

AttestLayer

08 - Verification Instructions

Package: BRP-SAMPLE-2026-08-0001-F1 **Generated at:** 2026-08-12T12:05:00Z

Package identifier: BRP-SAMPLE-2026-08-0001-F1

1. In 06-canonical-manifest.json, inspect files. For every entry, hash the archive member named by path; its SHA-256 and byte length must equal sha256 and size_bytes, and role must be package_payload.
2. Confirm 06-canonical-manifest.json is canonical JSON. Hash its exact bytes and compare the result with manifest_sha256 in 07-signed-receipt.json.
3. Confirm package_identifier, package_stage, profile_identifier, and generated_at agree between 06-canonical-manifest.json and 07-signed-receipt.json. Every package PDF footer repeats package_identifier, the YYYY-MM-DD portion of generated_at, and Page N of M.
4. In 07-signed-receipt.json, remove signature, canonicalize the remaining object with JCS, and verify signature.value with Ed25519. Use the separately published issuer key identified by receipt key_id and manifest issuer_key_id (attestlayer-brp-sample-2026-08-0001).
5. In 09-checksums.txt, each line is SHA-256, two spaces, and an archive path. It covers every payload plus 06-canonical-manifest.json and 07-signed-receipt.json; it intentionally does not list itself.

Offline verification: extract the ZIP, open verifier/index.html, select the complete extracted package directory, and select a separately obtained AttestLayer issuer JWKS. A key inside the package cannot establish trust.

Hosted verification: <https://verify.attestlayer.com/>