Evidence Pack Index (Trust Hub)

Procurement-friendly map of what is public vs. available upon request — with a minimal-PII evidence request pattern.

Document ID: MVG-TRUST-EVIDENCE-INDEX-1.0.2

Version: 1.0.2

Effective date: 2026-02-10

Status: Public

Formats: PDF (controlling) • DOCX (convenience)

Classification: Trust documentation (public-safe; request-based links)

Primary contact: procurement@meridianverity.com (procurement / evidence requests)

Security contact: security@meridianverity.com

1. Purpose

This index helps reviewers quickly find evidence artifacts that can be replay-verified (public) and understand which items are available upon request under confidentiality controls.

Public artifacts are designed to be independently verifiable (e.g., hashes + signatures). Request-only artifacts are gated to protect security, confidentiality, and intellectual property.

2. Public artifacts (typical)

- /trust — Trust hub (links to public artifacts and verification entry points).
- /verify — Offline verifier (browser-run; no uploads).
- /downloads — Public-safe downloads (sample conformance pack, manifests, SBOMs, keys, briefs).
- /legal — Procurement-oriented public policies (Terms, Privacy, DPA, Subprocessors, Cookies, Security Disclosure).
- Signed Artifacts Manifest (SHA-256 inventory) and Release Signature (DSSE envelope).
- SBOM(s) for verifier assets (e.g., CycloneDX).
- Verifier trust anchors / key registry snapshot (public-safe).
- Public-safe Sample Conformance Pack (.zip) and FAIL test vector (tampered pack).
- Selected public drafts (when published) with DOIs.

3. Available upon request (NDA-gated where appropriate)

Depending on scope and eligibility, MVG may provide:

- Public Sector Addendum (negotiation template) and clause matrix (request-based; not publicly posted).
- ACR/VPAT-style accessibility report scoped to a specific version and surface.
- Authoritative Subprocessor List for the relevant service/region (varies by product and deployment).
- Security & assurance artifacts (redacted pen-test summaries / third-party letters if/when available).
- Customer-specific audit-by-evidence plan, incident reporting procedures, and evidence acceptance criteria for your control point.
- Evaluation materials under NDA (e.g., deeper conformance packs, acceptance tests, SDK/CLI documentation).
- Patents/claim materials that are non-public (made available only under request/NDA, where appropriate).

4. Restricted (generally not provided publicly)

- Unpublished patent claims and prosecution strategy details (shared only under strict controls, if at all).
- Vulnerability details before coordinated remediation/disclosure.
- Trade-secret implementation details that would materially increase security risk.
- Third-party confidential reports that we are not authorized to share.

5. Request procedure (email and web form)

Primary routing (recommended):

-
- Subject suggestion: “Evidence request — <Org> — <Scope>”

Procurement-friendly web form pattern (no form vendor; minimal PII):

- Publish: /trust/evidence
- Provide a “Request artifacts” form that generates a ready-to-send email draft (mailto) — no backend required.
- Required fields: (1) work email, (2) artifact categories requested.
- Optional fields: organization, reviewer role, region, NDA required (Y/N), deadline, short context.
- Hard rule: no attachments; do not include sensitive personal data.

Privacy/retention alignment:

- State clearly: “We don’t track you. The form generates an email draft on your device.”
- Link to /legal/retention and use the same retention language for evidence request communications.
- If you later add a server-side intake endpoint, limit logs and retain them only as described in /legal/retention.

6. Minimum information to include (to accelerate turnaround)

- Your organization and reviewer role (security / audit / procurement / legal).
- Scope (website-only vs specific product/pilot/SDK).
- Highest-risk action surface and what evidence must prove (acceptance criteria).
- Which artifacts you need and your timeline.
- Whether NDA is required and your preferred workflow.

Security note: Do not include sensitive personal data. For vulnerabilities, use security@meridianverity.com.

7. Non-binding note

This index is informational. Availability, scope, and delivery format depend on product surface, region, and security constraints. Binding terms are set only in signed agreements. This index does not grant any license to patents, copyrights, or other intellectual property; licenses are granted only in executed agreements.

Change log

- v1.0.2 — Tightened wording for public posting; clarified IP/license boundary; standardized PDF/DOCX roles.
- v1.0.1 — Added website request-form pattern (minimal PII) + explicit retention alignment guidance.
- v1.0.0 — Initial publication.