10              | Live deepfake (generated in real time)                                      | A — virtual camera                | Blocked |
| 11              | AI-generated synthetic face (GAN), with no corresponding real person        | A — virtual camera                | Blocked |
| 12              | Previously captured sample of the subject, re-submitted                     | C — replay                        | Blocked |
| 13              | Sample of another real user                                                 | B — hooking                       | Blocked |
| 14 <sup>†</sup> | Forged context payload/metadata (device/browser spoofing)                   | B — hooking                       | Blocked |
| 15              | 2.5D/parallax synthetic animation of a static photograph                    | A — virtual camera                | Blocked |
| 16              | Static face swap (identity swap in a single portrait)                       | A — virtual camera                | Blocked |

**Consolidated coverage: 15 IAI species · 3 IAM (A — virtual camera, B — hooking, C — replay) · 18 runs, corresponding to 18 attack types with evidence · 0 bypasses**

<sup>†</sup> Complementary attack type: under Table 1 (Clause 6.2) of the standard, forged context is not a species of IAI, as it is not a biometric sample. It does not count towards the 15 species.