**MCPX‑KendoBridge — Product Backlog & Acceptance (Epics, Stories, Gherkin)**

**Document:** docs/15\_backlog.docx  
**Project Code:** MCPX‑KendoBridge  
**Version:** 1.0.0 (Draft)  
**Last Updated:** 2025‑09‑25  
**Document Owner:** DoSE (Accountable) — DocFactory (Responsible)

**Purpose.** Provide the **single source of truth** for Epics, Features, and Stories—each with **acceptance criteria (Gherkin)**, **dependencies**, **DoR/DoD**, and **traceability to FR/NFR**—for the MCPX‑KendoBridge service. This backlog is aligned to Technijian’s **GitHub‑first SDLC**, **four environments (Alpha → Beta → RTM → Prod)**, and **guardrails**: **No‑Hard‑Coding**, **Stored‑procedure‑only** DB access, **add‑only** migrations, and **≥ 1‑year evidence retention**.

**DB COMPLIANCE (applies to every story):** **Add‑only** schema; **Stored‑procedure‑only** DAL; **No‑Hard‑Coding** of dynamic values. All configurable behavior (child command/args/cwd, timeouts, keep‑alive, allowed origins, feature flags) comes from SQL Server via sp\_Config\_\*, sp\_Feature\_IsEnabled, and sp\_Lookup\_Get. Secrets live **only** in GitHub Environments or vendor portals—**never** in code/docs/DB.

**Document Control**

**Revision History**

| **Version** | **Date** | **Author/Role** | **Summary of Changes** |
| --- | --- | --- | --- |
| 1.0.0‑D | 2025‑09‑25 | DocFactory (R) | Initial comprehensive backlog with epics, AC, DoR/DoD, release plan |

**Approvals**

| **Name / Role** | **Responsibility** | **Signature / Date** |
| --- | --- | --- |
| Director of Software Engineering | Accountable (A) | \_\_\_\_ / \_\_\_\_ |
| Systems Architect (T‑Arch) | Consulted (C) | \_\_\_\_ / \_\_\_\_ |
| Security Lead | Consulted (C) | \_\_\_\_ / \_\_\_\_ |
| QA Lead | Consulted (C) | \_\_\_\_ / \_\_\_\_ |

**Table of Contents**

1. How to Use This Backlog
2. Estimation, Labels, and Workflow
3. Release Train & Milestones (Alpha → Beta → RTM → Prod)
4. Epic Catalog (E‑01…E‑16)
5. Feature/Story Details with Acceptance Criteria
6. Traceability (FR/NFR/Endpoints/SPs ↔ Stories)
7. Definition of Ready (DoR) / Definition of Done (DoD)
8. Non‑Functional Backlog (Cross‑cutting)
9. Risks, Assumptions, and Dependencies
10. Next Steps
11. Appendices (Gherkin Extracts)

**1) How to Use This Backlog**

* Create one **GitHub Issue** per **Story**, grouped under **Milestones** that correspond to environments and releases.
* For each story, include: **Context**, **FR/NFR mapping**, **Gherkin**, **Test Notes**, **SPs touched**, and **Evidence artifacts** to attach at release time.
* This document is authoritative; GitHub issues link back to the Story IDs here. Evidence retention **≥ 1 year** follows the Evidence Pack spec.

**2) Estimation, Labels, and Workflow**

**Estimation:** Fibonacci SP (1, 2, 3, 5, 8, 13). **Sizing guidance:**

* *1–2 SP:* pure config/UI copy; *3–5 SP:* single endpoint/story w/ tests; *8–13 SP:* multi‑module changes or new infra.

**Labels (examples):** epic/E-01, area/api, area/db, area/observability, security, perf, legacy-flag, ui-optional, evidence.

**Workflow:** Draft → Ready (DoR met) → In Progress → In Review → Merge Queue → Done (DoD met) → Released (env).

**Branch policy:** PRs to main only; **merge queue** required; checks: Build/Tests, **CodeQL**, **Dependency Review**, **Secret Scanning**, **OpenAPI lint/diff**, **SBOM**.

**3) Release Train & Milestones**

| **Milestone** | **Purpose** | **Required Proofs** |
| --- | --- | --- |
| **Alpha** | Functional bring‑up | /mcp basic JSON + SSE; sessioning; child spawn; /healthz; **OpenAPI** draft; unit/integration tests passing |
| **Beta** | Hardening | Origin allow‑list; /ready; /config/effective; metrics/logs; perf **smoke**; CI gates green |
| **RTM** | Parity on **Prod DB (read‑only)** | Contract re‑run; config parity report; no writes; promotion approvals |
| **Prod** | GA | Canary → rollout; **24‑h post‑release** checks; Evidence Pack complete & attached (retain ≥ 1 year) |

**4) Epic Catalog (overview)**

| **Epic ID** | **Title** | **Outcome** | **FR/NFR** |
| --- | --- | --- | --- |
| **E‑01** | Transport & Content Negotiation | /mcp POST (JSON/SSE) + GET (SSE) with canonical headers | FR‑001, FR‑011 |
| **E‑02** | Sessioning & Child Lifecycle | One child per Mcp‑Session‑Id; spawn/teardown; drain | FR‑002, FR‑004, FR‑006, FR‑012 |
| **E‑03** | STDIO Bridge | Async stdin/stdout routing; streaming chunks → SSE | FR‑005 |
| **E‑04** | Origin Allow‑List & Security | Enforce DB‑driven allow‑list; 403 envelope; no secret logs | FR‑007 |
| **E‑05** | Health, Readiness & Config | /healthz, /ready, /config/effective (redacted) | FR‑008, FR‑009 |
| **E‑06** | Observability (Logs/Metrics) | JSON logs + basic metrics; correlation ids | FR‑010 |
| **E‑07** | Legacy Endpoints Flag | /messages + /sse behind EnableLegacyHttpSse | FR‑003 |
| **E‑08** | Optional Ops UI | Read‑only KendoReact dashboard; a11y smoke | FR‑013 |
| **E‑09** | Data & DB Contracts | Tables, SPs, seeds; EXEC grants; add‑only | — (supports all) |
| **E‑10** | OpenAPI 3.1 & Governance | Servers (alpha/beta/rtm/prod), bearer, error envelope; lint/diff | — (supports all) |
| **E‑11** | CI/CD & Repo Guardrails | Build/Test, CodeQL, Dep Review, Secret Scan, SBOM; deploy A→B→RTM→P | FR‑014 |
| **E‑12** | Performance & Scale | P50/P95, TTFB ≤ 200 ms; ≥ 200 sessions/replica | NFR‑Perf |
| **E‑13** | Monitoring & SLOs | Dashboards, alerts, synthetic; 24‑h checks | NFR‑Avail/Oper |
| **E‑14** | Evidence Pack | Release artifacts & index; retention ≥ 1 year | Evidence |
| **E‑15** | Runbooks | Deploy/Rollback/Incident/License rotation | Operability |
| **E‑16** | Compliance & ADRs | ASVS/HIPAA mapping; ADRs (transport, session, SP‑only, RTM) | Compliance |

Every Epic inherits the **No‑Hard‑Coding** and **SP‑only** rules.

**5) Feature/Story Details with Acceptance Criteria**

**Notation.** S‑### = Story. Each story lists **Description**, **Acceptance Criteria (Gherkin)**, **Tasks**, **Dependencies**, **Estimate**, **FR/NFR**, **Evidence**.

**E‑01 — Transport & Content Negotiation**

**S‑001 — POST /mcp returns JSON by default**  
**Desc.** Implement /mcp POST accepting one JSON‑RPC message; return application/json unless Accept: text/event-stream.  
**AC (Gherkin):**

Feature: /mcp JSON response

Scenario: Default non-streaming response

Given a valid JSON-RPC 2.0 request

When the client POSTs to /mcp without Accept "text/event-stream"

Then the response status is 200

And the Content-Type is "application/json"

And the body is a valid JSON-RPC response

**Tasks.** Controller; OpenAPI; unit tests; contract tests; evidence upload.  
**Deps.** E‑10 (OpenAPI). **Estimate:** 3 SP. **FR:** FR‑001, FR‑011. **Evidence:** OpenAPI, unit/contract test reports.

**S‑002 — POST /mcp streams SSE when requested**  
**AC (Gherkin):**

Scenario: Streamed SSE response

Given an existing session

When the client POSTs to /mcp with Accept "text/event-stream"

Then the server responds "text/event-stream"

And emits "event: message" with incremental "id"

And heartbeat comments are sent per configured keepalive

**Tasks.** SSE writer with heartbeats from Network:SseKeepAliveSeconds (DB); integration tests w/ fake child.  
**FR:** FR‑001. **NFR:** TTFB ≤ 200 ms. **Estimate:** 5 SP.

**S‑003 — GET /mcp SSE subscribe**  
**AC.**

Scenario: Background notifications

Given a valid Mcp-Session-Id

When the client opens GET /mcp

Then the connection remains open

And notifications from the child are forwarded as "event: message"

**Tasks.** Session broadcast; multi‑subscriber fan‑out; integration tests. **FR:** FR‑001, FR‑006. **Estimate:** 5 SP.

**S‑004 — Canonical headers** (Mcp-Session-Id, MCP-Protocol-Version)  
**AC.**

Scenario: Session header echo

When the client POSTs to /mcp without Mcp-Session-Id

Then the response contains a generated Mcp-Session-Id

And subsequent requests bind to the same session when header is provided

**FR:** FR‑002. **Estimate:** 3 SP.

**E‑02 — Sessioning & Child Lifecycle**

**S‑010 — Spawn child from DB‑sourced config**  
**Desc.** Spawn @progress/kendo-react-mcp via command/args/cwd sourced **only** from DB (Mcp:ChildCommand|Args|Cwd).  
**AC.**

Scenario: Child spawn with DB-sourced configuration

Given AppConfig contains ChildCommand, ChildArgs, ChildCwd

When the first request for a session arrives

Then the server spawns the child using those values

And no literals are hard-coded in application code

**FR:** FR‑004. **Estimate:** 5 SP. **Evidence:** config snapshot; code review checklist.

**S‑011 — One child per session; cleanup on end**  
**AC.**

Scenario: Per-session child lifecycle

Given a session with a running child

When the session is closed or idle TTL elapses

Then the child process terminates

And the session registry is updated with no zombie PIDs

**FR:** FR‑006, FR‑012. **Estimate:** 5 SP.

**S‑012 — Graceful shutdown drains SSE**  
**AC.**

Scenario: Draining on shutdown

Given active SSE streams

When the service receives a termination signal

Then it stops accepting new work

And continues heartbeats until final events are sent

And terminates child processes afterwards

**FR:** FR‑012. **Estimate:** 3 SP.

**E‑03 — STDIO Bridge**

**S‑020 — Bidirectional routing with backpressure**  
**AC.**

Scenario: STDIO routing fidelity

Given a JSON-RPC request to /mcp

When the proxy writes the request to the child's stdin

Then stdout lines are emitted as SSE "message" events

And message boundaries are preserved without transformation

**FR:** FR‑005. **Estimate:** 5 SP.

**E‑04 — Origin Allow‑List & Security**

**S‑030 — Enforce Origin allow‑list from DB**  
**AC.**

Scenario: Disallowed Origin is denied

Given Security:AllowedOrigins excludes "https://evil.example"

When a client from that Origin POSTs to /mcp

Then the response is 403 with error code "origin\_forbidden"

And the error envelope matches the canonical schema

**FR:** FR‑007, FR‑011. **Estimate:** 3 SP. **Evidence:** tests; logs show no secret leakage.

**E‑05 — Health, Readiness & Config**

**S‑040 — /healthz liveness** → fields: status, uptimeSeconds, sessionCount, childProcesses. **FR:** FR‑008. **Estimate:** 2 SP.  
**S‑041 — /ready readiness** → SP reachability + (optional) child probe. **FR:** FR‑009. **Estimate:** 3 SP.  
**S‑042 — /config/effective redacted** → only **non‑secret** keys. **FR:** FR‑009. **Estimate:** 3 SP.

**E‑06 — Observability (Logs/Metrics)**

**S‑050 — Structured JSON logs** (requestId, sessionId, childPid; no payload bodies). **FR:** FR‑010. **Estimate:** 3 SP.  
**S‑051 — Metrics**: session\_count, child\_up, child\_restart\_count, http\_request\_duration\_ms, stream\_first\_byte\_ms. **FR:** FR‑010. **Estimate:** 5 SP.

**E‑07 — Legacy Endpoints Flag**

**S‑060 — /messages & /sse gated by EnableLegacyHttpSse**  
**AC.**

Scenario: Legacy endpoints require feature flag

Given the feature flag EnableLegacyHttpSse is false

When the client accesses /sse

Then the response is 403 with "feature\_disabled"

When the flag is true

Then /messages and /sse behave per spec

**FR:** FR‑003. **Estimate:** 3 SP.

**E‑08 — Optional Ops UI (read‑only)**

**S‑070 — Dashboard & Sessions grid** (KendoReact Fluent v12 + ThemeBuilder overrides). **FR:** FR‑013. **Estimate:** 8 SP.  
**S‑071 — A11y smoke (axe)** on /, /sessions, /config. **NFR:** A11y. **Estimate:** 2 SP.

**E‑09 — Data & DB Contracts**

**S‑080 — Create schema & seeds** (AppConfig, FeatureFlag; seeds for child cmd/args/cwd, allowed origins, keep‑alive, timeout). **Estimate:** 3 SP.  
**S‑081 — Create SPs** (sp\_Config\_GetValue, sp\_Config\_GetAll, sp\_Feature\_IsEnabled, sp\_Lookup\_Get). **Estimate:** 3 SP.  
**S‑082 — EXEC grants only** to app role; no table SELECT. **Estimate:** 2 SP.  
**Evidence:** migration scripts, SP files, grant script; **add‑only** naming VYYYYMMDDHHMM\_\_\*.sql.

**E‑10 — OpenAPI 3.1 & Governance**

**S‑090 — Author OpenAPI (servers, bearer, error envelope; stream negotiation)**.  
**S‑091 — Lint & Diff gates in CI; attach outputs to Release.**  
**Estimate:** 5 SP total. **Evidence:** api/openapi/mcp-proxy.yaml, lint/diff artifacts.

**E‑11 — CI/CD & Repo Guardrails**

**S‑100 — CI pipeline** (Build/Tests, coverage gates; merge‑queue event).  
**S‑101 — Security gates**: **CodeQL**, **Dependency Review**, **Secret Scanning**, **SBOM**.  
**S‑102 — Deploy pipeline**: Alpha → Beta → **RTM (Prod DB read‑only)** → Prod; approvals, canary, rollout.  
**Estimate:** 8 SP. **Evidence:** workflow YAMLs, gate results, approvals export.

**E‑12 — Performance & Scale**

**S‑110 — k6 non‑streaming latency tests** (P50≤300 ms; P95≤800 ms). **Estimate:** 5 SP.  
**S‑111 — Streaming TTFB harness** (≤ 200 ms). **Estimate:** 5 SP.  
**S‑112 — Concurrency test** (≥ 200 sessions/replica; CPU‑bound before memory). **Estimate:** 5 SP.  
**Evidence:** perf reports in Evidence Pack; monitoring snapshot.

**E‑13 — Monitoring & SLOs**

**S‑120 — Dashboards** (latency p50/p95, TTFB, error rate, sessions/children). **Estimate:** 5 SP.  
**S‑121 — Alerts** (P1/P2/P3 thresholds). **Estimate:** 3 SP.  
**S‑122 — 24‑h post‑release checklist** automation & snapshot export. **Estimate:** 3 SP.  
**Evidence:** snapshot PDF attached to Release.

**E‑14 — Evidence Pack**

**S‑130 — Collector job** (index.yaml, checksums, artifacts). **Estimate:** 3 SP.  
**S‑131 — Attach to Release; retention ≥ 1 year**. **Estimate:** 2 SP.

**E‑15 — Runbooks**

**S‑140 — Deploy**; **S‑141 — Rollback**; **S‑142 — Incident**; **S‑143 — License rotation**; **S‑144 — Scale‑out**.  
**Estimate:** 5 SP total. **Evidence:** runbook markdowns referenced from Releases.

**E‑16 — Compliance & ADRs**

**S‑150 — ASVS/HIPAA mapping**; **S‑151 — ADRs** (Transport, Legacy flag, Session model, SP‑only, RTM on Prod DB).  
**Estimate:** 5 SP. **Evidence:** docs/13\_compliance, adr/\*.md.

**6) Traceability (FR/NFR/Endpoints/SPs ↔ Stories)**

| **FR/NFR** | **Stories** |
| --- | --- |
| **FR‑001** Transport | S‑001, S‑002, S‑003 |
| **FR‑002** Session header | S‑004 |
| **FR‑003** Legacy endpoints flag | S‑060 |
| **FR‑004** Child spawn config | S‑010 |
| **FR‑005** STDIO routing | S‑020 |
| **FR‑006** Per‑session child | S‑011, S‑003 |
| **FR‑007** Origin allow‑list | S‑030 |
| **FR‑008** Health | S‑040 |
| **FR‑009** Readiness/Config | S‑041, S‑042 |
| **FR‑010** Logs/Metrics | S‑050, S‑051 |
| **FR‑011** Error envelope | S‑001, S‑030 |
| **FR‑012** Graceful shutdown | S‑012 |
| **FR‑013** Optional UI | S‑070, S‑071 |
| **FR‑014** CI/CD | S‑100, S‑101, S‑102 |
| **NFR‑Perf** p50/p95, TTFB | S‑110, S‑111, S‑112 |
| **NFR‑Avail/Oper** | S‑120..S‑122 |
| **DB/SP Compliance** | S‑080..S‑082 |

**7) Definition of Ready (DoR) / Definition of Done (DoD)**

**DoR (Story cannot start unless all true):**

1. FR/NFR mapping identified; 2) Dependencies listed; 3) OpenAPI changes stubbed (if any); 4) SP changes proposed (**add‑only**); 5) Acceptance (Gherkin) drafted; 6) No secrets required; 7) Test data plan prepared.

**DoD (Story cannot complete unless all true):**

1. Code merged via **merge queue** with required checks (**Build/Tests**, **CodeQL**, **Dependency Review**, **Secret Scanning**, **OpenAPI lint/diff**, **SBOM**); 2) Unit/integration (and E2E if applicable) pass; 3) Logs show no secrets; 4) OpenAPI updated (if applicable) and attached to Evidence Pack; 5) If touching DB: migrations are **add‑only**, SP signatures stable, grants reviewed; 6) Story evidence (test report/screenshots) attached to Release.

**8) Non‑Functional Backlog (Cross‑cutting)**

* **NF‑01:** SSE ingress configuration verified in each environment (no buffering; heartbeats honored).
* **NF‑02:** Structured logging redaction rules applied (drop/obfuscate secret‑like patterns).
* **NF‑03:** Perf profile of STDIO bridge to ensure CPU‑bound saturation before memory.
* **NF‑04:** Resilience drill: restart to /ready ≤ 30 s; graceful drain validated.
* **NF‑05:** A11y smoke (UI) integrated into CI with axe.
* **NF‑06:** Evidence export scripted and verified for retention policy.

**9) Risks, Assumptions, and Dependencies**

**Key Risks & Mitigations**

* *Ingress buffers SSE* → Configure explicit streaming settings; add synthetic SSE checks.
* *Child process flaps* → Add jittered retries and child\_restart\_count alerts.
* *Config drift across envs* → RTM validation against **Prod DB (read‑only)** blocks Prod promotion.
* *Secret leakage in logs* → Enforce redaction and prohibit logging payload bodies; CI **Secret Scanning**.

**Assumptions**

* Platform provides bearer authentication; DB reachable; **SP‑only** DAL; **add‑only** migrations; Evidence retention **≥ 1 year**.

**External Dependencies**

* @progress/kendo-react-mcp availability via npx; Telerik license configured in environment (never DB).

**10) Next Steps**

1. Open GitHub Epics/Issues for all **E‑01…E‑16** and seed Stories **S‑001…S‑151** with the AC and tasks above.
2. Wire CI gates and OpenAPI lint/diff to block merges until contracts are updated.
3. Execute Alpha stories (S‑001…S‑012, S‑020, S‑030, S‑040, S‑080…S‑082, S‑090, S‑100/S‑101) to reach first deploy.
4. Prepare RTM parity checks against **Prod DB (read‑only)**; schedule 24‑hour post‑release Evidence export.

**11) Appendices — Gherkin Extracts (copy to /tests/gherkin/\*.feature)**

**A. Session Establishment**

Feature: Establish MCP session

Scenario: New session id issued

Given a client without a Mcp-Session-Id

When it POSTs to /mcp with a valid JSON-RPC message

Then the response is 200

And header "Mcp-Session-Id" is present

**B. Streamed Tool Call**

Feature: Streamed response

Scenario: SSE for tool call

Given an existing session

When the client POSTs to /mcp with Accept "text/event-stream"

Then the response is "text/event-stream"

And "event: message" frames are received with incremental ids

**C. Background Notification**

Feature: Notifications

Scenario: Receive background event

Given GET /mcp is open with a valid Mcp-Session-Id

When the child emits a notification

Then the client receives an SSE "message"

**D. Origin Denied**

Feature: CORS/Origin enforcement

Scenario: Disallowed Origin

Given Security:AllowedOrigins excludes the request Origin

When the client POSTs to /mcp

Then status is 403

And the error envelope code is "origin\_forbidden"

**E. Readiness & Config**

Feature: Operability endpoints

Scenario: Ready with DB available

When a client GETs /ready

Then status is 200

And fields "status","sessionCount","childProcesses" exist

Scenario: Effective non-secret config

When a client GETs /config/effective

Then status is 200

And only non-secret keys are present

**F. Legacy Endpoints Flag**

Feature: Legacy transport gating

Scenario: Disabled by default

When a client GETs /sse

Then status is 403

And error code is "feature\_disabled"

**Footer (optional for Word header/footer):**  
*MCPX‑KendoBridge • Product Backlog & Acceptance • Version 1.0.0 (Draft) • 2025‑09‑25 • Confidential — Technijian Internal*