**MCPX‑KendoBridge — Functional Requirements (FR)**

**Document:** docs/05\_fr.docx  
**Project Code:** MCPX‑KendoBridge (MCP Remote Proxy for Telerik KendoReact MCP STDIO)  
**Version:** 2.0.0 (Updated for Kendo migration)  
**Last Updated:** 2025‑09‑27  
**Owner:** DoSE (Accountable) — DocFactory (Author/Responsible) — T‑Arch & SecLead (Consulted)

**Purpose.** Define the **functional behavior** of MCPX‑KendoBridge across **four environments** (**Alpha → Beta → RTM → Prod**) with explicit acceptance criteria and traceability to OpenAPI, tests, and runbooks. Requirements uphold Technijian guardrails: **GitHub‑first SDLC** (merge queue + required checks), **No‑Hard‑Coding**, **Stored‑procedure‑only** database access, **add‑only** migrations, and **secrets only** in environment stores (never in code or DB).

**DB COMPLIANCE — applies to any item that touches configuration:** All dynamic values (child command/args/cwd, timeouts, keep‑alive, Origin allow‑list, feature flags) come from SQL Server **via stored procedures** (sp\_Config\_\*, sp\_Feature\_IsEnabled, sp\_Lookup\_Get). The app has **EXECUTE‑only** permissions on SPs; **no table access**. **Secrets** (SQL connection string, Telerik license) are **never** stored in code/docs/DB and are configured only in **GitHub Environments**.

**1) References**

* **OpenAPI 3.1:** /api/openapi/mcp-proxy.yaml (servers: alpha/beta/rtm/prod; bearer; stable error envelope; SSE examples).
* **Runbooks:** runbooks/deploy.docx, runbooks/rollback.docx, runbooks/incident.docx, runbooks/scale\_out.docx.
* **UI/UX:** docs/08\_ui\_ux.docx (KendoReact Fluent v12 + ThemeBuilder, WCAG 2.2 AA).
* **Test Strategy:** docs/09\_test\_strategy.docx (unit/integration/E2E, axe, contract tests).
* **Compliance & Evidence:** docs/13\_compliance.docx, docs/12\_evidence\_pack.docx.

**2) Functional Requirements (enumerated)**

Each FR includes a **code**, **statement**, **rationale**, and **acceptance criteria** (AC).  
**Traceability keys:** *OAS* (OpenAPI op), *Test* (Gherkin or unit/integration), *Runbook* (operational check).

**FR‑001 — Transport: Streamable‑HTTP with JSON or SSE**

**Statement.** The proxy SHALL expose a primary endpoint **POST /mcp** that accepts one JSON‑RPC 2.0 request and responds **either** as a single JSON body (application/json) **or** as **Server‑Sent Events** (text/event-stream) when the request includes Accept: text/event-stream. A session‑scoped SSE channel SHALL be available at **GET /mcp**.

**Rationale.** Enable incremental outputs and background notifications while remaining proxy/CDN‑friendly.

**AC.**

* AC‑001.1: POST /mcp with Accept: text/event-stream returns 200 and Content‑Type: text/event-stream with event: message frames and monotonic id. (*OAS: /mcp POST; Test: 02\_streamed\_tool\_call*)
* AC‑001.2: POST /mcp without Accept returns 200 JSON with an opaque JSON‑RPC envelope. (*OAS: /mcp POST; Test: 02\_streamed\_tool\_call*)
* AC‑001.3: GET /mcp opens an event stream for the session (see FR‑003). (*OAS: /mcp GET; Test: 01\_session\_establish*)

**FR‑002 — Error Envelope (stable)**

**Statement.** All HTTP errors MUST return a **stable error envelope**:  
{ code: string; message: string; requestId?: string }. No secrets or payload bodies are logged or returned.  
**Examples:** origin\_forbidden, missing\_session\_id, feature\_disabled, timeout. (See Error Catalog.)

**AC.**

* AC‑002.1: Disallowed Origin returns 403 with { code: "origin\_forbidden", ... }. (*OAS: 403 examples; Test: 04\_origin\_denied*)
* AC‑002.2: Missing Mcp-Session-Id on GET /mcp returns 400 with { code: "missing\_session\_id", ... }. (*OAS: 400 example added*)
* AC‑002.3: Legacy endpoints disabled return 403 feature\_disabled. (*OAS: 403 featureDisabled*)

**FR‑003 — Sessioning: one child process per Mcp‑Session‑Id**

**Statement.** The system SHALL associate each **Mcp‑Session‑Id** with exactly **one child process** (Kendo MCP via STDIO). Requests in the same session **stick** to the same replica while active, and notifications are delivered to all session subscribers.

**AC.**

* AC‑003.1: On first POST /mcp, the server issues Mcp‑Session‑Id header; subsequent calls echo the same ID. (*OAS: response headers; Test: 01\_session\_establish*)
* AC‑003.2: GET /mcp requires Mcp‑Session‑Id; absence yields 400 missing\_session\_id.
* AC‑003.3: Background notification pushed by the child reaches every open SSE subscriber for the session within 10s. (*Test: 03\_background\_notification*)

**FR‑004 — Process Bridge: spawn & route via STDIO**

**Statement.** On first request (or explicit initialize), the proxy SHALL spawn the **@progress/kendo-react-mcp** child using **DB‑sourced** command/args/cwd; forward JSON‑RPC bidirectionally over STDIO; supervise lifecycle; and terminate children on drain/shutdown. **No hard‑coded** child paths/args.

**AC.**

* AC‑004.1: Effective child configuration is **visible** (non‑secret) via /config/effective keys Mcp:ChildCommand|Args|Cwd. (*OAS: /config/effective*)
* AC‑004.2: Child PID appears in structured logs (no payload bodies).
* AC‑004.3: Readiness fails if child spawn probe fails during rollout. (*Runbook: deploy/ready*)

**FR‑005 — Streaming semantics: heartbeats & TTFB**

**Statement.** Streaming responses SHALL send **heartbeats** as : comment lines every **Network:SseKeepAliveSeconds** (DB‑sourced). **TTFB** for streamed calls SHALL be observable.

**AC.**

* AC‑005.1: Heartbeats occur at configured cadence (±1s tolerance). (*Test: 02\_streamed\_tool\_call*)
* AC‑005.2: UI exposes connection state and heartbeat age (read‑only). (*UI/UX*)
* AC‑005.3: Monitoring captures TTFB p95. (*Monitoring doc*)

**FR‑006 — Security: Origin allow‑list (DB‑driven)**

**Statement.** If an Origin header is supplied, it MUST match the **DB‑configured** allow‑list Security:AllowedOrigins, else return 403 origin\_forbidden. No wildcard origins in code.

**AC.**

* AC‑006.1: POST /mcp with Origin: https://evil.example returns 403 envelope. (*Test: 04\_origin\_denied*)
* AC‑006.2: Allow‑listed origin succeeds and returns JSON or SSE as requested.
* AC‑006.3: Allow‑list values are visible (non‑secret) via /config/effective. (*OAS: example values*)

**FR‑007 — Health & Readiness**

**Statement.** The service SHALL expose **GET /healthz** (liveness) and **GET /ready** (readiness) with fields { status, uptimeSeconds, sessionCount, childProcesses }. Readiness checks DB SP reachability and (optionally) child spawn probe.

**AC.**

* AC‑007.1: /healthz returns 200 with fields above during normal operation.
* AC‑007.2: /ready fails with 503 not\_ready during DB outage or child spawn failure.
* AC‑007.3: RTM readiness uses **Prod DB (read‑only)**. (*Runbook: deploy RTM*)

**FR‑008 — Config Surface (read‑only, non‑secret)**

**Statement.** The service SHALL expose **GET /config/effective** returning **non‑secret** key/value pairs driving runtime behavior. Secrets are **never** included.

**AC.**

* AC‑008.1: Response includes keys Mcp:Child\*, Security:AllowedOrigins, Network:SseKeepAliveSeconds, Network:RequestTimeoutSeconds.
* AC‑008.2: No secrets appear; redaction is enforced server‑side.
* AC‑008.3: UI displays keys read‑only with “non‑secret” annotation. (*UI/UX*)

**FR‑009 — Legacy compatibility (feature‑flagged)**

**Statement.** **POST /messages** and **GET /sse** SHALL be available **only** if feature flag EnableLegacyHttpSse (DB‑driven) is **true**; otherwise return 403 feature\_disabled.

**AC.**

* AC‑009.1: With flag OFF (default), calls return 403 feature\_disabled.
* AC‑009.2: With flag ON, behavior mirrors /mcp JSON and SSE semantics for compatibility.

**FR‑010 — KendoReact Admin Portal (read‑only ops)**

**Statement.** The Admin Portal SHALL be implemented with **KendoReact (Fluent v12)** themed via **ThemeBuilder** (tokens from **Figma Make**), and MUST:  
(a) render /ready and /healthz on Dashboard;  
(b) list non‑secret config via /config/effective;  
(c) visualize session/SSE state;  
(d) avoid external images/CDNs; and  
(e) meet **WCAG 2.2 AA** via axe smoke tests in CI.

**AC.**

* AC‑010.1: Dashboard shows uptime/session/child counts with accessible colors.
* AC‑010.2: Config page lists only non‑secret keys; copy‑to‑clipboard is available.
* AC‑010.3: Sessions page shows heartbeat age and stream status; no writes.
* AC‑010.4: No requests to third‑party image/CDN domains; CSP locked down. (*Compliance*)

**FR‑011 — AuthN/AuthZ (platform‑provided bearer)**

**Statement.** The API SHALL accept a **bearer token** (platform‑provided). The Admin Portal SHALL **not** persist tokens; no token values are logged. (AuthZ model beyond scope; deny unauthenticated if enabled at gateway.)

**AC.**

* AC‑011.1: Requests without valid bearer (when enabled) return 401 unauthorized envelope.
* AC‑011.2: Logs never contain bearer or payload bodies.

**FR‑012 — Graceful drain & shutdown**

**Statement.** On shutdown/scale‑in, the service SHALL stop accepting new sessions, maintain heartbeats to active streams, send any final message, then close connections and terminate child processes. (Ingress must not buffer SSE.)

**AC.**

* AC‑012.1: During rolling updates, existing SSE streams are drained gracefully (no abrupt truncation).
* AC‑012.2: Readiness flips to fail before termination to quiesce new traffic. (*Runbook: scale\_out, deploy*)

**FR‑013 — Environment promotion & RTM parity**

**Statement.** Releases SHALL promote **Alpha → Beta → RTM → Prod**. **RTM** validates against the **Prod DB (read‑only)** to detect config drift prior to Prod. Evidence (readiness, config snapshots) is attached to the Release and retained ≥ 1 year.

**AC.**

* AC‑013.1: RTM /config/effective parity matches expected Prod values (non‑secret).
* AC‑013.2: Promotion blocks on parity failure.

**3) Traceability Matrix (FR ↔ OpenAPI ↔ Tests ↔ Runbooks)**

| **FR** | **OpenAPI operation(s)** | **Tests (gherkin)** | **Runbooks/Docs** |
| --- | --- | --- | --- |
| 001 | POST /mcp, GET /mcp | 02\_streamed\_tool\_call | Deploy, Incident |
| 002 | All error responses | 04\_origin\_denied + unit | Error Catalog, OpenAPI |
| 003 | POST /mcp, GET /mcp | 01\_session\_establish, 03\_background\_notification | Scale‑out, Deploy |
| 004 | n/a (internal) | Integration “fake child” | Deploy, Incident |
| 005 | POST /mcp (SSE), GET /mcp | 02\_streamed\_tool\_call | Monitoring |
| 006 | All (Origin) | 04\_origin\_denied | Compliance |
| 007 | /healthz, /ready | Health smokes | Deploy |
| 008 | /config/effective | Contract tests | Compliance, Evidence |
| 009 | /messages, /sse | Legacy on/off tests | Incident |
| 010 | (UI consumes endpoints) | axe + contract tests | UI/UX, CI/CD |
| 011 | All (bearer) | Unit/integration | Compliance |
| 012 | n/a (lifecycle) | N/A | Scale‑out, Rollback |
| 013 | All | Promotion checks | Deploy, Evidence |

**4) Example Requests/Responses (non‑secret)**

**A. Streamed tool call (POST /mcp with SSE)**

*Request headers*

Accept: text/event-stream

Content-Type: application/json

Mcp-Session-Id: <client-supplied-or-issued>

Authorization: Bearer <token>

*Request body*

{ "jsonrpc":"2.0", "id":"9", "method":"ping", "params":{"stream":true} }

*Response (excerpt)*

: heartbeat

event: message

id: 1

data: {"jsonrpc":"2.0","id":"9","result":{"partial":true}}

: heartbeat

event: message

id: 2

data: {"jsonrpc":"2.0","id":"9","result":{"final":true}}

**B. Disallowed Origin**  
403

{ "code": "origin\_forbidden", "message": "Origin not allowed", "requestId": "req-abc123" }

**C. Missing session on GET /mcp**  
400

{ "code": "missing\_session\_id", "message": "Header Mcp-Session-Id is required", "requestId": "req-xyz789" }

**5) Quality Gates (functional slice)**

* **OpenAPI lint/diff** required; attach results to Evidence.
* **Unit/integration/E2E** pass; **axe** smoke green (UI).
* **CodeQL**, **Dependency Review**, **Secret Scanning**, **SBOM** completed per CI.
* **24‑hour** post‑release checks (Prod): availability, error rate, p50/p95, **SSE TTFB**, readiness stability.

**6) Assumptions & Out‑of‑Scope**

* **AuthZ** policy is handled by gateway/IdP; this service enforces bearer (if enabled) and Origin rules.
* **DB writes** are not performed by UI; **RTM** is read‑only to Prod DB.
* **Rate limiting** may be introduced later (future ADR/code).

**7) Glossary (select)**

* **MCP:** Model Context Protocol (JSON‑RPC oriented).
* **SSE:** Server‑Sent Events (text/event-stream).
* **TTFB:** Time to First Byte for streaming response.
* **ThemeBuilder:** Progress tool for generating Kendo theme overrides from design tokens.
* **Add‑only / SP‑only / No‑Hard‑Coding:** Technijian DB & config policies (see banner).

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