# KYC Webhook Verification Record

Blank working record - complete one per delivery under review

Record the authentication decision before changing application state. Use an internal delivery reference and a restricted evidence reference. Leave unresolved verification as NOT_VERIFIED.

**delivery_ref**

Internal delivery reference. Use a synthetic or access-controlled reference, not an applicant identity.

**provider_doc_version**

Provider, documentation URL, revision if supplied and access date. If no revision is shown, say so.

**body_capture_method**

Where original HTTP body bytes are captured before parsing or other transformation.

**signature_scheme**

Expected algorithm, signed material, header format and encoding from the selected provider contract.

**key_identifier_only**

Non-secret internal key label or version only. Do not copy the signing secret.

**verification_result**

PASS, FAIL or NOT_VERIFIED with a reason and the checks actually completed.

**rejection_route**

Named handler for failure or missing evidence; state whether application state remains unchanged.

**redacted_evidence_ref**

Access-controlled reference to redacted evidence. Do not paste payloads or identity documents.

**owner**

Role accountable for the verification decision and unresolved configuration questions.

PASS does not approve an applicant or establish freshness. Apply separate schema, duplicate and state-transition checks. Do not paste raw payloads, credentials or identity documents.

# Fictional V-01 / V-02 Example

Local synthetic HMAC exercise only - no provider delivery or client test

The same synthetic JSON value is represented by original and compactly reserialized bytes. The original signature matches V-01 and fails V-02. The internal key label is a placeholder, not a provider header or a secret.

| | | |
|---|---|---|
| **delivery_ref** | | |
| | **V-01:** V-01 | **V-02:** V-02 |
| **provider_doc_version** | | |
| | **V-01:** Sumsub webhook-manager; accessed 2026-10-27; revision not exposed | **V-02:** Sumsub webhook-manager; accessed 2026-10-27; revision not exposed |
| **body_capture_method** | | |
| | **V-01:** Original synthetic HTTP body bytes before JSON parsing | **V-02:** Parsed and compactly reserialized JSON; intentional negative fixture |
| **signature_scheme** | | |
| | **V-01:** HMAC_SHA256_HEX; hex digest over body bytes; local fixture only | **V-02:** HMAC_SHA256_HEX; hex digest over body bytes; local fixture only |
| **key_identifier_only** | | |
| | **V-01:** fixture-key-01 (internal label, not a provider header) | **V-02:** fixture-key-01 (internal label, not a provider header) |
| **verification_result** | | |
| | **V-01:** PASS_LOCAL_FIXTURE: digest matches original bytes | **V-02:** FAIL_BODY_CHANGED: digest does not match original signature |
| **rejection_route** | | |
| | **V-01:** Continue to separate schema, duplicate and state-transition checks; no applicant decision | **V-02:** Reject authentication; application state unchanged; use documented response policy |
| **redacted_evidence_ref** | | |
| | **V-01:** fixture/V-01/original-bytes (synthetic local reference) | **V-02:** fixture/V-02/changed-bytes (synthetic local reference) |
| **owner** | | |
| | **V-01:** Integration engineering (fictional role) | **V-02:** Integration engineering (fictional role) |

Sources: docs.sumsub.com/docs/webhook-manager; OWASP Webhook Security Cheat Sheet. Checked October 27, 2026. Provider revisions and response policies must be reviewed for the actual integration.

Open the online template for field guidance, sources and the example CSV.