**MCPX‑KendoBridge — Test Strategy (API, Streaming, and KendoReact UI)**

**Document:** docs/09\_test\_strategy.docx  
**Project Code:** MCPX‑KendoBridge  
**Version:** 2.0.0 (Kendo Migration)  
**Last Updated:** 2025‑09‑27  
**Owner:** QA Lead (Responsible) — DoSE (Accountable) — DocFactory (Author) — T‑Arch & SecLead (Consulted)

**Purpose.** Define an **audit‑ready** testing approach that validates MCPX‑KendoBridge across **four environments** (**Alpha → Beta → RTM → Prod**), with **RTM validating on the Prod DB (read‑only)**. The strategy covers unit, integration, contract, E2E (Gherkin), performance (including **SSE TTFB**), accessibility (**WCAG 2.2 AA / axe**), security checks, observability assertions, and Evidence Pack collection. It enforces Technijian guardrails: **GitHub‑first**, **No‑Hard‑Coding**, **Stored‑procedure‑only** DB access, **add‑only** migrations, and secrets **only** in environment stores.

**DB COMPLIANCE — applies to all tests:** Tests must **never** rely on hard‑coded dynamic values (child cmd/args, keep‑alive cadence, request timeout, Origin list). All such values are read from the API (/config/effective, /ready) which, in turn, sources **non‑secret** values from SQL Server via **SPs** (sp\_Config\_\*, sp\_Feature\_IsEnabled, sp\_Lookup\_Get). Secrets are **not** stored in DB or test fixtures.

**1) Scope & Objectives**

**In scope**

* API transport (**Streamable‑HTTP + SSE**) and **error envelope** stability.
* Sessioning (one child per Mcp‑Session‑Id), STDIO bridge, graceful drain, origin allow‑list enforcement.
* KendoReact Admin Portal (read‑only): Dashboard, Sessions (SSE), Config (non‑secret), Access Control (visibility).
* Performance budgets: non‑streaming p50≤300 ms / p95≤800 ms; **SSE TTFB p95≤200 ms** intra‑VPC.

**Out of scope**

* Editing config/feature flags via UI (UI is read‑only).
* Secrets display/logging (prohibited).

**2) References**

* **Functional Requirements:** docs/05\_fr.docx (v2.0.0)
* **UI/UX SOP:** docs/08\_ui\_ux.docx (Kendo Fluent v12 + ThemeBuilder)
* **CI/CD Plan:** docs/10\_ci\_cd.docx
* **NFRs & Monitoring:** docs/06\_nfr.docx, docs/11\_monitoring.docx
* **Error Code Catalog:** docs/error\_catalog.docx
* **OpenAPI 3.1:** /api/openapi/mcp-proxy.yaml
* **Runbooks:** deploy/rollback/incident/scale\_out
* **Evidence Pack:** docs/12\_evidence\_pack.docx (≥ 1‑year retention)

**3) Principles & Test Data Policy**

1. **Contract‑first.** Generate client types from OpenAPI; assert schema shape in tests.
2. **Environment‑aware.** Tests run against Alpha/Beta/RTM/Prod with environment‑specific base URLs and tokens provided **outside** the repo (CI secrets).
3. **No secrets.** Tests never echo tokens, credentials, or license content; logs are scrubbed.
4. **Determinism.** Use a **fake child** MCP in CI to deterministically emit notifications and error conditions.
5. **Add‑only / SP‑only.** Integration tests call **SPs** via API surfaces **only**; no inline SQL.

**4) Test Levels & Coverage Targets**

| **Level** | **Target Coverage** | **Scope** |
| --- | --- | --- |
| **Unit** (.NET) | **80%** lines, **90%** for core utils | JSON‑RPC envelope parsing, error envelope, config provider, origin validator, STDIO frame parser |
| **Integration** (.NET + DB) | Critical paths | Config provider → SPs, feature flag evaluation, readiness behavior, child spawn probe |
| **Contract** (TS) | 100% endpoints touched | OpenAPI 3.1 shape checks for /ready, /healthz, /config/effective, /mcp JSON response |
| **E2E (Gherkin)** | All FRs | 01\_session\_establish, 02\_streamed\_tool\_call, 03\_background\_notification, 04\_origin\_denied |
| **Performance** (k6) | Budgets met | Non‑streaming latency; **SSE TTFB** and heartbeat cadence; concurrency & soak |
| **Accessibility** (axe) | 0 critical | /, /sessions, /config, /access (Kendo components) |
| **Security & SCA** | Pass | CodeQL (C#/JS), Dependency Review (fail on **high**), Secret Scanning (org/repo setting) |

**5) Test Design**

**5.1 Unit Tests (xUnit / .NET 8)**

* **Error envelope**: Ensure { code, message, requestId? } returned for forced failures (e.g., disallowed Origin).
* **Origin allow‑list**: Security:AllowedOrigins enforcement; ensure no wildcard acceptance.
* **STDIO bridge**: Validate line framing, monotonic SSE id, back‑pressure handling.
* **Config provider**: Pulls values via SPs (mock DAL layer); **no literals**.

**Sample assertion (C# pseudo):**

var err = await Client.Post("/mcp", origin:"https://evil.example");

Assert.Equal(403, err.StatusCode);

Assert.Equal("origin\_forbidden", err.Body.code);

Assert.NotEmpty(err.Body.message);

Assert.Matches("^req-", err.Body.requestId);

**5.2 Integration Tests**

* **Readiness probe**: Break DB connectivity (in test env) → /ready returns 503 not\_ready.
* **SP round‑trip**: Set seed (add‑only), verify /config/effective reflects values.
* **Child spawn**: With a fake child command from DB, assert readiness covers child probe behavior.

**5.3 Contract Tests (TypeScript)**

* Generate types with openapi-typescript from /api/openapi/mcp-proxy.yaml.
* Assert shapes for /ready, /healthz, /config/effective, and JSON mode of /mcp.
* Confirm **error examples** (e.g., missing\_session\_id, feature\_disabled) match schema.

**Example (TS/Jest):**

import { paths } from './api/types';

type Ready = paths['/ready']['get']['responses']['200']['content']['application/json'];

**5.4 E2E (Gherkin)**

Use the provided features under /tests/gherkin:

1. **01\_session\_establish** — Session issuance and header echo.
2. **02\_streamed\_tool\_call** — SSE streaming with monotonic id and heartbeats; JSON fallback.
3. **03\_background\_notification** — Fan‑out across subscribers in same session.
4. **04\_origin\_denied** — 403 envelope on disallowed Origin; success on allow‑listed host.

**5.5 Accessibility (axe on KendoReact)**

* Run axe smoke on /, /sessions, /config, /access.
* Validate focus indicators (ThemeBuilder), ARIA labels on Grid, Dialog, AppBar, Drawer.
* Fail CI on **critical** violations; track minors for backlog.

**5.6 Performance & Reliability (k6)**

**Metrics:** non‑streaming latency p50/p95; **SSE TTFB** p50/p95 (≤ 200 ms, intra‑VPC); heartbeat cadence equal to Network:SseKeepAliveSeconds (±1 s).  
**Scenarios:**

* **Smoke**: 1–5 VUs, 2–3 min, confirm budgets.
* **Load**: growth to target sessions/replica; ensure CPU‑bound before memory.
* **Soak**: 30–60 min streaming, verify no drops and stable heartbeats.

**k6 pseudo‑snippet:**

import http from 'k6/http';

import { check, sleep } from 'k6';

export const options = { vus: 5, duration: '3m' };

export default function () {

const res = http.post(`${\_\_ENV.BASE}/mcp`, JSON.stringify({jsonrpc:"2.0",id:"1",method:"ping",params:{}}),

{ headers: { 'Content-Type':'application/json' }});

check(res, { '200': (r)=> r.status === 200 });

}

**6) Streaming Test Harness**

**POST /mcp (SSE):** Use fetch() streaming to parse SSE event: message frames and compute **TTFB**; verify id monotonic and heartbeat cadence.  
**GET /mcp (SSE notifications):** Use EventSource (or fetch streaming) with Mcp-Session-Id; assert fan‑out behavior.  
**Failure cases:** missing\_session\_id, feature\_disabled, origin\_forbidden → assert **error envelope** and no silent retries.

**7) Environment Matrix & Promotion Rules**

| **Env** | **Base URL** | **DB** | **Secrets Source** | **Test Focus** |
| --- | --- | --- | --- | --- |
| **Alpha** | https://alpha…/api | Alpha DB | GitHub Env: **alpha** | Functional smoke; unit/integration on PRs |
| **Beta** | https://beta…/api | Beta DB | GitHub Env: **beta** | E2E + perf smoke; a11y smoke |
| **RTM** | https://rtm…/api | **Prod DB (read‑only)** | GitHub Env: **rtm** | Parity checks; contract tests; **no writes** |
| **Prod** | https://prod…/api | Prod DB | GitHub Env: **prod** | Canary observation; 24‑h post‑release checks |

Promotion requires all **CI gates** green and **RTM parity** (config/effective snapshot) before Prod.

**8) CI Integration & Evidence**

**CI hooks (see docs/10\_ci\_cd.docx):**

* Build & Test (.NET), optional UI build (Kendo license injected at build time), OpenAPI lint/diff, CodeQL, Dependency Review, SBOM, Secret Scanning (repo setting).
* **Artifacts to Evidence Pack:** test results, OpenAPI lint/diff, SBOM, CodeQL SARIF, a11y report, monitoring snapshot, approvals (Alpha → Beta → RTM → Prod). Retain **≥ 1 year**.

**9) Defect Severity & SLA**

| **Sev** | **Definition** | **Examples** | **Target Response** |
| --- | --- | --- | --- |
| **P1** | Prod outage/critical degradation | /ready failing; TTFB p95>200 ms sustained; session loss | Page on‑call; mitigate ≤30 min |
| **P2** | Significant but limited | SSE heartbeat drift; origin regression | Acknowledge ≤15 min; fix ≤24 h |
| **P3** | Minor / cosmetic | UI content, non‑blocking a11y | Plan into sprint |

**10) Flakiness Control**

* **Retries**: Max 1 automatic retry for transient network assertions; no retry on functional failures.
* **Quarantine**: Tag flaky tests and exclude from merge‑queue gates until stabilized.
* **Observability**: Attach requestId/sessionId to failure logs; store screen recordings for UI E2E.

**11) Traceability (FR/NFR ↔ Tests)**

| **Requirement** | **Tests** |
| --- | --- |
| FR‑001 Transport (JSON/SSE) | 02\_streamed\_tool\_call, contract tests |
| FR‑002 Error Envelope | Unit (envelope), 04\_origin\_denied |
| FR‑003 Sessioning | 01\_session\_establish, 03\_background\_notification |
| FR‑004 Process Bridge | Integration + fake child |
| FR‑005 Heartbeats/TTFB | 02\_streamed\_tool\_call (perf), k6 stream |
| FR‑006 Origin Allow‑list | 04\_origin\_denied |
| FR‑007 Health/Ready | Health smokes; integration |
| FR‑008 Config Surface | Contract tests; UI page assertions |
| FR‑009 Legacy flag | Unit/integration; toggled E2E |
| FR‑010 Kendo UI | a11y smoke; contract/UI tests |
| NFR‑Perf/Avail | k6, monitoring snapshot |

**12) Roles & RACI (Testing)**

| **Activity** | **A** | **R** | **C** | **I** |
| --- | --- | --- | --- | --- |
| Test plan & maintenance | DoSE | QA Lead | T‑Arch, SecLead | Dev, SRE |
| E2E harness & SSE tests | DoSE | QA Lead | Dev Lead | SRE |
| A11y pipeline | DoSE | QA Lead | UI Lead | SRE |
| Perf/k6 | DoSE | SRE Lead | QA Lead | Dev |
| Evidence Pack | DoSE | DocFactory | QA Lead | All |

**13) Entrance / Exit Criteria**

**Entrance (per feature/PR):**

* OpenAPI updated; data contracts stable; feature toggles defined (if any).
* Test data and fake child hooks in place.

**Exit (per release):**

* All CI gates green; E2E and a11y smoke pass; perf smoke meets budgets; **RTM parity** verified; Evidence Pack assembled.

**14) Example Commands (non‑secret)**

# .NET unit/integration

dotnet test --no-build -p:CollectCoverage=true

# Generate TS types from OpenAPI

npx openapi-typescript api/openapi/mcp-proxy.yaml -o web/src/api/types.ts

# Run a11y smoke (example script)

npm --prefix web run test:a11y

# k6 smoke (example)

BASE=https://beta.example.com/api k6 run tests/perf/smoke.js

**15) Risks & Mitigations**

* **Ingress buffering SSE** → Validate deploy config; include in perf smoke; roll back on regression.
* **Feature‑flag drift** → **RTM on Prod DB (RO)** parity checks block promotion.
* **Secret leakage** → Secret Scanning + redaction rules; no payload bodies in logs.

**16) Assumptions**

1. KendoReact UI exists and is read‑only; **Telerik license** is injected at CI build only (never stored).
2. Test credentials are provisioned per environment via **GitHub Environments**, not in repo.
3. The DB remains **add‑only** with **SP‑only** access; RTM uses **Prod DB (read‑only)**.

**17) Next Steps**

* Land the SSE harness and a11y smoke in CI; generate OpenAPI types in the UI.
* Add perf smoke scripts for TTFB and heartbeat cadence.
* Expand contract tests to cover all error examples in OpenAPI and the Error Catalog.

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