Universal Data Bridge v1.3

Regulator Verification Guide

How to independently verify automation evidence, audit logs, and cryptographic integrity.

1. Purpose of This Guide

This document enables regulators, auditors, and independent reviewers to verify that automation actions performed by Universal Data Bridge were executed as claimed, without reliance on vendor tooling or proprietary systems.

This guide assumes no prior access to internal systems.

2. Contents of an Audit Export Pack

Each audit export ZIP contains the following artifacts:

- **audit/audit.jsonl** – append-only event log of all actions
- **captures/** – screenshots or visual evidence captured during execution
- **handoff/** – pending and approved human review artifacts
- **manifest.json** – list of included files with SHA■256 hashes
- **manifest.sig** – cryptographic signature over manifest.json
- **public-key.pem** (if present) – public key used for verification
- **signing.json** – signing mode and key identifier

3. Verification Procedure Overview

Verification is performed in three independent steps: (1) integrity checking via hashes, (2) cryptographic signature verification, and (3) logical review of the event log.

No proprietary software is required.

4. Step 1 – Verify File Integrity (Hashes)

Open **manifest.json**. For each file listed, compute its SHA■256 hash using any standard cryptographic tool and confirm it matches the value in the manifest.

Example (OpenSSL):

```
openssl dgst -sha256 audit/audit.jsonl
```

If any file hash does not match, the audit pack must be considered invalid.

5. Step 2 – Verify Cryptographic Signature

The file **manifest.sig** is a signature over the raw contents of **manifest.json**. Verification ensures the manifest has not been altered and confirms the identity of the signing key.

Example (Ed25519 with OpenSSL):

```
openssl pkeyutl -verify -pubin -inkey public-key.pem -sigfile manifest.sig
-rawin -in manifest.json
```

If verification succeeds, the manifest and its listed files are cryptographically authentic.

6. Step 3 – Review Event Log Semantics

The **audit.jsonl** file is a newline■delimited JSON event stream. Each entry includes a timestamp, action type, and structured payload.

Key event types include:

- **VISION_EXTRACT** – AI-based data extraction output
- **REVIEW_POLICY_EVAL** – policy decision enforcing review
- **REVIEW_WEB_PENDING** – human approval required
- **HUMAN_APPROVED** – approval granted
- **ACTION_EXECUTED** – UI interaction performed

Reviewers should confirm that no execution events occur before required human approval when policy thresholds mandate review.

7. Interpretation Notes

- Absence of HUMAN_APPROVED where review is required indicates non-compliance.
- Presence of --no-review bypass flags should be treated as non-production usage.
- All timestamps are ISO■8601 UTC and sortable lexicographically.

8. Conclusion

By following this guide, an independent reviewer can verify that Universal Data Bridge executed automation deterministically, under policy control, with human oversight and cryptographically verifiable evidence.