Deterministic, Zero-Custody Machine-Audit Reproducibility of Bitcoin-Anchored Digital Audit Trails: A Double-Blind, HMAC-Randomized Validation Study Across a 7,239-File Multi-Entity Evidence Corpus

Ordinal 14

Regulatory Submission Software (Audit Target): AuditLog.AI

Date: December 02, 2025

Inventor and Primary Contact

Dr. Fernando Telles, BMedSc(Adv), MD(Dist)[1,2]

Position: CEO & Founder, CDA AI **Email:** Dr.Telles@aihumansynergy.org **Phone:** Provided on Request **Address:** 21 Shields St, Flemington VIC 3031, AU **Web:** www.aihumansynergy.org

Engineers

Lead Software Engineer: Dr. Jacob Yang, BEng, MEng, PhD[1] **Software Engineer:** Benjamin Hookey, BEng (Mechatronics & Robotics), FSEng[1]

Independent Investigator

Operator 2: Dr. Sam Francis MBBS, MTrauma, PhD, DPM, FFPM (Principal Investigator, Pharmaceutical Physician)

Affiliations [1] **Cardiovascular Diagnostic Audit & AI Pty Ltd (ACN 638 019 431)** – Registered Australian company conducting AuditLog.AI software development, audit and research services [2] **Telles Investments Pty Ltd (ACN 638 017 384)** – Private IP holder

IP Rights

Submitted as part of the AuditLog.AI Global Regulatory Submission Package (FDA/EMA/TGA/PCAOB/ISA Alignment)

Deterministic, Zero-Custody Machine-Audit Reproducibility of Bitcoin-Anchored Digital Audit Trails: A Double-Blind, HMAC-Randomized Validation Study Across a 7,239-File Multi-Entity Evidence Corpus

Ordinal 14

Abstract

Importance

Digital audit trails are vulnerable to content alteration, selective omission, metadata manipulation, and unverifiable reproduction. Most GxP systems rely on vendor-controlled logs rather than cryptographic proof. A zero-custody, Bitcoin-anchored, deterministic machine-audit framework that demonstrates proof-of-unchanged for regulatory-grade evidence has not previously been shown.

Objective

To evaluate the reproducibility integrity of AuditLog.AI under independent, deterministic machine-audit re-execution using Sentinel QMS v4 by: **1)** Reproducing all dual-hash outputs (SHA-256 and RIPEMD-160(SHA-256)) for 16 historical regulatory runs, and **2)** Detecting both expert-designed and HMAC-randomized negative controls across single-entity and multi-entity blinded evidence streams.

Design, Setting, and Participants

Single-site, dual-operator deterministic machine audits were conducted under full-screen capture with pre-audit evidence freezing and Bitcoin anchoring of pre- and post-audit states. All audits were executed on an independent QMS environment with newly installed tools using macOS at CDA-AI Headquarters (Melbourne, Australia) between 18 and 01 December 2025. The primary corpus comprised **1,087** original files across **16 AuditLog.AI sessions** (REGULATORY-RUN001–016), including FDA/EMA/TGA reference sets, session logs, and Ordinals 11–13 evidence bundles. For Stage IIIB, this was extended with a blinded multi-entity corpus of **6,152** files (SENTINFRA, METAVAL, and corporate/trust evidence), yielding an aggregate of **21,717** files across **6 QMS sessions**.

Exposures (Interventions)

Stage I — Amplify stress test (QMS RUN001–002). Deterministic re-execution of frozen positive-control sets (Ordinals 11–13; regulatory references; session logs v4001–v4071) using Sentinel QMS utilities. All inputs were frozen and anchored as pre-audit evidence (RUN001), then re-processed and re-anchored as audit outputs (RUN002).

Stage II — Deterministic re-audit of the complete AuditLog.AI corpus (QMS RUN003–004). QMS scripts (`qms_prepare_manifests_v4.py` , `qms_prepare_evidence_v4.py` , `qms_prefix_evidence_v4.py`) cloned manifests and frozen evidence into QMS run roots, preserving bytes and directory structure. The cloned corpus was re-hashed with `batch_dualhasher_multi_v3.3.py` , compared to original manifests using `qms_compare_manifests_v4.py` , and both pre-audit state (RUN003) and audit results (RUN004) were anchored to Bitcoin.

Stage IIIA — Human-designed adversarial tamper challenge (QMS RUN005–009). A qualified medical investigator (Operator 1) introduced **34 randomly selected negative controls** across 16 regulatory runs, using pre-specified challenges: micro-edits to numerical results, document-level changes (PDF/DOCX), file deletions, spurious insertions, file swaps, and metadata-only edits; three filename-only changes served as controls. All tampering was performed on an unprotected working copy under continuous full-screen capture, with the original frozen corpus preserved. The QMS pipeline re-hashed and compared tampered versus baseline manifests, anchoring the plan (RUN005), baseline reconstruction (RUN006), tampered corpus (RUN007), positive-control Unprotected Storage Simulation (USS) re-export (RUN008), and final QMS comparison (RUN009).

Stage IIIB — Dual-arm multi-entity blind HMAC deletion challenge (QMS RUN010–016). Stage IIIB extended testing to a **dual-arm, dual-operator, double-blind** cryptographic audit:

Arm 1 (Multi-Entity): Baseline AMP_REPRODUCIBILITY-RUN010_MULTI_BASELINE, HMAC-deleted working corpus RUN012_MULTI_HMAC_WORKING_TAMPER, and positive-control USS re-export RUN014_MULTI_PC_ReExport_USS.

Arm 2 (AuditLog.AI): Baseline AMP_REPRODUCIBILITY-RUN011_AUDITLOGAI_BASELINE, HMAC-deleted working corpus RUN013_AUDITLOGAI_HMAC_WORKING_TAMPER, and positive-control USS re-export RUN015_AUDITLOGAI_PC_ReExport_USS.

Evidence directories were first anonymized using a randomized QMS Bates-renaming procedure (`qms_bates_renamer_v4.1`), producing content-agnostic blinded identifiers to prevent targeted deletions and obscure evidence identities. A HMAC-based randomization script (`qms_hmac_salt_blinding_v4.py` ; `k_global = 20` , `max_frac_per_run = 0.10`) then generated a secret SALT and applied deletions to “WORKING_TAMPER” runs only, moving selected files into _HMAC_DELETED/ while leaving baseline QMS runs intact.

Operator 1 and a system-naive Operator 2 alternated execution across baselines, HMAC tamper runs, and positive controls. Both operators were **blinded** to the HMAC selection pattern and to file identities beyond Bates-renamed labels. All six runs were summarized in the six-way QMS comparison aggregator RUN016_AMPLIFY_QMS_AUDIT. All steps were performed under full-screen recording with audio narration and anchored session logs on an independent QMS environment.

Main Outcomes and Measures

Primary outcomes were:
1. **Dual-hash parity**, defined as exact SHA-256 and RIPEMD-160(SHA-256) concordance

between frozen originals and re-executed outputs. 2. **Negative-control detection**, defined as correct identification of all deliberately altered or deleted files with no false positives on untouched files. 3. **OP_RETURN payload and Bitcoin anchoring parity**, defined by concordant `SENTINEL|TYPE|ripemd160|sha8` payloads, TXIDs, and block heights between user-side and AMPLIFY ledgers. 4. **Human verification audit time**, constrained by pre-registered checklists and Bitcoin-anchored metadata.

Results

Stage I (Amplify stress test).
A total of **12,945 files (59 GB)** were processed, with a PRE→POST dual-hash execution interval of **58 seconds and 100.0% dual-hash parity** between original and re-executed outputs. RUN-001 and RUN002 were successfully anchored on Bitcoin (TXIDs `3e9a4db08c6badf62eff-b497b6ada36f5b27b30c5a3f954fd96073d7714792c4` and `9c2eb239046535b65ff14f0fea7dde5b-c7899d913ae9e24ad33069961305d156`; blocks 923818 and 923939).

Stage II (Deterministic re-audit of the complete corpus).
Across 16 regulatory runs, **1,087/1,087 files (100.0%)** were reproduced with matching SHA-256 and RIPEMD-160(SHA-256) hashes (`rows_unmatched_total = 0`). RUN003 and RUN004 were anchored with OP_RETURN payloads conformant to SENTINEL v4 schema (TXIDs `9721d68449ce57b9ba0d25ff86bc50d57eeac5c132156ff922026e47b66af8f7` and `4873e651228ed6374801b52d1c5723b7bf95b7ef66c330e6d5e0772b7c793e9e`; blocks 924058 and 924061).

Stage IIIA (Human adversarial tamper challlenge).
Across all tamper categories (content edits, deletions, insertions, swaps, metadata tampering), **34/34 negatively control files (100.0%) were detected** as mismatches. All **1,053/1,053** untouched files and three filename-only controls retained full dual-hash parity (**0 false positives**). RUN005–RUN009 were successfully anchored (TXIDs `d1d78c40ff7a8907b022cbcc1d5005bf0b-d889622f9620169438326edd007682` – `9de8e1d1ac4313e1dbb43afaff205d99beaf6a38e20c0bb83371ccf9a3111d73`; blocks 924781 – 924793).

Stage IIIB (dual-arm, HMAC-randomized machine-audit challenge).
In Stage IIIB we extended the Sentinel QMS v4 pipeline to a double-blind, dual-arm HMAC deletion challenge spanning six QMS runs (RUN010–RUN015). A frozen Multi-Entity corpus (6,152 evidence files) and the AuditLog.AI regulatory corpus (1,087 files) were each (i) re-hashed as blinded baselines, (ii) cloned to external User Simulation Storage (USS) as positive controls, and (iii) cloned again to working copies in which a secret HMAC SALT randomly deleted 20 Bates-labelled files per arm (k=20; max-fraction-per-run 0.10). Across all six Stage IIIB runs this produced **21,717 evidence-file instances** (7,239 unique files × 3 passes). Sentinel QMS v4 detected **40/40 (100.0%)** HMAC-selected deletions at the dual-hash level (SHA-256 and RIPEMD-160(SHA-256)) with **0/21,677** false-positive mismatches. Human verification, constrained by pre-registered checklists and Bitcoin-anchored metadata, required a total of **5,258 seconds** (≈87.6 minutes) to exhaustively verify all Stage IIIB outputs, corresponding to a mean **0.24 seconds of human time per evidence file** (0.62 s/file in tamper runs, 0.05 s/file in

baseline + positive-control runs). The six-way QMS aggregator (RUN016) reproducibly summarized this pattern on an independent QMS environment, and all Stage IIIB runs were anchored on Bitcoin (TXIDs `5b0fdf19a0c2a9813079a1b73c30a4fda4c0fda85844a7de6d6398fda254dce0` – `0915251fd7130ebd4f568574b9f6c4824e530dc74e9413c90a20a96e15313262`; blocks 925776 – 925812).

Conclusions and Relevance

Across four Stages (I–IIIB), AuditLog.AI and Sentinel QMS v4 reproducibly re-executed frozen regulatory evidence under adversarial and cross-platform constraints, with **100% dual-hash parity for all PASS baselines and positive controls**, **100% sensitivity to HMAC-randomized deletions**, and **no false-positive digest mismatches** across 21,717 Stage IIIB evidence comparisons. The combination of (i) deterministic dual-hash manifests, (ii) blinded Bates identifiers, (iii) explicit HMAC-driven non-compliance challenges, and (iv) tightly logged Human Verification Time (HVT) per evidence file demonstrates that modern digital audit trails can support CRO-grade reproducibility and machine-auditability without sacrificing human interpretability. These findings suggest a practical template for regulators and sponsors seeking verifiable evidence integrity, reproducible AI-assisted auditing, and auditable human-in-the-loop QA at scale.

Stage IIIB — Human Verification Time (HVT)

Per-run HVT is expressed as **seconds of human verification per evidence file** (Δ / N). Baseline and positive-control runs are expected to pass; tamper runs are expected to fail with exactly 20 HMAC-selected deletions per arm.

RUN ID	Auditor	HV Start (UTC)	HV End (UTC)	Δ (s)	N (files)	HVT (s/file)
RUN010 (MULTI BASELINE)	Dr. Fernando Telles	2025-11-30T02:30:13Z	2025-11-30T02:33:09Z	175	6,152	0.03
RUN011 (AUDIT-LOGAI BASELINE)	Dr. Sam Francis	2025-11-30T02:35:09Z	2025-11-30T02:38:45Z	216	1,087	0.20
RUN014 (MULTI PC USS)	Dr. Sam Francis	2025-11-30T05:14:38Z	2025-11-30T05:17:28Z	170	6,152	0.03
RUN015 (AUDIT-LOGAI PC USS)	Dr. Fernando Telles	2025-11-30T04:14:26Z	2025-11-30T04:18:06Z	220	1,087	0.20
Baseline + PC Total				**781**	**14,478**	**0.05**
RUN012 (MULTI HMAC TAMPER)	Dr. Fernando Telles	2025-11-30T02:43:40Z	2025-11-30T03:29:16Z	2,736	6,152	0.44
RUN013 (AUDIT-LOGAI HMAC TAMPER)	Dr. Sam Francis	2025-11-30T05:20:00Z	2025-11-30T05:49:01Z	1,741	1,087	1.60
Tamper Challenge Total				**4,477**	**7,239**	**0.62**
Combined Total				**5,258**	**21,717**	**0.24**

Stage IIIB — Double-Blind, HMAC-Randomized Machine-Audit Design

Central flow of the dual-arm, dual-operator Stage IIIB protocol. Multi-Entity and AuditLog.AI frozen evidence corpus are cloned to Baselines and Bates-renamed, branched into external USS export and HMAC-deleted working corpora, then re-executed in a clean-slate, logically isolated Sentinel QMS v4 environment and aggregated under `AMP_REPRODUCIBILITY–RUN016_AMPLIFY_QMS_AUDIT`.

1 FROZEN EVIDENCE CORPUS → BYTE-IDENTICAL COPIED → CLEAN QMS V4 ENVIRONMENT

Historical regulatory evidence already frozen, dual-hashed, Bitcoin-anchored, is cloned from frozen source into a clean-slate Sentinel QMS v4 environment for deterministic machine-audit.

Multi-Entity Corpus
Pre-blinded (layer 1) under `Sentinel.QMS.v4.MultiEntityAnchor` and then joined to Stage IIIB.
CDAAI- · LTPTY- · TINV- · TFT- · LTSFBTC- · LCC- | plus SENTINFRA · METAVAL

N = 6,152 (5.99GB) EVIDENCE FILES (MULTI-ENTITY)

AuditLog.AI Corpus
User-simulation evidence and regulatory sessions from `AuditLogAI.REG.GlobalSubmission.v4`.
Sessions v4001–v4071 (REGULATORY-RUN001–REGULATORY-RUN016)

N = 1,087 (10.4GB) EVIDENCE FILES BLINDED PER STAGE IIIB AUDIT DESIGN

2 DOUBLE-BLIND, HMAC-RANDOMIZED TWO-ARM CHALLENGE

After Bates renaming, each baseline branches to a USS baseline and an HMAC tamper copy. Operators alternate runs and are blinded to identities and HMAC deletions.

Multi-Entity Arm

SENTINFRA · METAVAL · CORPORATE/TRUST

RUN010 — MULTI_BASELINE
Blinded baseline in QMS v4 (Bates IDs applied).
BASELINE · OPERATOR 1

BRANCH: USS & WORKING COPY

RUN012 — MULTI_HMAC_TAMPER
HMAC SALT randomly deletes a bounded fraction of Bates files into `_HMAC_DELETED/`.
HMAC TAMPER · OPERATOR 1 · _HMAC_DELETED/

RUN014 — MULTI_PC_USS
External USS baseline re-imported and re-hashed as positive control (no intentional tamper).
POSITIVE CONTROL · OPERATOR 2

Bates Renaming

All file and directory names are converted to randomized Bates IDs; operators see only anonymized labels.

HMAC SALT

A secret SALT selects files and deletes them in working tamper runs only; pattern is hidden from both operators.

Clean QMS v4 Environment

All Stage IIIB runs execute in a logically isolated, zero-custody QMS v4 environment on the same macOS workstation.

AuditLog.AI Arm

USER SIMULATION CORPUS

RUN011 — AUDITLOGAI_BASELINE
Blinded baseline in QMS v4 (deduped manifests, Bates IDs applied).
BASELINE · OPERATOR 2

BRANCH: USS & WORKING COPY

RUN013 — AUDITLOGAI_HMAC_TAMPER
HMAC SALT deletes a blinded subset of Bates files; deletions tracked in `_HMAC_DELETED/`.
HMAC TAMPER · OPERATOR 2 · _HMAC_DELETED/

RUN015 — AUDITLOGAI_PC_USS
AuditLog.AI USS baseline re-exported and re-hashed as positive control (no intentional tamper).
POSITIVE CONTROL · OPERATOR 1

3 RUN016 — DETERMINISTIC MACHINE-AUDIT AGGREGATOR

All six Stage IIIB runs (two baselines, two HMAC tampers, two USS positive controls) are compared under `AMP_REPRODUCIBILITY–RUN016_AMPLIFY_QMS_AUDIT`. Each sub-comparison produces deterministic parity outputs; HMAC deletions surface as digest mismatches only in working tamper runs.

Six-of-Six QMS Comparisons
Alternating-operator sequence using the same QMS compare pipeline in the clean QMS v4 environment.
Runs: `010` · `011` · **`012`** · **`013`** · `014` · `015`

Dual-hash parity baselines + PCs · **Tamper detected** in RUN012 & RUN013

QMSv4 Detection Pattern (Stage IIIB)

Result: 100% detection, 0 false positives.

Files audited: **21,717** evidence-file instances (7,239 unique files × 3 passes).

- Multi-Entity deletions: **20/20** detected
- AuditLog.AI deletions: **20/20** detected
- Untouched files: **0/21,677** false-positive mismatches

PRE and POST states for RUN010–RUN016 are independently anchored to Bitcoin (OP_RETURN payloads and TXIDs described in the main text and anchoring figure).

Human Verification Layer (post-QMS). Deterministic QMS comparators output structured mismatch and PASS tables as `pre_HV_*.md`. Human auditors then verify each QMS-identified mismatch using timestamped HV START/END PDFs and metadata generators (`qms_pre_hv_report_v4.py`, `qms_hv_start_pdf_v4.py`, `qms_hv_metadata_v4.py`), yielding a total Human Verification Time (HVT) of **5,258 s** (~**87.6 min**) across **21,717** files, equating to **0.24 s/file** (**0.62 s/file** in tamper runs; **0.05 s/file** in baselines + positive controls). This human-verification layer does not alter the deterministic machine-audit outputs of RUN016.

Cental Figure. Stage IIIB Double-Blind, HMAC-Randomized Machine-Audit and Human-Verification Workflow.

This figure summarizes the Sentinel QMS v4 Stage IIIB protocol evaluating the reproducibility of the AuditLog.AI and Multi-Entity evidence corpora under a dual-arm, dual-operator, double-blind HMAC deletion challenge.

Panel 1 shows preparation of a clean QMS environment: frozen, Bitcoin-anchored regulatory evidence is cloned into an isolated workspace and blinded using randomized Bates identifiers.

Panel 2 depicts branching of each baseline run into a USS positive-control copy and an HMAC-deleted working copy, with operators alternating arms while remaining blinded to identities and deletion patterns.

Panel 3 shows the deterministic machine-audit aggregator (RUN016), which compares all six Stage IIIB runs using identical QMS comparison logic, yielding dual-hash parity for baselines and positive controls, and detecting HMAC-selected deletions only in working-tamper runs.

A downstream **Human Verification Layer (HVT)** confirms each QMS-identified mismatch using timestamped START/END audit metadata; this layer validates but does not modify machine-audit results.

Stage IIIB Human-Verification Artifacts and Dual-Hash Digests

This table lists the human-verified QMSv4 human-verification (HV) PDFs for each Stage IIIB run and their associated dual-hash digests. For each QMSv4 RUN ID, the table records:

- the **auditor** who performed the HV step, and
- the SHA-256 and RIPEMD-160(SHA-256) digests of the final, human-annotated HV PDF.

These PDFs contain the signed pre_HV_*.md tables, initials for each verified mismatch, and final signatures/time-stamps for HV START and HV END. The same digests appear in the corresponding HV metadata JSON files (HV_METADATA_QMS_COMPARE_*.json) and in the QMSv4 session logs, allowing any third party to:

1. recompute the digests from the archived PDFs and confirm bit-level integrity; and
2. re-derive the Human Verification Time (HVT) per run from the recorded START/END times.

This table therefore provides the **cryptographic evidence** for the HVT metrics reported in Stage IIIB (0.62 s/file for tamper runs, 0.05 s/file for baselines and positive controls, 0.24 s/file overall).

QMSv4 RUN ID	Auditor	Human-Verified PDF SHA-256	Human-Verified PDF RIPEMD-160
RUN010_MULTI_BASELINE	Dr Fernando Telles	eb67cafa27277b45d1e84692dbe2dfcc3a977ab223113e10baae95c8d815baa5	1de0e8bb30ad3bfe8139e46edf20b5336637bd1c
RUN011_AUDITLOGAI_BASELINE	Dr Sam Francis	7dc86eba2e283c56f5ed1a5a06039918fcdb1b8759132e1743bd89ea4ea0c0f8	5e72d5d8228afab4cbd8582d18286cab2b0cd55a
RUN012_MULTI_HMAC_WORKING_TAMPER	Dr Fernando Telles	5ce6f2fad142ce844413702171458d3745d158e4c9274d5867af07bb1bb6cc2f	964db5e7151a540a7811c1c825863ffa3d947734
RUN013_AUDITLOGAI_HMAC_WORKING_TAMPER	Dr Sam Francis	8bab2e7ccfdb4ff7c86e6aba4fbfddba5c4714357d4971b93f8f3183afd209fc	e99ec1af9464a5175fd44b88d8ffafdcced092f7
RUN014_MULTI_PC_ReExport_USS	Dr Sam Francis	cf60696770e5f9d774f48c2b007281adf43f6535cdc5e8b56c2daae38b338df6	4a88f82e5089e344bc78260740f18163bf943028
RUN015_AUDITLOGAI_PC_ReExport_USS	Dr Fernando Telles	4d0d30e19c674fc1684f7a2f1be8e151183d91f18302802d7b56de549cd4f7e0	39a4c5446764ab7eb9d4a86ba1493a670ab9f1a2

Bitcoin Anchors – Sentinel QMS v4 Reproducibility Study (Ordinal 14)

This section lists representative anchoring events from the AMPLIFY ledger for the QMS v4 Stages I–IIIB described in the abstract. (All TXIDs reference public Bitcoin mainnet confirmations logged in the AMPLIFY ledger; payloads follow SENTINEL OP_RETURN schema: SENTINELI SESSIONIripemd160Isha8.)

Stage I (RUN001–002 – Amplify Stress Test)

RUN001 (Sentinel.QMS.v4.Amplify.REPRODUCIBILITY.001)

TXID: `3e9a4db08c6badf62effb497b6ada36f5b27b30c5a3f954fd96073d7714792c4`
Block: 923818
Payload: `SENTINEL|SESSION|ddbdb990cd4b0dc81439574184da367518f39a75|9f3c43d8`

RUN002 (Sentinel.QMS.v4.Amplify.REPRODUCIBILITY.005)

TXID: `9c2eb239046535b65ff14f0fea7dde5bc7899d913ae9e24ad33069961305d156`
Block: 923939
Payload: `SENTINEL|SESSION|99d34e624d3c105aec61a35dfefae71a1b2240ae|caa24427`

Stage II (RUN003–004 – Deterministic Re-Audit)

RUN003 (Sentinel.QMS.v4.Amplify.REPRODUCIBILITY.009)

TXID: `9721d68449ce57b9ba0d25ff86bc50d57eeac5c132156ff922026e47b66af8f7`
Block: 924058
Payload: `SENTINEL|SESSION|be31ff46db2b5ddc4fdbe2f299d38f0d56f71c02|d2fcccb1`

RUN004 (Sentinel.QMS.v4.Amplify.REPRODUCIBILITY.013)

TXID: `4873e651228ed6374801b52d1c5723b7bf95b7ef66c330e6d5e0772b7c793e9e`
Block: 924061
Payload: `SENTINEL|SESSION|98404a94fb61ef21f1277f499fa7130371c6f5c7|434a3c0b`

Stage IIIA (RUN005–009 – Randomized Adversarial Tamper Challenge)

RUN005 (Sentinel.QMS.v4.Amplify.REPRODUCIBILITY.017)

TXID: `d1d78c40ff7a8907b022cbcc1d5005bf0bd889622f9620169438326edd007682`
Block: 924781
Payload: `SENTINEL|SESSION|47c4d5159a6a62eb80096c8b73e3c7f41db51a01|f6b3fe8a`

RUN006 (Sentinel.QMS.v4.Amplify.REPRODUCIBILITY.021)

TXID: `04e9e36906bfbc84b4e33be49c572aec69ef102c6a0027c9becff0411091164e`
Block: 924784
Payload: `SENTINEL|SESSION|f136f13e24c879eff1ccfdbecfb8aa2aa870efcb|c3d2044a`

RUN007 (Sentinel.QMS.v4.Amplify.REPRODUCIBILITY.025)

TXID: `2771f59341767eadd54660d46f2cc125ce966cc502b5c133b7d14a6bad5a18d6`
Block: 924791
Payload: `SENTINEL|SESSION|eedf994da253366d5c9b1b3abec344fa6e763b37|fc3ce368`

RUN008 (Sentinel.QMS.v4.Amplify.REPRODUCIBILITY.029)

TXID: `6a5ce85f88519b64942c4278537c677dfdd1359b20220a58c25629260394d9c9`
Block: 924792
Payload: `SENTINEL|SESSION|02fee7bf9c5069e15711b52f201f8143e039ae02|aef7c0a9`

RUN009 (Sentinel.QMS.v4.Amplify.REPRODUCIBILITY.033)

TXID: `9de8e1d1ac4313e1dbb43afaff205d99beaf6a38e20c0bb83371ccf9a3111d73`
Block: 924793 **Payload:** `SENTINEL|SESSION|0521313f7fc323d51fb68f2134974acf9371bb81|3b50396d`

Stage IIIB (RUN010–016 – Dual-arm Blind HMAC challenge)

Multi-Entity Baseline Corpus Anchor (Sentinel.QMS.v4.MultiEntityAnchor.001)

This anchor attests to the existence and integrity of the Multi-Entity evidence corpus used in RUN010–RUN016. **TXID:** `6e3f074462fe12b331250e982068265c74303677dfa688c3d660b-ca66b1c3e7f`
Block: 925073
Payload: `SENTINEL|SESSION|158fdb62a83f78bd48017266bb8266789ef97729|ece96f13`

RUN010 (Sentinel.QMS.v4.Amplify.REPRODUCIBILITY.037)

TXID: `5b0fdf19a0c2a9813079a1b73c30a4fda4c0fda85844a7de6d6398fda254dce0`
Block: 925776
Payload: `SENTINEL|SESSION|f1c2b10af79f185616bea2ff183d68f593f233aa|9d5508aa`

RUN011 (Sentinel.QMS.v4.Amplify.REPRODUCIBILITY.041)

TXID: `48f8b6a07af856007a5a8dd66cce205e40e52a6c418e0c440c1cea6776799ddc`
Block: 925782
Payload: `SENTINEL|SESSION|26e4d77bbd914d5ad6e331f33ea27812111c7cc1|0899e329`

RUN012 (Sentinel.QMS.v4.Amplify.REPRODUCIBILITY.045)

TXID: `4fec07d96ecdb7e8a733f1c8dccd59f8ca95455fd79e34d56a59029e7ee10ad0`
Block: 925784
Payload: `SENTINEL|SESSION|c85d4d886ef4c32ad069a58c15d9748a11072d65|840e6f7b`

RUN013 (Sentinel.QMS.v4.Amplify.REPRODUCIBILITY.049)

TXID: `2f5682c49c90cf144c1f8c1566d723933967540faf9973b6cc33122c7ea81eac`
Block: 925786
Payload: `SENTINEL|SESSION|16a43d8320fec3f071b542526b6ad43ffd3a2943|34506146`

RUN014 (Sentinel.QMS.v4.Amplify.REPRODUCIBILITY.053)

TXID: `b29e56dbe9a9a5e7bd1a24eae7f469569ba1ffd7eac144f8f6a8967ba145c93a`
Block: 925787
Payload: `SENTINEL|SESSION|6b4cdfcb67a3e0fcd67e35f418357f497c519dd8|413e776e`

RUN015 (Sentinel.QMS.v4.Amplify.REPRODUCIBILITY.057)

TXID: `d84fc66bb825561157124aafa2bda4a02f06051da9161fc6017a0c8120d61a84`
Block: 925802
Payload: `SENTINEL|SESSION|3ab1936d68859bacc680e4c193dfe7470cb82e06|dfb52fa3`

RUN016 (Sentinel.QMS.v4.Amplify.REPRODUCIBILITY.061)

TXID: `0915251fd7130ebd4f568574b9f6c4824e530dc74e9413c90a20a96e15313262`
Block: 925812
Payload: `SENTINEL|SESSION|c1058654ce59718fa6deaee28cbe2161198bbbc2|564b25c2`

All anchors listed above were broadcast and confirmed prior to Ordinal 14. Ordinal 14 references these TXIDs as immutable proof-of-execution