**MCPX‑KendoBridge — Threat Model (STRIDE) & Data‑Flow Diagrams**

**Document:** docs/17\_threat\_model.docx  
**Project Code:** MCPX‑KendoBridge  
**Version:** 2.0.0  
**Last Updated:** 2025‑09‑27  
**Owner:** Security Lead (Responsible) — DoSE (Accountable) — DocFactory (Author) — SRE/Dev/T‑Arch/QA (Consulted)

**Purpose.** Provide an **audit‑ready** threat model for the MCPX‑KendoBridge proxy and Admin Portal. We document **assets**, **trust boundaries**, **data flows**, **STRIDE threats**, **abuse cases**, and **controls** mapped to FR/NFR, OpenAPI, monitoring, CI/CD gates, and runbooks. This model follows Technijian guardrails: **GitHub‑first** SDLC (merge queue + required checks), **No‑Hard‑Coding**, **Stored‑procedure‑only** DAL, **add‑only** migrations, **four environments** (**Alpha → Beta → RTM → Prod**) with **RTM validating on Prod DB (read‑only)**.

**Compliance banner (applies throughout):** All dynamic values (child command/args/cwd, keep‑alive cadence, request timeouts, Origin allow‑list, feature flags) are **DB‑sourced via stored procedures** (sp\_Config\_\*, sp\_Feature\_IsEnabled, sp\_Lookup\_Get). **Secrets** (SQL connection strings, Telerik license) live **only** in **GitHub Environments**; **never** in code/docs/DB/logs. The Admin Portal is **read‑only** and must not expose secrets.

**1) System overview & assets**

**Primary goal.** Bridge Remote MCP clients (e.g., ChatGPT Connector) over **HTTP/Streamable‑HTTP** to the **Telerik KendoReact MCP** process via **STDIO**, with **SSE** support for streaming and notifications.

**Key assets (confidentiality/integrity/availability — CIA):**

1. **Transport surfaces**: /mcp (POST JSON or SSE), /mcp (GET SSE), legacy /messages + /sse (flagged), /healthz, /ready, /config/effective.
2. **Session binding**: Mcp‑Session‑Id (routing key; **not** an auth secret).
3. **Child process**: @progress/kendo-react-mcp (spawned via **DB‑driven** command/args).
4. **Config plane**: non‑secret keys/flags in SQL Server (AppConfig, FeatureFlag via SPs).
5. **Secrets**: SQL connection strings; **Telerik license** (CI build‑time only).
6. **Observability**: JSON logs (requestId/sessionId/childPid; no payloads), metrics (TTFB, heartbeat gaps, readiness, errors by code).
7. **Release evidence**: OpenAPI, CodeQL, SBOM, secret‑scan summaries, perf/monitoring snapshots (retained ≥ 1 year).

**Actors:**

* **Remote MCP client** (primary)
* **Legacy MCP client** (optional; feature‑flagged)
* **Kendo MCP child process** (STDIO)
* **Ops Admin** (read‑only Admin Portal; promotion Alpha → Prod)

**2) Trust boundaries & data‑flow diagrams (DFDs)**

**2.1 Context & trust boundaries (Level‑0)**

flowchart LR

subgraph Internet [Untrusted Internet]

C1[Remote MCP Client]

C2[Legacy MCP Client]

end

subgraph Edge [Ingress / LB / WAF]

GW[Gateway / Ingress]

end

subgraph App [MCPX‑KendoBridge API Pod]

A1[/POST /mcp (JSON or SSE)/]

A2[/GET /mcp (SSE)/]

L[/Logs + Metrics/]

CP[Child Supervisor]

end

subgraph Child [Kendo MCP Child Process]

K[@progress/kendo-react-mcp<br/>STDIO]

end

subgraph DB[SQL Server (non-secret config/flags)]

SP[(SPs: sp\_Config\_\*, sp\_Feature\_IsEnabled,<br/>sp\_Lookup\_Get)]

end

C1 -->|HTTPS| GW --> A1

C1 -->|HTTPS| GW --> A2

C2 -->|HTTPS (flagged)| GW --> A1

A1 <-->|STDIO| K

CP --- K

A1 -->|EXECUTE via SP| SP

A2 -->|EXECUTE via SP| SP

A1 --> L

A2 --> L

**Trust boundaries:**

1. Internet ↔ Edge, 2) Edge ↔ App, 3) App ↔ Child (local process boundary), 4) App ↔ DB (network/database boundary). Admin Portal traffic follows the same **Edge→App** path and calls **read‑only endpoints**. RTM shares the Prod DB in **read‑only** mode.

**2.2 Expanded flows (Level‑1: sessions & streaming)**

sequenceDiagram

participant Client as Remote MCP Client

participant API as MCPX API (/mcp)

participant Child as Kendo MCP Child (STDIO)

participant DB as SQL SPs (Config/Flags)

Client->>API: POST /mcp {jsonrpc...} (Accept: text/event-stream?)

API->>DB: sp\_Config\_GetAll / sp\_Feature\_IsEnabled

alt First request (new session)

API->>Child: spawn with DB-driven cmd/args/cwd

API-->>Client: 200 + Mcp-Session-Id (header)

end

API->>Child: forward JSON-RPC over STDIO

Child-->>API: stdout lines (partial + final)

API-->>Client: SSE frames (event: message, id: n) + heartbeats (":" every N sec)

**3) STRIDE analysis — threats & mitigations (by boundary)**

**Legend:** **Mitigation mappings** reference our specs: **FR** (Functional Requirements), **NFR**, **OpenAPI**, **Compliance**, **Monitoring**, **Runbooks**. Controls derive from Technijian DocFactory defaults.

**3.1 Edge ↔ App (HTTP/Streamable‑HTTP, SSE)**

| **STRIDE** | **Threat** | **Likelihood/Impact** | **Mitigations (implemented / planned)** |
| --- | --- | --- | --- |
| **S**poofing | Origin spoofing via crafted Origin header | M / M | **DB‑driven allow‑list** Security:AllowedOrigins → **403 origin\_forbidden** (FR‑006, OpenAPI error examples, Monitoring panel), UI displays allow‑list (read‑only). |
| **S**poofing | Session hijack via forged Mcp‑Session‑Id | L / L | Mcp‑Session‑Id is **routing only** (not auth); gateway **bearer** optional; sticky routing ensures per‑session isolation on a replica (FR‑003/011). |
| **T**ampering | SSE frame injection / newline smuggling | L / M | Strict framing; server‑side origin check; JSON encode data: payloads; **no payload echo** in logs; tests for partial frame handling (Test Strategy). |
| **R**epudiation | Lack of audit for streamed calls | M / M | **Structured logs** with requestId, sessionId, childPid, `mode=json |
| **I**nformation Disclosure | Secrets in responses or logs | L / H | **Non‑secret** config surface only; **never** return secrets; redact logs; Secret Scanning in CI; Evidence reviews (Compliance, CI/CD, Evidence Pack). |
| **D**oS | Ingress buffers SSE → stalled streams | M / M | Ingress policy: **no buffering** for text/event-stream; timeouts aligned to DB cadence; SLO for **SSE TTFB p95 ≤ 200 ms** with alerts (NFR, Monitoring, Runbooks). |
| **E**oP | Abuse of legacy endpoints | L / M | Legacy /messages /sse **OFF by default** (feature flag); **403 feature\_disabled** + tests (FR‑009; Error Catalog). |

**3.2 App ↔ Child (process/STDIO)**

| **STRIDE** | **Threat** | **Likelihood/Impact** | **Mitigations** |
| --- | --- | --- | --- |
| **S**poofing | Executing an unintended binary | L / H | **DB‑sourced** `Mcp:ChildCommand |
| **T**ampering | Malicious STDIO payload alters state | L / M | Proxy treats JSON‑RPC as **opaque**; **no DB writes**; stable error envelope; back‑pressure handling in bridge; tests cover framing. |
| **R**epudiation | No traceability per child | M / M | Include childPid, sessionId, requestId in logs; child restarts counted via metrics; evidence retained ≥ 1 year. |
| **I**nformation Disclosure | Child outputs leak sensitive data | L / H | **Do not log payload bodies**; surface only envelopes; Admin Portal is **read‑only** and never prints secrets. |
| **D**oS | Child crash flaps sessions | M / M | **Graceful drain** in rollouts; sticky sessions; monitor child\_restart\_count; **rollback** runbook; code rollback to LKG. |
| **E**oP | Child escapes sandbox | L / H | Run with least privileges; locked down file system; no access to DB credentials (they live in app process/Env). |

**3.3 App ↔ DB (config & flags)**

| **STRIDE** | **Threat** | **Likelihood/Impact** | **Mitigations** |
| --- | --- | --- | --- |
| **S**poofing | App principal mis‑scoped | L / H | **EXECUTE‑only** on SPs; **no table rights**; role‑based grants reviewed in Evidence (Compliance). |
| **T**ampering | Inline SQL or destructive DDL | L / H | **Add‑only** migrations; **SP‑only**; PR checks include No‑Hard‑Coding checklist; Code Owners. |
| **R**epudiation | Config changes untracked | M / M | Idempotent seed migrations; snapshots of /config/effective per env; Evidence Pack (≥ 1 year). |
| **I**nformation Disclosure | Secrets stored in DB | L / H | **Prohibited**; secrets in **GitHub Environments only**; /config/effective is explicitly non‑secret. |
| **D**oS | SP latency spikes | M / M | Monitor config\_fetch\_duration\_ms (p95 ≤ 200 ms); alert/tune; readiness reflects DB reachability (Monitoring; NFR). |
| **E**oP | Privilege escalation via SPs | L / H | Narrow SP surface (GetAll, GetValue, IsEnabled, Lookup\_Get); audit SP signatures; unit/integration tests. |

**4) Abuse cases (attacker stories) & responses**

1. **Forge Origin** to scrape streaming data.
   * **Outcome:** Request blocked with **403 origin\_forbidden**; metrics show spike; incident playbook investigates allow‑list drift vs. abuse. (FR‑006; Monitoring; Incident Runbook).
2. **Spam streaming calls** to exhaust child spawns.
   * **Outcome:** Observed in **TTFB p95** and child\_restart\_count; scale‑out per runbook; consider rate‑limit ADR (future); evidence captured. (NFR, Scale‑out Runbook).
3. **Use legacy endpoints to bypass policy.**
   * **Outcome:** **403 feature\_disabled** by default (FR‑009); enabling requires change control + Evidence.
4. **Attempt session hijack via Mcp‑Session‑Id.**
   * **Outcome:** Harmless; it’s not auth; sticky routing only. Gateway bearer (if enabled) still required per request. (FR‑003/011).
5. **Ingress buffering causes SSE truncation.**
   * **Outcome:** Alerts on **TTFB** / heartbeat gap; **rollback** or ingress fix; post‑mortem & config hardening. (Monitoring; Rollback Runbook).
6. **Accidental logging of secrets.**
   * **Outcome:** Secret Scanning detects; incident opened; scrub logs; rotate in **GitHub Environments**; publish rotation evidence. (Compliance; Rotate License Runbook).

**5) Controls library (mapped to requirements & artifacts)**

| **Control** | **Where enforced** | **Evidence** |
| --- | --- | --- |
| **Origin allow‑list (DB)** | FR‑006; /config/effective | Error Catalog (403); OpenAPI examples; tests; monitoring panel |
| **Stable error envelope** | FR‑002; OpenAPI component | Error catalog; contract tests; logs without payload bodies |
| **Session‑per‑child** | FR‑003 | Metrics (session\_count, child\_up), logs (childPid) |
| **SSE heartbeats & TTFB** | FR‑005; NFR/Monitoring | k6/perf smoke; dashboards; alerts |
| **Legacy flag OFF** | FR‑009 | /messages//sse return 403; tests |
| **Readiness gates** | FR‑007 | /ready behavior; rollout logs |
| **Non‑secret config surface** | FR‑008 | /config/effective snapshots |
| **Auth (bearer, gateway)** | FR‑011 | 401 envelope when enabled |
| **No‑Hard‑Coding; SP‑only; Add‑only** | Compliance; Data Contracts | Migrations/SPs; CI checks; Evidence Pack |
| **Kendo license at build only** | CI/CD; Compliance | CI logs (scrubbed); rotation runbook |

**6) Security testing plan (complementary to Test Strategy)**

* **SAST & SCA**: **CodeQL** (C#/JS), **Dependency Review** fail on **High**; **SBOM** artifact per build.
* **Contract tests**: error envelope codes (origin\_forbidden, missing\_session\_id, feature\_disabled, not\_ready, etc.) verified against OpenAPI 3.1 responses.
* **Streaming harness**: assert **SSE TTFB p95 ≤ 200 ms**; heartbeat cadence equals Network:SseKeepAliveSeconds (±1s).
* **Ingress conformance**: automated probe verifies **no buffering** and acceptable read/idle timeouts for text/event-stream.
* **UI a11y**: **axe** smoke for /, /sessions, /config, /access; CSP denies third‑party egress.
* **RTM parity**: /config/effective diff vs. expected Prod; **Prod DB (read‑only)** validations.

**7) Residual risks & deferred items**

* **Rate limiting / quotas** (deferred): introduce per‑IP/session rate limits; add OpenAPI 429 rate\_limited in active use.
* **Child sandboxing hardening**: apparmor/seccomp review (platform dependent).
* **Malicious payloads in JSON‑RPC**: opaque tunnel by design; consider content length caps per request (config‑driven).
* **Ingress vendor drift**: periodic conformance tests in CI to catch buffering/timeouts deviations.

**8) Diagrams for architecture reviews (paste‑ready)**

**8.1 Data Flow Diagram (DFD L‑0) — Mermaid**

flowchart TB

ext[Clients (Remote/Legacy)]:::ext --> gw[Ingress/LB]:::ctrl --> api[MCPX API]:::trusted

api --> db[(SQL Server via SPs)]:::db

api --> child[Kendo MCP (STDIO)]:::proc

classDef ext fill:#fff,stroke:#c33,stroke-width:2px

classDef ctrl fill:#f9f9f9,stroke:#888,stroke-dasharray: 3 3

classDef trusted fill:#e8f5ff,stroke:#06c

classDef db fill:#efe,stroke:#070

classDef proc fill:#ffe,stroke:#aa0

**8.2 Sequence (streamed tool call) — Mermaid**

sequenceDiagram

participant C as Client

participant A as API

participant K as Child

C->>A: POST /mcp (Accept: text/event-stream)

A->>K: forward JSON-RPC via STDIO

K-->>A: stdout partials

A-->>C: event: message / id: n

A-->>C: : heartbeat every N sec

K-->>A: final

A-->>C: final message; close stream

**9) Review & acceptance checklist (security sign‑off)**

* **OpenAPI 3.1** includes error envelope and streaming examples; servers: Alpha/Beta/RTM/Prod; bearer security.
* **FR/NFR** reflect Origin allow‑list, session‑per‑child, RTM on **Prod DB (RO)**, and SSE budgets.
* **CI/CD** enables CodeQL, Dependency Review, Secret Scanning, SBOM; merge‑queue required.
* **Monitoring** dashboards/alerts for Availability, JSON p50/p95, **SSE TTFB**, heartbeat gaps, child restarts.
* **Runbooks** (deploy, rollback, incident, scale‑out, rotate license) linked and tested.
* **Evidence Pack** contents defined and retained ≥ 1 year.

**10) Cross‑references**

* **Functional Requirements:** docs/05\_fr.docx
* **Non‑Functional Requirements:** docs/06\_nfr.docx
* **OpenAPI 3.1:** api/openapi/mcp-proxy.yaml
* **Monitoring & SLOs:** docs/11\_monitoring.docx
* **Security & Compliance:** docs/13\_compliance.docx
* **Error Catalog:** docs/error\_catalog.docx
* **Runbooks:** deploy / rollback / incident / scale\_out / rotate\_telerik\_license  
  All of the above implement the guardrails and SDLC per DocFactory defaults.

**11) Assumptions**

1. **Ingress** passes text/event-stream without buffering; read/idle timeouts align with Network:SseKeepAliveSeconds.
2. **RTM** uses **Prod DB (read‑only)** for parity validation before Prod promotion.
3. **Admin Portal** is read‑only; CSP denies third‑party egress; license handled **at CI build only**.

**12) Next steps**

* Add an **ingress conformance test** to CI (assert SSE pass‑through, timeouts).
* Evaluate lightweight **rate limiting** (429 + ADR) for sustained abuse patterns.
* Schedule a **threat‑model review** each release or on material changes (transport/ingress/runtime).

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