MCP-INTEGRATION-SPEC

Layer 2 Procedural File 6 of 6 — The Dash / NornGate at SBS Implements: 00-NornGate-Architecture.md (legacy estate; Vanaheim trust) and 00-Take-Notice.md (status carried across the boundary). Enforced by: Njord (transmission ownership) · Baldr (G4 handle check) · Sif (post-execution reconciliation).

Purpose

The pattern by which The Dash integrates with the SBS legacy estate via the Model Context Protocol (MCP). The WideOrbit MCP is the first and canonical connector — it is the first integration built under Deployment-Playbook Phase 3 and the first write path cut over in Phase 7. This document generalizes its pattern so the remaining estate connectors (MusicMaster, SIMS, Oracle, ADP, SAP, vCreative, CPT) can be added without re-deriving the architecture.

The LaMusica exclusion is stated before anything else: LaMusica is a closed department. No MCP, no connector, no credential, no exception — this pattern must never be instantiated for LaMusica. An attempted crossing is SEV-1 per 00-NornGate-Architecture.md (the LaMusica Rule).

What MCP Means in This Context

The Model Context Protocol is a standard interface for connecting AI agents to external systems. In The Dash’s context, an MCP integration:

- Allows an agent to transmit instructions to a legacy-system counterparty;
- Receives acknowledgments and execution confirmations back;
- Captures the full transmission lifecycle in the audit trail per the Four-Record Sequence in 10-Audit-Trail-Spec.md;
- Carries the G2 authorization handle from 10-Governance-Gate-Spec.md through to the counterparty for non-repudiation;
- Operates under per-connector credential isolation — Vanaheim trust: federation, not absorption. Each integration’s trust is negotiated and scoped per connector, never shared across the estate.

MCP is not:

- A general-purpose API client (those are direct service-to-service);
- A retrieval mechanism (reads from the estate are Hermóð's gated retrieval under Hel's classification — they traverse G0/G1 but do not produce transmission records);
- A replacement for the gates (every MCP transmission of a material instruction rides the full G0→G4 pipeline and requires a Gate-issued authorization handle).

The MCP boundary is the boundary between the bench's internal trust domain and the legacy estate's trust domains. The audit-trail discipline at this boundary is correspondingly elevated.

The WideOrbit MCP (The Canonical Example)

What WideOrbit Is at SBS

WideOrbit is SBS's traffic and order-to-cash system — the revenue-side system of record for broadcast inventory: order entry and revision, spot placement, makegoods, copy instructions, the daily traffic log, and the billing extracts that feed Oracle and SAP. An error here is not a data problem; it is on-air inventory and recognized revenue.

Njord is the only agent on the bench whose actions transmit through WideOrbit. Every Njord-staged action that mutates WideOrbit state — order entry, order revision, spot placement, makegood, copy-instruction attachment, traffic-log edit, invoice-extract trigger, payment application, credit memo — passes through the WideOrbit MCP. Material writes require a G2 handle per the action-category matrix in 10-Governance-Gate-Spec.md.

The Four-Record Audit Sequence

Per the Four-Record Sequence in 10-Audit-Trail-Spec.md, every Njord → WideOrbit transmission produces four sequential audit-trail records, hash-chained and cross-referenced:

```
Record 1: njord.transmission.wideorbit_mcp.queued
  - agent_id=njord; authorization_handle_id (from the G2 decision)
  - payload: the queued instruction
  - prior_record_hash linked to Njord's prior record in the chain
Record 2: njord.transmission.wideorbit_mcp.acknowledged
  - cross_agent_handoff_record_id → Record 1
```

  - payload: WideOrbit's acknowledgment with timestamp and latency_ms
  - WideOrbit-side reference ID captured
Record 3: njord.transmission.wideorbit_mcp.executed
  - cross_agent_handoff_record_id → Record 1
  - payload: WideOrbit's execution confirmation
  - post-execution state captured (log revision, order totals,
    affected spot inventory)
Record 4: sif.reconciliation.wideorbit_post_execution
  - cross_agent_handoff_record_id → Record 1
  - reconciliation_record_id → Record 1 (closes the loop)
  - payload: state diff, reconciliation outcome
  - any discrepancy escalation triggered here

A four-record sequence missing any record is a SEV-1 integrity event per 00-Incident-Response-Matrix.md (Track B). Sif’s integrity sweep detects missing records on the daily / weekly cadence per the verification cadence in 10-Audit-Trail-Spec.md; the IT Director and the break-glass roster are engaged per 00-Single-Maintainer-Appendix.md.

Per-Connector Credential Isolation

WideOrbit MCP credentials are connector-specific. There is no shared credential across the estate — each connector has its own account / API key / client certificate set, provisioned under Deployment-Playbook Phase 3, held in the Asgard control plane, and rotated quarterly (Tyr issues; Heimdall hygiene-scans). Credential starvation applies in full: Njord never holds the WideOrbit credential; it is injected only into an approved, committed action at G4.

A cross-connector credential exposure is operationally a SEV-1 incident:

1. Heimdall detects via continuous credential-hygiene scan;

2. Tyr rotates all affected connectors’ credentials immediately;

3. Forseti routes the incident to the IT Director; outside-counsel cybersecurity-disclosure analysis (SBS is an SEC-reporting issuer);

4. The counterparty system owner is notified.

Governance Gate Coupling

Every WideOrbit MCP transmission carries a Gate-issued authorization handle per 10-Governance-Gate-Spec.md. The handle is hash-bound to the request payload and the approver decision, expiry-bounded, and revocable between approval and execution. An expired approval holds — Baldr’s

rule: no commit on a stale handle, ever.

The connector-side adapter validates handle structure on receipt; transmissions without a valid handle are rejected at the adapter — Checkpoint 2 in the two-checkpoint architecture (Checkpoint 1 is Baldr's G4 commit validation). This makes the Gate's authorization the necessary substrate for any estate mutation; bypass would require simultaneous compromise of the Gate, the audit trail, AND the connector-side validation — three independent layers.

Failure Mode Taxonomy

Failure	Detection	Response
WideOrbit returns acknowledgment timeout	Njord's transmission monitoring	Retry within the workflow; SEV-2 if persistent; immediate escalation if a traffic-log deadline is implicated — air dates do not accept rescheduling (10-Operating-Rhythm.md)
WideOrbit returns execution failure	Record 3 captures the error code	SEV-2; Njord re-stages a corrected instruction; pattern triggers Track B review
Acknowledgment but no execution	Sif's reconciliation step (Record 4)	SEV-2; investigation; WideOrbit system owner engaged
Njord transmits without an authorization handle	Adapter rejects at Checkpoint 2	**SEV-1** — the bench attempted an unauthorized transmission; Heimdall + Tyr + IT Director; full forensic
Handle expired between Gate and transmission	Adapter rejects at Checkpoint 2	Routine — re-stage with a new G2 request; Baldr's rule working as designed
Handle conditions not verified	Adapter rejects at Checkpoint 2	Routine — conditions surface to the approver via request_more_info (Forseti)
Cross-connector credential exposure	Heimdall's credential-hygiene scan	**SEV-1**; full rotation of affected connectors; outside-counsel disclosure analysis
Four-record sequence incomplete	Sif's integrity sweep	**SEV-1**; halt Njord → WideOrbit transmissions; root-cause; engage the counterparty
Hash-chain integrity break in Njord's chain	Verification sweep per 10-Audit-Trail-Spec.md	**SEV-1**; halt all estate writes; full forensic; SOX § 802 records-integrity impact assessment

Future Connector MCPs

MusicMaster, SIMS, Oracle, ADP, SAP, vCreative, and CPT follow this pattern, in the cutover order set by 10-Deployment-Playbook.md. Each addition requires:

1. Its own integration spec following this document's pattern, naming exactly one transmitting agent of record;

2. A 10-Governance-Gate-Spec.md action-matrix update (new categories);
3. Provisioning per 10-Deployment-Playbook.md Phase 3 (credentials, adapter, shadow mode);
4. The owning agent's SKILL file (operational ownership — SKILL files are scheduled under Phase 2).

No connector is added by modifying this file alone; each is its own specification with its own evidence package.

Authoritative For

- Any agent-to-estate transmission pattern question
- Connector credential isolation and rotation
- The transmission-level audit record sequence and its SEV classifications
- Counterparty-side validation requirements for new connectors

What's Not Here

- The gate pipeline itself — 00-NornGate-Architecture.md
- Authorization classes and the action-category matrix — 10-Governance-Gate-Spec.md
- Ledger storage, retention, and verification cadence — 10-Audit-Trail-Spec.md
- Retrieval (read) discipline — Hermóð's gated retrieval under Hel's classification; see the agent files

Modification Protocol

Proposal drafted by the responsible agent → legal/sufficiency review where statutory interpretation is implicated → Odin staffs the synthesis pass → G2 request with full evidence package → human decision per the Single-Maintainer-Appendix authority structure. Approved modifications are versioned (1.0 → 1.1 minor; 1.x → 2.0 material) and captured in Urd's ledger as policy_change-class records. Layer 1 files are not modified by this protocol — they require SBS Board / IT Governance authorization via Asgard Policy Review.

Document Control: SBS-DASH-PROC-06 · v1.0 · 2026-08-05 · SHA-256 (content above): eb3b…7f7c · Sealed under Audit-Trail-Spec § 8.2. Modification authority: SBS Board / IT Governance via Asgard Policy Review (Governance-Gate); revalidation propagates per Tyr-SKILL § 3.4.

Revision #1
Created 2026-08-05 04:14:19 UTC by SBS Admin
Updated 2026-08-05 04:15:35 UTC by SBS Admin