**MCPX‑KendoBridge — Evidence Pack Specification & Checklist**

**Document:** docs/12\_evidence\_pack.docx  
**Project Code:** MCPX‑KendoBridge  
**Version:** 2.0.0 (Kendo Migration)  
**Last Updated:** 2025‑09‑27  
**Owner:** DoSE (Accountable) — DocFactory (Author/Responsible) — SRE Lead, QA Lead, SecLead, DBA (Consulted)

**Purpose.** Define **what evidence to collect, how to package it, and where to store it** for each release across **Alpha → Beta → RTM → Prod**. The pack proves conformance to gates (Build/Tests, OpenAPI lint/diff, CodeQL, Dependency Review, Secret Scanning, SBOM), **SSE streaming budgets** (TTFB), **RTM parity** on **Prod DB (read‑only)**, and post‑release stability. Evidence is retained **≥ 1 year** under GitHub Releases (and optional external archive). This follows Technijian DocFactory defaults and GitHub‑first SDLC.

**Compliance banner:** **Add‑only** schema; **Stored‑procedure‑only** DAL; **No‑Hard‑Coding** of dynamic values (child cmd/args/cwd, allowed origins, timeouts, keep‑alive) — all sourced from SQL Server AppConfig/FeatureFlag via sp\_Config\_GetValue, sp\_Config\_GetAll, sp\_Feature\_IsEnabled, sp\_Lookup\_Get. **Secrets** (SQL connection strings, Telerik license) **never** appear in evidence. Configure secrets exclusively in **GitHub Environments**.

**1) Scope & Goals**

* **Scope:** API (Streamable‑HTTP + SSE), Admin Portal (KendoReact Fluent v12, read‑only), DB contracts, CI/CD, monitoring.
* **Goals:** Provide **auditable, reproducible** records for every promotion (Alpha → Beta → RTM → Prod), enabling third‑party review without revealing secrets.

**2) When to Capture Evidence**

| **Stage** | **Capture Window** | **Why** |
| --- | --- | --- |
| **Alpha** | After CI gates pass and Alpha deploy completes | Prove basic health and contract correctness |
| **Beta** | After Beta deploy + perf smoke | Prove latency budgets and streaming TTFB |
| **RTM** | After RTM deploy on **Prod DB (read‑only)** | Prove parity and prevent Prod drift |
| **Prod** | (a) Immediately post‑canary; (b) **24‑hour** post‑release | Prove production stability; attach monitoring snapshot |

**3) Evidence Contents (canonical list)**

**No secrets**; only **non‑secret** artifacts and summaries.

**A. Contracts & Design**

1. **OpenAPI**: /api/openapi/mcp-proxy.yaml (exact copy)
2. **OpenAPI Lint** output (Redocly)
3. **OpenAPI Diff** vs previous tag (if applicable)
4. **Error Code Catalog** snapshot (optional PDF)
5. **UI Theme assets**: ThemeBuilder export (non‑secret) and token parity checklist

**B. Build, Tests & Security Gates**

1. **.NET build & tests**: TRX files, coverage lcov
2. **E2E/Gherkin logs**: 01–04 feature runs (session, streaming, background notification, origin denial)
3. **Accessibility**: axe smoke report for /, /sessions, /config, /access
4. **Contract tests** (TS) summary
5. **CodeQL** SARIF (C#/JS)
6. **Dependency Review** report (no **High** admitted)
7. **Secret Scanning** summary (from repo/org settings; redacted summary only)

**C. Supply Chain & Integrity**

1. **SBOM** (CycloneDX JSON)
2. **(Optional)** Build provenance / attestations (SLSA, cosign)
3. **Container image digest** used per environment

**D. Deploy, Readiness & Parity**

1. **Readiness outputs** (/ready) per environment (JSON)
2. **Health outputs** (/healthz) per environment (JSON)
3. **Config snapshots** (/config/effective) per environment (non‑secret)
4. **RTM parity check results** vs expected Prod values (diff summary)

**E. Performance & Streaming**

1. **Latency smoke**: non‑streaming p50/p95 summary (Beta, Prod)
2. **Streaming TTFB** histogram/p95 (Beta, Prod), heartbeat cadence results
3. **(Optional)** k6 outputs (JSON/HTML)

**F. Monitoring & Post‑Release (Prod)**

1. **Monitoring screenshots** (Availability, Latency, **TTFB**, Readiness) immediately post‑deploy
2. **24‑Hour post‑release** checklist results + monitoring snapshot

**G. Approvals & Change Control**

1. **Environment approvals** (Alpha → Beta → RTM → Prod) — export/PNG or PDF
2. **Release notes** with version, image digest, dates, links to CI jobs
3. **Incident/rollback records** (if any) and resolution notes

**4) Packaging & Naming**

**4.1 Release Tagging**

* **Tag format:** mcpy-<YYYYMMDD>-<seq> (e.g., mcpy-20250927-01).
* **Release title:** MCPX‑KendoBridge v2.0.0 — <environment>.
* **GitHub Release**: attach the evidence ZIP(s) and link CI runs.

**4.2 Evidence ZIP structure**

evidence/

00\_meta/

index.yaml

release.json # version, image digest, commit, tag, createdAt

01\_contracts/

openapi.yaml

openapi.lint.txt

openapi.diff.txt

error\_catalog.pdf

themebuilder\_export.zip # no secrets, non-proprietary

02\_tests/

dotnet-tests/ # TRX, coverage

e2e-gherkin/ # logs & screenshots (if any)

axe/ # a11y report

contract-tests/ # TS assertions summary

03\_security/

codeql.sarif

dependency-review.json

secret-scan-summary.txt

04\_supply\_chain/

sbom.cdx.json

provenance.json # optional attestation

image-digest.txt

05\_ops/

ready.alpha.json

ready.beta.json

ready.rtm.json

ready.prod.json

healthz.alpha.json

...

config.alpha.json

config.beta.json

config.rtm.json

config.prod.json

rtm-parity.diff.txt

06\_perf/

latency-beta.json

latency-prod.json

streaming-ttfb-beta.json

streaming-ttfb-prod.json

heartbeat-cadence-beta.json

07\_monitoring/

prod-postdeploy.png

prod-24h.png

08\_approvals/

alpha-approval.png

beta-approval.png

rtm-approval.png

prod-approval.png

09\_incidents/ # only if occurred

incident-<id>.pdf

**4.3 Index file (evidence/00\_meta/index.yaml)**

release:

tag: "mcpy-20250927-01"

version: "2.0.0"

commit: "<sha>"

image: "registry.example/mcp-proxy@sha256:<digest>"

createdAt: "2025-09-27T18:30:00Z"

retention: ">= 1 year"

artifacts:

- path: "01\_contracts/openapi.yaml"

sha256: "<...>"

rationale: "Contract of record"

- path: "03\_security/codeql.sarif"

sha256: "<...>"

rationale: "Static analysis record"

- path: "05\_ops/config.rtm.json"

sha256: "<...>"

rationale: "RTM parity (Prod DB RO)"

- path: "06\_perf/streaming-ttfb-prod.json"

sha256: "<...>"

rationale: "Streaming performance budget"

signing:

provenance: "04\_supply\_chain/provenance.json" # optional

signedBy: "build-bot@technijian"

**5) Collection Workflow (how the pack is assembled)**

* **Trigger:** Upon successful deployment to each target environment.
* **Source of truth:** CI artifacts + API snapshots.
* **Automation:**
  + CI jobs upload artifacts (tests, SBOM, OpenAPI outputs).
  + Deploy workflow runs helper scripts that call /ready, /healthz, /config/effective and save JSON.
  + Performance smoke runs capture non‑streaming latency and streaming **TTFB** + heartbeat cadence.
  + A post‑release job (Prod) captures monitoring screenshots and the **24‑hour** checklist.

These steps reflect DocFactory defaults for Evidence Packs and GitHub‑first workflows.

**6) Acceptance Criteria (evidence‑gate checklist)**

**A. CI Gates**

* Build & tests passed; TRX/coverage artifacts present
* OpenAPI lint + diff attached
* CodeQL SARIF present; no untriaged **High/Critical**
* Dependency Review passed (no **High**)
* Secret Scanning summary attached (no new leaks)
* SBOM attached (CycloneDX JSON)

**B. Deploy & Ops**

* /ready and /healthz JSON captured per environment
* /config/effective captured (non‑secret); **no secrets** present
* **RTM parity** diff attached; promotion blocked on mismatches

**C. Performance & Streaming**

* Non‑streaming latency within budgets (p50≤300 ms; p95≤800 ms)
* **Streaming TTFB p95 ≤ 200 ms**; heartbeat cadence nominal (±1s)
* Perf smoke artifacts stored (Beta, Prod)

**D. Monitoring & Post‑Release**

* Monitoring screenshots (post‑deploy and **24‑h**) attached
* Availability ≥99.9%; error rate <1%; readiness stable

**E. Approvals & Notes**

* Environment approvals (Alpha → Beta → RTM → Prod) archived
* Release notes with image digest and links to CI runs
* Incident/rollback documents attached (if any)

**7) Retention & Access**

* **Retention:** **≥ 1 year** from the Release date; recommend **18 months** for safety.
* **Primary store:** GitHub Releases attachments (immutable once finalized).
* **Optional secondary store:** Internal artifact vault (encrypted).
* **Access:** Read access for auditors, DoSE, Security, SRE, QA; write access limited to release engineers.

**8) Redaction & Privacy Rules**

* Never store **secrets** in evidence (connection strings, tokens, Telerik license).
* Logs must be scrubbed: **no request bodies**, no tokens, no license content.
* Monitoring screenshots should not include PII; use restricted dashboards.

**9) Cross‑References**

* **CI/CD Plan:** docs/10\_ci\_cd.docx — defines jobs that produce the pack.
* **Monitoring & SLOs:** docs/11\_monitoring.docx — defines SLIs/SLOs and post‑release checks.
* **Functional Requirements:** docs/05\_fr.docx — maps FRs to tests and evidence.
* **Compliance:** docs/13\_compliance.docx — secrets policy, CSP/egress, DB rules.
* **Threat Model:** docs/17\_threat\_model.docx — trust boundaries, STRIDE.

**10) Example Evidence Collector Snippets (non‑secret)**

**A. Save API snapshots (bash)**

set -euo pipefail

BASE="$1" # e.g., https://beta.example.com/api

OUT="$2" # e.g., evidence/05\_ops

mkdir -p "$OUT"

curl -fsS "$BASE/ready" > "$OUT/ready.beta.json"

curl -fsS "$BASE/healthz" > "$OUT/healthz.beta.json"

curl -fsS "$BASE/config/effective" > "$OUT/config.beta.json"

**B. Create index with SHA256 (bash)**

pushd evidence

echo "release:" > 00\_meta/index.yaml

echo " tag: \"$GITHUB\_REF\_NAME\"" >> 00\_meta/index.yaml

echo "artifacts:" >> 00\_meta/index.yaml

for f in $(find . -type f ! -path "./00\_meta/index.yaml"); do

sum=$(sha256sum "$f" | cut -d' ' -f1)

echo " - path: \"${f#./}\"" >> 00\_meta/index.yaml

echo " sha256: \"$sum\"" >> 00\_meta/index.yaml

done

echo "retention: \">= 1 year\"" >> 00\_meta/index.yaml

popd

**C. Attach to GitHub Release (gh cli)**

gh release upload "$TAG" evidence/\*\* --repo <org>/<repo>

**11) Risks & Mitigations**

| **Risk** | **Impact** | **Mitigation** |
| --- | --- | --- |
| Evidence contains secrets | Audit failure, exposure | Strict redaction rules; reviewer checklist; Secret Scanning; separate secret stores |
| Parity drift missed | Prod regressions | **RTM on Prod DB (read‑only)** parity checks block promotion |
| Missing TTFB metrics | Streaming regressions | Enforce perf smoke step and add SLIs for **TTFB** and heartbeat cadence |
| Artifact sprawl | Hard to audit | Canonical ZIP structure + index.yaml with SHA256; evidence checklist |

**12) RACI (Evidence)**

| **Activity** | **A** | **R** | **C** | **I** |
| --- | --- | --- | --- | --- |
| Define evidence scope & gates | DoSE | DocFactory | SecLead, SRE, QA, DBA | Dev |
| Collect CI artifacts | DoSE | SRE/CI | QA | All |
| Capture API snapshots | DoSE | SRE/QA | Dev | All |
| Perf & streaming evidence | DoSE | SRE | QA | Dev |
| Monitoring screenshots | DoSE | SRE | QA | All |
| Approvals & release notes | DoSE | Release Eng | SecLead | All |
| Final pack assembly & upload | DoSE | SRE/CI | DocFactory | All |

**13) Assumptions**

1. GitHub Environments are configured with approvals; **RTM** points to **Prod DB (read‑only)**.
2. CI produces artifacts listed in §3; deploy workflows can call public endpoints for snapshots.
3. No secrets are required to **read** /ready, /healthz, or /config/effective outputs (they are non‑secret).

**14) Next Steps**

* Embed the **collector snippets** in deploy workflows for each environment.
* Add index.yaml generation and SHA256 hashing to CI.
* Ensure **24‑hour post‑release** job captures monitoring snapshots and checklist outputs.

**Footer (optional for Word header/footer):**  
*MCPX‑KendoBridge • Evidence Pack • v2.0.0 • 2025‑09‑27 • Confidential — Technijian Internal*