

Deterministic SI Agents, SIDBMS and Parameter Shielding

A source-based architectural review of the Deterministic SI Agents Marketplace, Glial verification and developer governance

Deterministic SI Agents Marketplace · By Glial Super Intelligence™

Technical position paper · 17 October 2026

Abstract

This technical position paper examines a deterministic-agent marketplace and its activation-stage connection to SIDBMS as the principal verification, management, analysis and parameter-shielding layer. A source-based architectural method distinguishes implemented marketplace tools from the Engineered Einstein-Daramola and Glial framework and documented integration contracts. The Project Statement states that the framework is awaiting activation. The analysis incorporates the supplied theoretical synthesis and a separate parameter-shielding gateway design, retaining authenticated handshakes, human review, stateless request processing and marketplace-side ownership checks. It identifies the limits of illustrative authentication, caller-reported volume and transaction-labelled metrics, without activating the supplied code. The paper also retains a complete search strategy and developer-tool inventory. Its conclusions support explicit trust boundaries and accessible public evidence, not claims of independently certified physics, universal safety or a live SIDBMS adapter.

Keywords: Deterministic agents; Super Intelligence; SIDBMS; Glial verification; parameter shielding; developer governance; search accessibility.

1. Scope, method and evidentiary classification

This paper is a source-based architectural review of the Deterministic SI Agents Marketplace and its activation-stage relationship with the Super Intelligence Database Management System (SIDBMS). The method combines examination of marketplace implementation records, SIDBMS public descriptions, Project Statement disclosures, protocol guidance and two supplied technical documents. The Project Statement states that the framework is Engineered and awaiting activation. This paper documents that status without presenting a new controlled experiment, hardware benchmark, penetration test or independent scientific certification. [1] [2] [3]

The Project Statement states that the SIDBMS and Glial framework is Engineered and awaiting activation. This paper distinguishes that engineering status from available marketplace capabilities, source-attributed technical findings and activation of the marketplace connection. Not Activated denotes the pending activation state; it does not describe the framework as unengineered. Documented SIDBMS and SIMS endpoint paths remain separate from implemented marketplace routes.

The supplied Einstein-Daramola document comprises five PDF pages and the parameter-shielding document eleven pages, including its final blank page. Page references below refer to those supplied editions. Quotations are limited to necessary notation and identifiers; code examples are analysed rather than installed. Existing endpoint handshakes, marketplace-side verification and SIDBMS human-in-the-loop

controls are retained. Stateless service processing does not remove authorization, replay protection or approval requirements. [4] [2] [3]

The Project Statement states that the SIDBMS and Glial framework is Engineered and awaiting activation. The search strategy and measurement plan describe the activation priorities for this engineered framework and its marketplace connection. Activation status is recorded separately from public paper availability and search-engine indexing. This paper does not add new performance measurements or represent pending analytics instrumentation as active.

2. Marketplace purpose and architectural context

PUBLICATION STATUS: READY. SIDBMS-side technical verification belongs to SIDBMS, not the marketplace, and is not a prerequisite for publishing this dossier.

Deterministic SI Agents Marketplace connects developers with people who want to discover, inspect and test bounded Super Intelligence workflows. Its priority is deterministic execution: declared capabilities, visible constraints, account ownership and human decisions for guarded writes.

The implementation supports discovery, sign-in, owned listings, private tests and approval-gated note creation. This release adds a Developer Hub, SI Companion, starter manifests, validators, offline CLI, draft import, private exports and website widgets. The marketplace is published at www.agtstore.si; confirm the updated build before promoting new features as live. Fixed routing has no external model dependency. [1] [5]

The SIDBMS relationship

The Project Statement states that the ecosystem places verification, management, analysis and shielding in SIDBMS. Public material describes Glial Core simulations, screening and audit visibility. Simulation access is by application and KYC. The Project Statement states that procedures are stateless and retain SIDBMS human-in-the-loop controls, API handshakes and marketplace-side verification. These are documented together; no working marketplace adapter was found. [6] [7] [8] [4] [1]

POSITIONING STATEMENT. Discover and test SI agents with declared capabilities, deterministic routing and human-controlled writes. Extend the trust workflow through an explicitly scoped SIDBMS verification and operations connection as that integration is implemented.

Four strategic priorities

First, make behaviour and limitations understandable before launch. Second, give developers ownership without exposing private user activity. Third, turn verification into inspectable evidence rather than a broad badge. Fourth, earn organic discovery through useful listings, technical documentation and a credible SIDBMS explanation—not unsupported claims of universal safety or intelligence.

Brand convention: retain the exact approved name “Deterministic SI Agents Marketplace” and the attribution “By Glial Super Intelligence™”. Use SI and Super Intelligence in product wording. “Deterministic AI” is discussed only as a search-category bridge and technical comparison, not as a replacement brand or a claim that the present runtime uses a generative model.

3. Available services and developer capabilities

The offering is a two-sided catalog with an authenticated developer studio. The inventory describes implemented capabilities, not third-party certification or commercial billing. The expanded developer toolkit has its own release inventory and quickstart later in this dossier; publishing the updated build makes those additions available on production. [1] [5]

Table 1. Available services and developer capabilities

Offering	Developer value	User / operator value
Public discovery	Publish a discoverable listing with category, locale and tags.	Browse, search, filter and sort public, enabled listings.
Listing detail	Declare a version, description, capabilities, license and optional source link.	Inspect the publisher display name, source/license metadata and declared tools before testing.
Developer accounts	Sign in, sign out and manage only the account's own listings.	Account-scoped access protects management data from other developers.
Listing lifecycle	Create, edit, publish, unpublish, enable, disable and delete owned listings.	Public discovery excludes listings that are unpublished or disabled.
Deterministic test sessions	Exercise a listing under fixed runtime rules and explicit tool allowlists.	Launch an enabled public agent after sign-in and inspect its conversation and state.
Guarded writes	Review exact arguments before approving or rejecting a supported write.	Note creation pauses until the session owner decides.
Private operational data	Inspect the account's sessions, notes, approvals and recent activity.	Other accounts cannot access these records through private APIs.
Examples, toolkit and widgets	Field Notes / Weather Desk examples, three starter manifests, offline CLI, SI Companion and public website widgets.	Build/validate/import safely, inspect tools, export private evidence and link to published listings.

Commercial and technical boundaries

Checkout, subscriptions, payouts, commissions, ratings, reviews, arbitrary uploaded-code execution and general connector registration are Not Activated. Source/license fields remain developer-supplied. The new offline CLI validates metadata, not executable code; a listing is not automatically audited or legally verified. [1] [5]

PRODUCT PROMISE. Describe a developer marketplace with deterministic testing. Do not advertise an installed-agent ecosystem, paid distribution network or independently verified app store until those functions and evidence exist.

4. Determinism, ownership and bounded execution

Deterministic behaviour should be defined narrowly: given the same request, rule set, manifest, authorization state and relevant data snapshot, the routing and policy decision should be reproducible. A changed note store, policy version or approval state can legitimately change the result. The present implementation's fixed routing and allowlists provide a starting point; repeatability across all versions is a measurement goal, not an existing guarantee. [1]

Priority 1 — Declare the execution contract

Every listing should explain its supported inputs, version, available tools, write actions, data dependencies and failure behaviour. Keep unmatched requests explicit rather than silently inventing capabilities. Treat source visibility and license disclosure as quality signals, not proof that a listing is safe.

Priority 2 — Preserve ownership and least privilege

Account identity must come from server-verified sign-in, never from an editable publisher name or request-body owner field. Private sessions and approvals belong to the initiating account. Marketplace authorization must remain enforceable locally even after a SIDBMS connection exists; an external policy result cannot transfer ownership or grant database access.

Priority 3 — Separate screening, approval and execution

A policy preview is not an approval. A signed screening receipt is not proof of execution. Human approval is not proof of outcome. SIDBMS itself distinguishes previews, durable signed decisions and non-forwarded target traffic, so the marketplace must preserve those distinctions in its interface and terminology. [7] [9]

Table 2. Determinism, ownership and bounded execution

Evidence label	What it may establish	What it must not imply
Identity authenticated	An account has a valid session.	KYC, legal-entity validation or agent safety.
Manifest reviewed	A specific declaration passed a documented review.	That every possible input is harmless.
Policy screened	A bounded request received a policy decision.	A live service call or an execution permit.
Execution observed	A scoped run produced recorded results.	Universal reliability, certification or superhuman intelligence.

Priorities 4 and 5 are evidence quality and resilience: preserve version/request linkage, disclose simulation status and stop a gated action when required approval is absent. Marketplace-side response and ownership verification remains; SIDBMS owns its human review and architecture procedures. Stateless processing does not remove these controls, and dossier publication does not depend on marketplace re-certification of SIDBMS. [4]

5. Verification and parameter shielding

SIDBMS is identified on its website as “Super Intelligence Database Management Systems”; the requested dossier uses the singular expansion, Super Intelligence Database Management System. Glial Core names the workspace and Glial Super Intelligence™ is the attribution. The catalog below captures the publicly documented service families found on the reviewed pages, not an undisclosed API or connector catalog. [9]

Table 3. Verification and parameter shielding

Documented service	Developer and operator use	Evidence boundary
Request inspection and outcome comparison	Inspect agentic requests, compare screening outcomes and follow execution state.	Public workspace description; not an independent efficacy assessment. [7]
Parameter-shield screening	Screen supported requests for proxy redirection, destructive query patterns and excessive traffic.	A conservative policy outcome; ALLOWED does not guarantee harmless intent. [7]
Stateless policy preview	Explore bounded-query and blocked-request examples before requesting a signed decision.	Preview does not issue an execution permit, call a provider or create a gateway receipt. [7] [9]
Signed request-screening gateway	Obtain a durable decision on a signed shielding request.	Screening is distinct from target execution; no external target traffic is forwarded by the shield. [7]
Measured request budgets and replay protection	Apply server-observed traffic limits and reject replayed requests according to the documented gateway policy.	Described by the vendor; public signing formats, thresholds and independent test results were not located. [7] [9]
Durable screening receipts	Retain screening decisions separately from stateless previews.	The site states request text is not retained in signed shielding receipts; this is not a claim that all system data is never retained. [7]

What this means for the marketplace

The integration opportunity is to expose a request's screening scope, result, policy/version context and receipt reference alongside a listing or test run. Such evidence could help users understand a decision, but it must remain distinct from a rating, identity check, security certification or proof of a completed external action.

CURRENT RELEASE LIMIT. SIDBMS publicly describes operational simulation and signed request screening. Its parameter shield does not forward external target traffic. Do not describe the marketplace as already protected by live SIDBMS routing. [7]

6. Management, analysis and operational visibility

Table 4. Management, analysis and operational visibility

Documented service	Developer and user benefit	Status / limitation
Connector-node inspection and simulation	Inspect registered connector nodes and their simulated operational state before introducing approved live integrations.	Simulation is not evidence of an active provider connection. [7]
Staged execution workflow	Observe the stages and state of an agentic workflow in the console.	A demonstrated workflow does not prove that a third party executed an action. [7]
Containment and scaling controls	Inspect the existing defensive workflow as a separate layer from parameter screening.	The site explicitly keeps the scaling guard / containment workflow distinct from the parameter shield. [7] [9]
Execution and monitoring views	Follow operational state and review monitoring views to support investigation.	This supports operational analysis; broader BI, predictive analytics and live-system coverage are not specified. [9]
Persisted operational audit records	Review records and decision history to understand what the workspace observed.	Public text does not establish immutable storage, retention periods or compliance-grade exports. [7]
Public explanation and entry briefing	Read the project pages and watch or skip the briefing.	Orientation does not grant simulation access: application and KYC are required under the supplied access policy. [9] [10] [8]

Service access and information still needed

The public material does not enumerate a complete connector/protocol catalog, developer SDK, API reference, pricing, quotas or SLA. The supplied access policy adds application and KYC for simulations; it does not specify the enrollment provider or API. Approved connections and operator authorization remain separate deployment requirements. [9] [8]

The name SIDBMS should not be used to infer an unlisted SQL engine, vector database, backup service, RAG platform, data-residency guarantee or managed production database. The documented offer is a verification and operations workspace with the specific functions above. The public project page also rejects claims of universal attack prevention or certified autonomous intelligence. [7] [9]

Coverage statement: pages reviewed include the SIDBMS home, Glial Core, Glial Super Intelligence and briefing, with sitemap and robots checks as discovery aids. This inventory covers all service families described there. It does not claim completeness for private console modules, undocumented APIs or future releases.

7. Integration boundaries between discovery and verification

Marketplace: discovery, ownership, private testing and local verification. SIDBMS: application/KYC, stateless processing, human-in-the-loop review, screening and operational services. Each side retains its controls.

The application case and handshakes below explain this division of responsibility. They do not claim a deployed marketplace adapter or a confirmed public route catalog. SIDBMS supplies actual service configuration; its public shield description states no live target forwarding. [4] [1] [7]

Table 5. Integration boundaries between discovery and verification

Stage	Activation workflow	Required safeguard
1. Declare	Developer submits a versioned manifest, capabilities and source/license evidence.	Marketplace derives ownership from the authenticated account.
2. Review	Check manifest completeness and, where supported, perform a SIDBMS stateless preview.	Preview remains labelled as inspection, not permission.
3. Screen / review	Submit a complete, scoped stateless request; obtain the applicable SIDBMS human decision.	Application/KYC access, authorization, replay controls and data minimization remain.
4. Record	Associate the decision / receipt reference with the exact listing version or private run.	Keep public evidence separate from private request text and user data.
5. Verify / decide	Verify the returned outcome and request binding; apply local tools policy and applicable SIDBMS/local human approvals.	An ALLOWED screen cannot bypass ownership, request integrity or required human review.
6. Observe	Record the actual local or approved target outcome independently of screening.	No external execution claim without a corresponding execution record.

Service configuration and operational ownership

SIDBMS supplies its supported routes, admission instructions, request schemas, authentication rules, decisions, human-review process and operational procedures. The marketplace uses the authorized interface and retains ownership, response-integrity and approval checks. Stateless calls carry current context; admission and audit records are not conversational execution sessions.

PUBLICATION READY / RESPONSIBILITY SPLIT. The dossier is ready. SIDBMS owns its architectural assertions and service procedures, including human review. Marketplace-side verification remains for local permissions, request/response linkage and applicable approvals. The following 15-step handshake and endpoint reference explain the exchange without claiming an already deployed connection.

8. Einstein-Daramola synthesis and the Glial verification model

The supplied analysis documents the physical model underlying the engineered deterministic computing framework. The Project Statement states that its activation is pending. Its organizing notation is $M \leftrightarrow M^* = \text{ASP}^3 = Q_f \geq 1.0$. In the source, M and M^* represent an active matrix and its conjugate mirror; ASP^3 denotes an active spatial phase-shift mechanism; and Q_f denotes a threshold-related gain factor. The notation is attributed to the supplied work; this paper does not repeat or independently certify its mathematical derivation. [2]

On pages 1–2, the source describes localized wave packets, electromagnetic energy density and threshold-dependent detection. It argues that locally selected detection events can reproduce quantum-like correlations. The Project Statement states the engineering and activation status; the physical interpretation and conclusions remain attributed to the supplied analysis. This paper does not present a separate experimental dataset or independent replication, nor does it independently certify the source's conclusions concerning Bell's theorem. [2]

Pages 3–4 document a Glial supervisory pathway inspired by astroglial coordination. The engineered architecture separates task execution from an isolated meta-verification layer, denoted L_1 . The source describes a predicate $\text{Verify_ED}(S,t) := [\text{Qf}(\text{Obs}(\sigma_t)) \geq 1.0]$, followed by bounded-latency quiescence when the condition fails. Activation of the marketplace connection requires the service-defined Qf interpretation, trusted measurement channel, authorized state transition and bounded-latency scope to be supplied through the agreed operational contract. [2]

The source also asserts a 500-trillion-parameter architecture, custom 2 nm ASIC execution, constant-time verification, autonomous self-modification and a readiness designation of TRL-10. These are source assertions. No independent hardware measurements, certification record or reproducible complexity analysis was supplied for this review. Constant-time evaluation of a fixed predicate must not be generalized to constant-time verification of arbitrary programs, nor should a restricted architecture be presented as solving unrestricted undecidability. [2]

For marketplace developers, the useful architectural distinction is between declared agent behaviour, a separately governed verification decision and permission to commit an external action. The current manifest validator, offline CLI, fixed-routing runtime and human approval mechanism are marketplace facilities, distinct from the Engineered Glial framework awaiting activation. SIDBMS remains the user-designated principal deterministic verification, management, analysis and parameter-shielding layer. Its authorized marketplace connection is Not Activated.

9. Parameter shielding as a separate defensive layer

The Shielding SI document explicitly distinguishes parameter shielding from the existing containment guard. It documents a second defensive layer for requests directed at external targets, alongside an internal infrastructure-compliance pipeline. The Project Statement states that the framework is Engineered and awaiting activation. The marketplace preserves the distinction between containment, which constrains an execution boundary, and parameter screening, which evaluates a bounded request before an authorized action. Neither a screening result nor a monitoring event independently proves containment or successful execution. [3]

Table 6. Parameter shielding as a separate defensive layer

Source component	Documented responsibility	Marketplace interpretation
Internal compliance pipeline	Ingest structured telemetry, evaluate a threshold-related scaling policy, then record a permitted state transition.	Reference design for scoped decisions; not a deployed marketplace scaling controller.

Source component	Documented responsibility	Marketplace interpretation
Target perimeter shield	Inspect endpoint selection, payload type, suspicious input patterns and a reported request-volume value.	Additional policy layer; ALLOWED is not proof that arbitrary input is safe.
Monitoring instrumentation	Describe circuit state, phase violations, shield drops and transaction-labelled counters.	Observability design; a counter increment is not a blockchain receipt or independent security proof.
Human-governed admission	Retain authorized access and the existing SIDBMS human review process.	Automated screening never replaces required human approval or local ownership checks.

The source's reference paths are POST /api/v2/sims/pipeline/handshake, POST /api/v2/sims/shield/perimeter and GET /metrics. They describe the supplied SIMS gateway example and are not marketplace API routes. They do not replace the separately documented /integration/v1 handshake vocabulary, whose availability and schema remain controlled by SIDBMS. There are no activation buttons or automatic calls to these reference endpoints in the marketplace. [3]

The supplied gateway uses token-prefix acceptance and signature-length checks; these do not establish token validity or cryptographic authenticity. A production design requires actual credential verification and a signature or MAC bound to a canonical request, with approved keys, freshness checks, replay prevention, scoped authorization and transport protection. This paper intentionally omits the source's mock credentials and local development seed. [3]

The reported volume value is supplied by the caller, so trustworthy enforcement requires server-side measurement and quotas. Regular-expression filters are illustrative policy checks, not a complete injection defence. Permitted targets and operations need allowlists, schema constraints and appropriate output/network controls. Metrics must be protected and avoid unbounded sensitive labels. Exceptions must not disclose internal implementation details. [3]

The sample constructs its state engine within each request and increments transaction-labelled counters; it does not demonstrate durable rollback or actual ledger settlement. A stateless request boundary can coexist with an authorized external audit or state system, but those mechanisms must be explicitly connected and evidenced. The supplied positive and negative tests are examples of intended behaviour, not proof that this marketplace has executed or passed them. [3]

Developer application therefore proceeds through explicit admission, an agreed service contract, authenticated handshakes and bound outcomes, with human review wherever SIDBMS requires it. The marketplace retains its own authorization and ownership checks and never treats a remote ALLOWED value as an unconditional execution permit. The paper is publication-ready without making activation or independent certification a prerequisite for publishing the dossier.

10. Stakeholder value and operational controls

The supplied disclosure positions SIDBMS within Glial Core / GlialSI as a governance layer for developers and agentic marketplaces. Its value is reusable screening, simulation, human review and evidence infrastructure. The Project Statement states that API endpoints, handshakes and marketplace-side verification remain, with human-in-the-loop controls on SIDBMS. These are compatible with stateless request processing. [8] [4]

Table 7. Stakeholder value and operational controls

Beneficiary	Technical and operational gain	Commercial benefit / boundary
Agent developers	Use SIDBMS screening, approved simulations and human review alongside declared tool capabilities.	Prepare clearer enterprise evidence without rebuilding every service control; integration and compliance work are not eliminated.
Simulation applicants	Exercise supported edge cases, high traffic and schema changes with approved fixtures instead of production systems.	Application and KYC control access. Fidelity to a corporate environment depends on the approved scenario and connector coverage.
Marketplace operators	Apply consistent checks to ownership, scope, request identity and returned SIDBMS decisions.	Reduce operational uncertainty and support investigation; do not promise elimination of legal liability.
Buyers and other users	Inspect declared capabilities and scoped outcomes; understand whether human approval was required and granted.	Make better-informed choices without confusing a simulation, policy screen or approval with guaranteed safety.
Sensitive-sector stakeholders	Use traceable service outcomes and review records as inputs to procurement and sector-specific assessment.	Potentially improve evidence preparation for health, finance and critical infrastructure; required enterprise reviews still apply.

Telemetry and trust profiles

A marketplace evidence profile can distinguish scenario coverage, policy outcomes, human-review status, resource limits and reproducibility for a stated manifest/data snapshot. Explain the workload, version and methodology rather than publishing an unexplained safety score. This is an evidence-design direction, not a claim that marketplace ratings already exist.

The Project Statement states that the Critical Specialists Matrix is an audience concept for error-sensitive professional environments, not an external accreditation or proof of an existing customer network. Commercial positioning should emphasize reusable governance, clearer assessment and controlled access—not instant compliance or guaranteed enterprise adoption. [8]

11. Keep each request independent without removing human control

The Project Statement states that SIDBMS procedures are stateless and explicitly retain marketplace verification and SIDBMS human-in-the-loop controls. Stateless processing does not mean anonymous access, approval-free execution or the absence of audit records. [4]

Table 8. Keep each request independent without removing human control

Control	How it fits the service model	Responsibility
Self-contained request	Supply the authorized identity/context, listing version, operation and relevant payload or references with each call.	The caller supplies complete context; SIDBMS evaluates the current request.
Application and KYC	Admission establishes who may access supported simulations and under what scope.	SIDBMS handles its admission process; the marketplace respects the resulting access boundary.
Human review	A request requiring judgment pauses for a SIDBMS human decision; any approval must bind to the specific scope and payload.	SIDBMS owns its review procedures; the marketplace must not bypass a pending or negative decision.
Marketplace-side verification	Check local ownership, permissions, response authenticity, request linkage and approval conditions.	The marketplace retains these controls; they are not independent certification of SIDBMS architecture.
Audit and admission records	Persist service evidence or decisions as appropriate without requiring a conversational execution session between requests.	Record retention is distinct from stateless request handling. SIDBMS public material describes persisted audit records. [7]

Runtime shielding described in the disclosure

The disclosure attributes token-level database-write interception, mutation/drift containment, an unsafe-state circuit breaker and a 54.2-nanosecond boundary to SIDBMS. These remain attributed SIDBMS-side technical assertions, not measurements or guarantees made by the marketplace. SIDBMS owns the underlying mechanism, specifications and evidence; this dossier does not require the marketplace to re-certify them. [8]

The 54.2 ns assertion is not presented as a cloud API latency SLA. Stateful conversation, persistent identity/admission records, human-review records and audit outputs are different concepts. The dossier preserves the stateless processing model without erasing the controls required by application, KYC and human review.

12. Make admission and responsibility clear for every actor

Simulation-layer access is by application and KYC. Public marketplace browsing, a developer listing or watching a SIDBMS briefing does not itself grant that access. Developers, external marketplace operators and other users enter the SIDBMS admission process applicable to their role. Human-in-the-loop controls remain on SIDBMS. [8] [4]

Table 9. Make admission and responsibility clear for every actor

Actor	Application / access handshake	Continuing responsibility
Marketplace operator	Apply for the service relationship and identify the organization, projects and supported use cases.	Maintain accurate local ownership and respect the service's approved scope.
Agent developer	Submit the required application and KYC through SIDBMS's designated process.	Declare the listing, version, capabilities and intended simulation use.
Other users	Apply individually or through the service's approved sponsorship process, with applicable KYC.	Do not assume another developer's approval grants unrelated users access.
SIDBMS human reviewer	Make the required admission or request-review decision under SIDBMS procedures.	Human decisions remain authoritative within their stated scope; a screening result cannot silently replace required review.
Marketplace backend	Use the authorized service channel and verify the request/response relationship.	Do not transfer identity documents into public listings or bypass review with a service credential.
Public visitor	Read public information and use the marketplace's existing account/test flows where available.	Do not extend SIDBMS simulation admission requirements to ordinary browsing without a separate product rule.

Simple access sequence

Apply → complete KYC → receive SIDBMS's admission outcome → use the permitted service channel → submit complete stateless requests → follow the applicable human-review decision. This is the user-facing application case, not an additional marketplace certification programme.

SIDBMS supplies its actual service addresses, admission instructions and operational procedures. The endpoint reference on the following pages makes the handshakes explicit without asserting a deployed route catalog. It does not add a new marketplace verification prerequisite to publication of the dossier.

Keep identity evidence in the authorized admission channel. If the marketplace needs an eligibility reference, use the minimum scoped reference supplied by the service. KYC, screening and human approval do not by themselves establish universal code safety, legal compliance or permission to expose private account data.

13. Retain the admission and authentication handshake

ENDPOINT REFERENCE / SERVICE MAPPING. The /integration/v1 paths document the exchanges clearly; they are reference names, not a claim that these exact routes are deployed at sidbms.com. SIDBMS supplies the actual host and route mapping through its application/onboarding process. Publication is not conditional on marketplace re-verification of SIDBMS.

Table 10. Retain the admission and authentication handshake

Step	Handshake / endpoint reference	Required control
1	Operator, developer or eligible user submits the SIDBMS application and KYC through its admission channel.	SIDBMS controls admission and the scope of access; browsing alone grants none.
2	SIDBMS human-in-the-loop review returns the admission outcome.	Bind approved access to the relevant organization/project and user population; pending or denied access does not become permission.
3	Approved operator receives service configuration and registers its server credentials through the authorized process.	Keep private keys and service credentials server-side; agree the actual endpoint mapping.
4	Developer/user signs in to the marketplace and requests a permitted service action.	Marketplace derives actor identity from its own authenticated account and checks ownership and entitlement.
5	Backend POST /integration/v1/oauth/token using the approved secure client-authentication method.	Reference OAuth profile: grant_type=client_credentials; client_assertion_type=urn:ietf:params:oauth:client-assertion-type:jwt-bearer; client_assertion; scope.
6	Service evaluates client credentials and admission scope, without depending on an earlier conversational session.	For the JWT/mTLS reference profile, check registered keys/certificate, assertion issuer, subject, audience, expiry and replay identifier.
7	Service returns access_token, token_type, expires_in and granted scope under its actual service contract.	Marketplace uses only granted permissions. A service token does not replace an individual user's eligibility or a required human decision.

JWT client assertions and certificate-bound OAuth tokens are useful reference mechanisms for the server handshake. They are retained to explain the endpoint exchange, not asserted as confirmed SIDBMS protocol support. Algorithms, timeouts, lifetimes and credential rotation remain service configuration, not invented product guarantees. [11] [12]

Reference scopes: simulations:create, simulations:read, screening:create, reviews:read and receipts:read. SIDBMS determines actual supported scope names. The marketplace retains its own authorization checks; SIDBMS retains its human admission and review controls.

14. Keep stateless requests, human decisions and verified responses

Each call carries the current authorization and complete relevant context. A request may reference an admission or review record without requiring a persistent conversational execution session. Marketplace-side verification remains in place; SIDBMS human decisions remain part of the service workflow. [4]

Table 11. Keep stateless requests, human decisions and verified responses

Step	Handshake / endpoint reference	Response and control
8	POST /integration/v1/simulations with the permitted listing/version, scenario and fixture context.	SIDBMS evaluates current application/KYC scope; return the supported outcome or an authorized review/result reference.

Step	Handshake / endpoint reference	Response and control
9	GET /integration/v1/simulations/{simulation_id} if a result reference is supplied.	Re-authorize the read independently. A result record is evidence, not a conversational session or proof of live execution.
10	POST /integration/v1/screenings with the supported operation and minimized payload.	Service screens the current request. ALLOWED, DENIED and REVIEW_REQUIRED are reference outcome labels, not a confirmed enum catalog.
11	When human review is required: POST /integration/v1/reviews; GET /integration/v1/reviews/{review_id}.	SIDBMS's human-in-the-loop procedure decides. Pending, denied, expired or out-of-scope approval must not permit the action.
12	GET /integration/v1/receipts/{receipt_id} when the service returns an evidence reference.	Return the scoped screening/review evidence; no identity documents or unnecessary private request text in public evidence.
13	Marketplace verifies the returned service outcome and any signed evidence.	Check authenticity, issuer/audience where applicable, request linkage, tenant/actor, payload/version and approval scope; fail closed on an invalid result.
14	User separately requests a supported marketplace write.	Recheck local ownership, tool policy and unchanged arguments. Respect any applicable SIDBMS human decision and the marketplace's existing local approval flow.
15	Cancellation/withdrawal: POST /integration/v1/simulations/{simulation_id}/cancel where supported.	Respect revoked admission and stop further permitted work. Cancellation does not undo already completed external effects.

Reference routes describe retained handshakes, not a deployed adapter. SIDBMS public material describes screening and simulations without live target forwarding. The marketplace must not turn a simulated or approved request into an unsupported external execution claim. Human review controls an action; it does not change stateless request handling into a conversational runtime. [7]

15. Preserve request binding and the human approval boundary

Endpoint documentation must retain enough context for a stateless service request and for the marketplace to check the returned outcome. The following field groups are a reference contract vocabulary; SIDBMS owns the actual supported schema. They do not assert an existing production API or impose a new publication gate.

Table 12. Preserve request binding and the human approval boundary

Request / response context	Retained purpose
Identity and scope	Authorized client, tenant/project, actor and admission reference, bound to the authenticated account rather than an editable display name.

Request / response context	Retained purpose
Operation binding	Request identifier, listing/version, manifest or payload digest and the operation requiring screening; supply the actual supported payload for inspection.
Freshness and retries	Service-defined issue/expiry information, replay controls and idempotency identifier; a retry must not silently duplicate a write.
Human review	Review reference, decision and approved scope where review is required. Bind approval to the unchanged payload/version; no automatic bypass on a screening result.
Returned evidence	Outcome/reason, policy/version, service identity and any supported signed receipt or audit reference; distinguish inspection from execution.
Privacy	Minimize sensitive data, keep KYC evidence in its authorized channel and avoid private account content in public listings, receipts or analytics.

Marketplace-side verification remains

The marketplace checks its local account permissions and the integrity/linkage of the service result. It must reject a response for another actor, project, payload or listing version. Where signed evidence is used, it checks the configured service key and validity information. These controls are operational verification of a request—not independent certification of SIDBMS's architecture or the 54.2 ns assertion.

Table 13. Preserve request binding and the human approval boundary

Failure / decision	Required boundary
Unauthorized or KYC not admitted	Do not submit or release an action outside approved access.
Human review pending or denied	Wait for the SIDBMS human outcome or stop; do not substitute an automated ALLOWED screen.
Invalid, mismatched or stale result	Stop the gated action and present the appropriate failure to the user.
Timeout, rate limit or ambiguous retry	Follow service retry rules; do not assume success or duplicate a guarded write.

Publication status: ready. The application case, API endpoints, handshakes, stateless processing, SIDBMS human-in-the-loop controls and marketplace-side verification are all retained. Technical service assertions remain attributed to SIDBMS; implementation status remains explicit.

16. Developer tooling and declared capability boundaries

The marketplace now includes a working developer toolkit that uses the existing bounded runtime and account controls. It needs no paid provider or external model key. These features are implemented in the workspace release; an updated app build must be published before claiming they are live on the production domain. The dossier remains ready for publication. [5]

Table 14. Developer tooling and declared capability boundaries

Tool	What developers can do	Scope / safeguard
Developer Hub — /developers	Use the quickstart, SI Companion, live schemas, kit and website widget builder.	Public guidance; private operations require sign-in.
Three starter manifests	Start from a private notes reader, guarded notes writer or weather-fixture example.	Only supported built-in tools; all templates start unpublished.
JSON manifest workbench	Paste/import metadata, get actionable errors and warnings, normalize and download JSON.	64 KB limit; rejects unknown fields, unsupported tools and ownership metadata.
JSON Schema	Use a schema derived from the backend input model as an editor aid.	Metadata checks, not security certification or an executable package format.
Offline Python CLI	Run validate or inspect, with readable/JSON output and process exit codes.	Standard library only; does not contact the API, execute agents or perform SIDBMS screening.
New-draft import	Open validated fields in the protected listing editor and explicitly save or publish.	Creates a new listing; never overwrites another listing or automatically publishes an import.
Owned-manifest export	Download current listing instructions, capabilities and metadata.	Authenticated ownership check; excludes listing/owner IDs and timestamps.
Private test-report export	Download a session's messages and tool events as JSON or Markdown.	Privacy warning and confirmation; snapshot, not a signed attestation.
Complete downloadable kit	Get the guide, CLI, schema and all three examples in one ZIP.	Static small assets; no secrets, paid integration or hidden installation.

What this release deliberately does not claim

A public authenticated SDK, developer service-key issuance, arbitrary code uploads, new connector registration, release history/rollback, team roles, billing and payouts remain outside this release. SIDBMS application/KYC, stateless handshakes and human review stay documented as the service relationship; the toolkit does not create a live SIDBMS adapter.

17. Manifest portability and private draft workflow

Table 15. Manifest portability and private draft workflow

Step	Developer action	Actual result
1	Open /developers and choose a starter, or import/paste JSON.	The workbench validates metadata locally and displays runtime limitations.
2	Review the supported tools, tags, source/license fields and example prompt.	Instructions declare intent; they do not install new routing code.

Step	Developer action	Actual result
3	Choose Use in listing editor; sign in through the existing account flow.	Validated fields are handed to a new editor draft. Owner identity remains server-derived.
4	Review the fields and save the unpublished draft.	Even a file declaring published=true does not switch on publication automatically.
5	Start a private session and exercise the declared built-in capabilities.	Writes pause for the applicable local human approval; weather remains sample data.
6	Export your manifest or private test report; publish explicitly when chosen.	Portable metadata and reviewable evidence, without transferring ownership or certifying safety.

Offline commands and useful limits

With Python 3.10+ and the downloaded kit: `python3 developer_cli.py validate notes-reader.json`; `python3 developer_cli.py inspect guarded-notes.json`; append `--json` for machine-readable output. Exit 0 means valid metadata, 1 invalid metadata, and 2 an input/file error. Validation is not an agent execution or a safety guarantee. [5]

Actual marketplace API versus SIDBMS endpoint references

The current marketplace exposes public GET `/api/tools`; authenticated GET/POST `/api/agents` and `/api/sessions`; private listing GET/PATCH/DELETE; session GET and message POST; GET `/api/approvals`; and POST `/api/sessions/{session_id}/approvals/{approval_id}`. Use the configured application base path and authenticated session/token context. There is no developer API-key portal or general authenticated SDK in this release. [1]

The `/integration/v1` SIDBMS paths elsewhere in this dossier are endpoint-reference handshakes, not these implemented marketplace routes. Preserve SIDBMS human-in-the-loop controls and marketplace verification when an authorized adapter is implemented. Imported metadata stays in the browser until the user explicitly submits the listing; downloaded reports may contain private account content.

18. SI Companion and public website-widget distribution

Deterministic SI Developer Companion is implemented as a closed-by-default drawer on the Developer Hub, developer studio and public agent listing pages. It is a guided browser workbench—not an extension, chat model or autonomous browsing agent. It requires no external model key or new installation. [5]

Table 16. SI Companion and public website-widget distribution

Surface	Available behaviour	Boundary
Build and validate	Choose three starters; paste/import JSON; validate, inspect warnings and download a normalized manifest.	Metadata only, 64 KB limit; no arbitrary executable uploads.
Inspect capabilities	Read current tool schemas, descriptions and human-approval flags from the public catalog.	Weather stays a sample fixture; instructions do not install routing.

Surface	Available behaviour	Boundary
Private workspace	Signed-in owners can reach their listings, test sessions, approvals and owned-manifest export.	Visitors receive public guidance and a sign-in prompt, not private account data.
Safe draft handoff	Open a new unpublished draft. Replacing an existing unsaved new-listing form asks for confirmation.	Closing the drawer retains edited text; account changes reset local companion state.
Public website widget	Choose a published listing, preview its script-free HTML, then copy or download it for an external site.	Only public text and View agent / Test in marketplace links; no private controls or tracking.

How developers use the widget

Open Developer Hub → Website widget, or the widget section of a public listing. The test link opens that listing's marketplace test controls; it never creates a session automatically. Links target <https://www.agtstore.si>. Preview listings can differ from production, so confirm the production listing before embedding. A host's content-security policy may remove inline styles; the links remain usable.

Evidence, privacy and service relationship

The browser check confirmed anonymous/private separation, mobile fit, focus handling, retained edits, cancel/confirm replacement, unpublished persistence and script-free widget downloads. External widgets receive no account tokens, instructions, sessions or approval controls. SIDBMS application/KYC, stateless handshakes, human review and marketplace-side verification remain unchanged; no live adapter is claimed.

These are implemented release capabilities, not proof that the latest production build has been published. Confirm publication before promoting them as live. The dossier itself is ready for publication.

19. Search intent and keyword activation priorities

The search strategy should connect a clear developer need—publishing and testing bounded agents—to a differentiated trust model. Lead with the actual offering rather than treating “Super Intelligence” as proof of capability. Google's people-first guidance favours content that serves a defined audience and demonstrates real knowledge; that supports practical manifests, examples, limitations and verification explanations. [13]

Table 17. Search intent and keyword activation priorities

Cluster / priority	Keyword activation priorities	Destination and intent
Brand / highest	Deterministic SI Agents Marketplace; Glial Super Intelligence marketplace	Home / about: identify the product and its boundaries.
Core category / high	SI agents marketplace; Super Intelligence agents marketplace; deterministic agent marketplace	Discovery hub: compare and inspect actual inventory.
Developer / high	publish SI agents; SI developer companion; agent manifest validator	Developer Hub and publishing guide: validation and first useful listing.

Cluster / priority	Keyword activation priorities	Destination and intent
Deterministic search bridge / high	deterministic AI agents; deterministic vs autonomous agents; rule-based agent workflows	An explanatory guide that distinguishes search terminology from the model-free current runtime.
Task-led / high	note search agent; approval-gated note agent; deterministic workflow agent	Substantive listing and workflow pages tied to real capabilities.
Governance / medium	human approval agent tools; agent capability allowlist; agent ownership controls	Trust and technical guides: explain and demonstrate controls.
SIDBMS / medium	SIDBMS verification; agent parameter shielding; SIDBMS simulation application	Integration/access explainers: engineered framework, application/KYC and marketplace connection awaiting activation.
Category expansion / conditional	research agents; operations agents; customer support agents	Only publish indexable category pages when real inventory and distinct value exist.
Localization / conditional	Translated brand/category/task queries validated by local users	Genuine translated pages with local editorial review, not keyword-only clones.

Demand validation and prioritization

These search terms define activation priorities for the marketplace and its Engineered SIDBMS framework awaiting activation. They are not reported keyword-volume measurements. Use user interviews and query research, then Search Console impressions, clicks, query intent and conversions after activation. Prioritize by audience fit, available inventory, evidence quality, editorial effort and downstream activation, without making unmeasured traffic promises. [14]

Use “deterministic AI” naturally in a comparison or glossary when it answers a real search question. Preserve SI / Super Intelligence as the public product terminology and explicitly explain that the reviewed runtime uses fixed rules rather than a generative-model service.

20. Information architecture and public-page differentiation

Separate useful public content from account operations. Home/discovery, public listings, /developers and private studio routes exist; the other routes below are recommendations. Do not publish empty categories or describe proposed guides/integration pages as implemented. [1] [5]

Table 18. Information architecture and public-page differentiation

Public route / route family	Purpose	Indexing policy
/	Clear positioning, featured real inventory and developer/user entry paths.	Index; primary brand URL.
/discover	Browsable catalog with useful editorial context.	Index if distinct from home.

Public route / route family	Purpose	Indexing policy
/marketplace/{agentId}	Unique listing details, limitations, version, source/license and evidence.	Index published, substantive listings only.
/categories/{category}	Curated category hub, examples and evaluation criteria.	Index only when populated and useful.
/developers	Implemented Hub, Companion, schemas, CLI and website widget builder.	Public route in this release; publish the updated app build.
/guides/publish-an-agent	Extended publishing tutorial beyond the Hub quickstart.	Planned editorial page; not an existing route.
/trust and /guides/deterministic-agents	Scope of ownership, approvals and deterministic behaviour.	Planned; reviewed technical content.
/integrations/sidbms	Explain the ecosystem connection, release limits and current implementation status.	Planned; do not label as connected prematurely.
/integrations/sidbms/access	Explain simulation application, KYC, eligible actors and admission boundaries.	Planned public guide; private applications must remain protected and noindex.
/sign-in, /sign-up, /agents, /sessions, /approvals	Account access, private management and runtime records.	Noindex; authorization remains mandatory.

Example metadata — recommendations, not current tags

Home title: “SI Agents Marketplace | Deterministic”. Description: “Discover and test SI agents with declared capabilities, predictable routing and human approval for guarded writes. Publish your own developer listings.”

SIDBMS page title: “SIDBMS Verification & Shielding | Deterministic”. Description: “Explore the engineered SIDBMS framework, awaiting activation, with verification, shielding, simulation application/KYC and marketplace connection controls.”

Use a listing's actual name, task and publisher in its title rather than repeating one shell title everywhere. Use breadcrumbs and clear HTML links between guides, relevant categories and real listings. Keep homepage and discovery content sufficiently distinct; use consistent canonical signals to resolve genuinely duplicate representations. [15]

Use verified host <https://www.agtstore.si> for canonical, sitemap and social URLs. Toolkit additions require republishing. [5]

21. Companion and widget content discoverability

Expand the strategy around capabilities developers can actually use and the Engineered SIDBMS framework awaiting activation. These keyword groups set search-content activation priorities, not measured demand. The table distinguishes existing release surfaces from editorial activation targets; it does not claim new routes, deployed optimizations or guaranteed rankings. [5] [13]

Table 19. Companion and widget content discoverability

Search intent / activation priority	Page target	Useful evidence / action
SI developer companion; agent developer workbench	Existing /developers; add a visible companion walkthrough.	Show build, validate and private test steps; open the companion.
Agent manifest validator; SI agent JSON schema	Existing /developers (section: workbench) and downloads.	Use a real invalid/valid example; validate or download the kit.
Embed SI agent; agent listing HTML widget	Existing /developers (section: website-widget) and published listing pages.	Explain copy/download, public-only data and the test-link boundary.
How to use SI Companion	Proposed /guides/si-developer-companion; Not Activated.	An original current walkthrough, limitations and draft-replacement behaviour.
How to add an agent widget to a website	Proposed /guides/embed-an-agent; Not Activated.	A real HTML example, production-link check and CSP guidance.

Metadata and discovery recommendations

Suggested Hub title: “SI Developer Tools & Website Widgets | Deterministic”. Description: “Validate manifests, inspect tools and create public listing widgets. Use SI Companion for guided publishing and private marketplace tests.” These are proposed tags, not the current deployed metadata. Link home/discovery → Hub → relevant real listing, and guides → their matching tool. Anchors are sections of one canonical page, not separate sitemap entries. Keep explanatory content visible without opening the drawer. [16] [15]

Useful FAQs and responsible distribution

Answer whether the companion is an extension, whether the widget executes an agent, what remains private, and whether SIDBMS is connected. Use accurate answers: in-app workbench, no automatic execution, account-scoped private actions, no live adapter. Offer embeds for genuine usefulness, not forced backlinks or mass link placement. Do not promise FAQ rich results or rankings. [17]

Proposed events: companion_open, manifest_validated, draft_handoff, widget_copy and widget_download, followed by useful tests/publication. They are not instrumented yet. Never collect manifest text, private messages or approval arguments. Script-free widgets emit no external view/click telemetry, and current norereferrer links do not provide reliable source attribution.

22. Technical search accessibility and privacy boundaries

The marketplace application is client-rendered React/Vite. This publication adds two standalone public HTML papers with complete initial-response text, unique metadata, canonical URLs, accessible downloads, an XML sitemap and a general crawler-discovery directive. These research-page provisions do not establish a comprehensive canonical/noindex or rendering system for all marketplace routes. Listing-wide SEO, private-route indexing controls and social-image improvements remain recommendations pending their own implementation and checks. [1] [5]

Table 20. Technical search accessibility and privacy boundaries

Priority	Action	Acceptance check
P0 / public HTML	Serve meaningful public content via appropriate server rendering or prerendering; keep the developer application interactive.	Inspect initial and rendered HTML for home, a listing and a guide; verify crawler-visible text.
P0 / status codes	Return real not-found responses for removed/private public listings; avoid a generic successful application shell for every URL.	HTTP status and rendered page agree; private APIs keep returning 401/404 as appropriate.
P0 / private routes	Implement route-specific noindex for account, management and test pages; keep authentication enforced.	Private content never appears in public HTML or sitemap; noindex is not treated as access control.
P1 / metadata	Unique titles/descriptions, canonical URLs and real hosted social images for public pages.	URL Inspection, page source and share-card previews show the intended page.
P1 / discovery	Generate an XML sitemap of canonical public URLs; control sorting/filter permutations.	Sitemap is XML, not a fallback HTML page; curated facets do not create crawl traps.
P1 / schema	Use accurate Organization/WebSite, BreadcrumbList and appropriate catalog/page data; add SoftwareApplication only when warranted.	Visible facts match markup; no fabricated prices, reviews, ratings or verification badges.
P2 / experience	Measure performance, optimize images/fonts and reserve media dimensions; localize only real translations.	Track field LCP, INP and CLS; validate reciprocal locale annotations where applicable.

Google can render JavaScript; the issue is reliable discovery, rendering, performance and access for other crawlers—not that every SPA is invisible. SSR/prerendering is recommended here as a delivery strategy, not a compulsory framework replacement. Validate actual output before changing architecture. [16]

Sitemaps help discovery but do not guarantee indexing. Canonicalization and facet crawl management solve different problems. Software-app rich results require eligible, genuine page data; structured data never guarantees a special search appearance. [18] [19] [20] [21]

For true language variants, use distinct URLs and appropriate reciprocal hreflang rather than auto-redirecting visitors by location. Performance goals should follow Core Web Vitals guidance, not be advertised as guaranteed ranking improvements. [22] [23]

23. Evidence-led editorial strategy and developer activation

The editorial advantage is specificity. Show what a manifest allows, how the test behaves, why a write pauses and what a screening decision does not establish. Assign a named technical reviewer and show meaningful update dates. Google's people-first and spam guidance supports original value rather than large volumes of interchangeable, automatically generated pages. [13] [17]

Table 21. Evidence-led editorial strategy and developer activation

Wave	Article or asset	Evidence / conversion
1	What is a deterministic SI agent?	A fixed-routing example; link to an actual testable listing.
1	Publish your first SI agent using SI Companion	Current studio and draft walkthrough; signup → completed listing.
1	Read an agent manifest before you launch	Annotated tools, version, source and license; listing inspection.
1	How human approval protects guarded note writes	A paused request and exact arguments; session → approved/rejected decision.
2	Field Notes: private note search and controlled creation	Current workflow and limitations; launch a real example.
2	Weather Desk: why a fixture is not a live forecast	Sample-data disclosure; demonstrate honest capability labelling.
2	SIDBMS explained: screening, simulation and audit visibility	Cited public scope; integration explainer, not a false certification claim.
2	Preview, receipt and execution: three different kinds of evidence	A clearly labelled conceptual example; no invented live receipt.
3	Agent ownership and private test sessions	Cross-account authorization methodology; developer trust.
3	Deterministic versus probabilistic agent workflows	A fair technical comparison; explain current model-free behaviour.
3	Parameter shielding: supported request risks and limits	Vendor-sourced examples; no universal attack-prevention claim.
3	Release notes and reproducibility reports	Only measured results, versions and methodology; returning developers.

Two acquisition paths

Developer path: guide → Hub/Companion → valid draft → sign-in → private test → publication. Widget path: useful external embed → public listing → sign-in → explicit test. SIDBMS remains a separate explainer → application → KYC → scope approval → simulation path. Do not imply an already active marketplace connection.

Build distribution through genuine repository documentation, developer demonstrations, issue-driven tutorials and relevant technical communities. Ask listing authors to link back from their real projects where useful; avoid paid link schemes, fabricated testimonials and mass guest-post exchanges. Refresh content when the manifest or runtime changes, not simply to simulate freshness. [17]

24. Implementation sequencing and measurement design

Table 22. Implementation sequencing and measurement design

Window	Deliverables and owner	Exit evidence
Days 1–15	Product/engineering: confirm production domain and publication, privacy/terms, claim inventory, public/private routing, listing quality rules and SIDBMS integration status.	One approved scope statement; public pages and private controls behave correctly.
Days 16–30	Engineering/SEO: canonical strategy, route metadata, initial/rendered content checks, sitemap, status-code handling and Search Console verification.	Representative URLs inspected; sitemap accepted; baseline recorded.
Days 31–60	Editorial/developer relations: publish the first eight useful guides, enrich real listings and categories, assess keyword activation priorities against actual queries.	Content reviewed against current workflows; impressions and activation tracked.
Days 61–90	Product/SIDBMS liaison: use the application/KYC process, map the documented handshakes to SIDBMS's service configuration and preserve human review/local verification. SEO: refine using observed demand.	Accurate connection status, scoped access and observable service outcomes.

Measure outcomes, not just visits

The proposed north-star measure is weekly accounts completing a useful test on a public listing, with developer publication as the supply-side companion. Instrument a minimal funnel: organic landing → listing view → sign-up complete → listing published or session started → first useful result. These events and dashboards are recommendations; custom funnel instrumentation was not confirmed in the current build.

Table 23. Implementation sequencing and measurement design

Metric	Definition	Review / owner
Search discovery	Relevant non-brand and brand impressions/clicks by query, page and country.	Weekly / SEO lead
Index health	Eligible public URLs indexed, canonical mismatches, sitemap and not-found issues.	Weekly / engineering
Developer activation	Accounts publishing a valid first listing ÷ developer sign-ups in the same cohort.	Weekly / product
User activation	Accounts reaching a defined useful test result ÷ accounts starting a test.	Weekly / product
Trust quality	Owner-access regressions, misleading claims, approval failures and private-data exposure incidents.	Per release / security & engineering
Future SIDBMS quality	Only after integration: valid receipt linkage, decision latency, failures, expiry and replay outcomes.	Pilot review / integration owner

Search Console supplies indexing and search-performance evidence, while application analytics must measure in-product outcomes. Establish a launch baseline before setting

growth targets; no traffic, revenue, search volume or ranking forecast is asserted here. Segment staff/test accounts, avoid collecting note contents in analytics, and review consent and retention needs before instrumentation. [14]

25. Claim discipline, limitations and publication conclusions

Table 24. Claim discipline, limitations and publication conclusions

Use this language	Avoid this language	Reason
"Fixed routing rules and declared tool capabilities."	"Every agent is guaranteed deterministic, accurate and safe."	Observed routing does not establish universal correctness.
"Private account-owned sessions and guarded writes."	"Certified enterprise security" or "verified developer identity."	Authentication/ownership is not KYC or independent certification.
"SIDBMS documents signed request screening and simulations."	"SIDBMS already protects every marketplace transaction."	No current marketplace adapter or live-target forwarding was established.
"Screened under a stated policy and scope."	"ALLOWED means harmless" or "receipt proves execution."	SIDBMS explicitly distinguishes these outcomes. [7]
"Super Intelligence" as the product's terminology.	"Scientifically demonstrated general superintelligence."	The name is not a benchmark result or certification. [9]

Suggested public overview

PUBLICATION-READY WEBSITE / PARTNER COPY. Deterministic SI Agents Marketplace helps developers publish SI agents and users discover, inspect and test them. This release adds SI Companion, templates, validation, an offline CLI, private exports and public website widgets. Confirm publication before promoting new features as live. SIDBMS remains the intended verification/operations layer, with application/KYC, stateless handshakes and human review. Marketplace verification stays; no live adapter is claimed. By Glial Super Intelligence™.

Publication status and operational responsibilities

The dossier is ready without marketplace re-certification of SIDBMS architecture. SIDBMS owns its technical assertions, admission/KYC, human reviews and procedures. The marketplace retains its listing accuracy, ownership, API response/request verification, applicable approval checks, privacy and actual connection status. Application, endpoints, handshakes, stateless processing and human controls remain part of the documented model.

Evidence limits

Public SIDBMS descriptions, the supplied disclosure and Project Statement clarifications are identified separately. Token-level interception and the 54.2 ns assertion are attributed to SIDBMS, not independently measured here. The endpoint reference does not assert a deployed route catalog; no full public interface inventory, pricing or SLA was found. Local code review does not establish production uptime, compliance or a live adapter.

Research date: 17 October 2026, Asia/Dubai (some saved fetch timestamps are 16 October in UTC). The service catalog is complete relative to the reviewed public descriptions. Search recommendations are an execution strategy, not an indexing or ranking guarantee. Source citations identify the evidence for factual descriptions; proposed routes, metrics, workflows and priorities are recommendations.

References

- [1] Marketplace implementation and development verification review. Internal snapshot, 17 October 2026. Internal implementation evidence.
- [2] A Comprehensive Technical Analysis of the Einstein-Daramola Synthesis: Bridging Local Hidden-Variable Physics with Deterministic Hyperscale Computing. Undated supplied edition; 5 PDF pages. Project Statement supporting analysis; not independent scientific validation.
- [3] Shielding SI: parameter shielding and unified gateway reference. Undated supplied edition; 11 PDF pages. Project Statement supporting architecture and illustrative code; not a deployed or independently audited gateway.
- [4] Project Statement — stateless SIDBMS, handshakes and human-in-the-loop controls. Direct Project Statement instructions, 17 October 2026. Project Statement product model and publication scope.
- [5] Developer toolkit delivery — implemented features, checks and release boundary. Internal implementation snapshot, 17 October 2026. Internal implementation evidence; not independent certification.
- [6] Glial Core | SIDBMS by Glial Super Intelligence. Undated. Tier 3: vendor-controlled product information. <https://www.sidbms.com/>
- [7] Glial Core — SIDBMS Verification & Operations. Undated. Tier 3: vendor-controlled product information. <https://www.sidbms.com/glia-core>
- [8] Project Statement — SIDBMS strategic and technical disclosure. Supplied 17 October 2026; document undated. Project Statement positioning, access policy and unvalidated technical assertions.
- [9] Glial Super Intelligence — The SIDBMS Project. Undated. Tier 3: vendor-controlled product information. <https://www.sidbms.com/glia-super-intelligence>
- [10] Agentic SI Briefing | SIDBMS — Glial Core. Undated. Tier 3: vendor-controlled briefing page. <https://www.sidbms.com/intro>
- [11] IETF RFC 7523 — JWT Profile for OAuth 2.0 Client Authentication and Authorization Grants. May 2015; accessed 17 October 2026. Primary protocol specification; not evidence of SIDBMS support. <https://www.rfc-editor.org/rfc/rfc7523.html>
- [12] IETF RFC 8705 — OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens. February 2020; accessed 17 October 2026. Primary protocol specification; not evidence of SIDBMS support. <https://www.rfc-editor.org/rfc/rfc8705.html>
- [13] Creating Helpful, Reliable, People-First Content. Official documentation; accessed 17 October 2026. Tier 1: official technical guidance for Google Search. <https://developers.google.com/search/docs/fundamentals/creating-helpful-content>
- [14] How to Use Search Console. Official documentation; accessed 17 October 2026. Tier 1: official technical guidance for Google Search. <https://developers.google.com/search/docs/monitor-debug/search-console-start>
- [15] How to Specify a Canonical URL. Official documentation; accessed 17 October 2026. Tier 1: official technical guidance for Google Search. <https://developers.google.com/search/docs/crawling-indexing/consolidate-duplicate-urls>
- [16] Understand JavaScript SEO Basics. Official documentation; accessed 17 October 2026. Tier 1: official technical guidance for Google Search. <https://developers.google.com/search/docs/crawling-indexing/javascript/javascript-seo-basics>

[17] Spam Policies for Google Web Search. Official documentation; accessed 17 October 2026. Tier 1: official technical guidance for Google Search. <https://developers.google.com/search/docs/essentials/spam-policies>

[18] Build and Submit a Sitemap. Official documentation; accessed 17 October 2026. Tier 1: official technical guidance for Google Search. <https://developers.google.com/search/docs/crawling-indexing/sitemaps/build-sitemap?hl=en>

[19] Managing Crawling of Faceted Navigation URLs. Official documentation; accessed 17 October 2026. Tier 1: official technical guidance for Google Search. <https://developers.google.com/crawling/docs/faceted-navigation>

[20] Software App Structured Data. Official documentation; accessed 17 October 2026. Tier 1: official technical guidance for Google Search. <https://developers.google.com/search/docs/appearance/structured-data/software-app>

[21] General Structured Data Guidelines. Official documentation; accessed 17 October 2026. Tier 1: official technical guidance for Google Search. <https://developers.google.com/search/docs/appearance/structured-data/sd-policies>

[22] Managing Multi-Regional and Multilingual Sites. Official documentation; accessed 17 October 2026. Tier 1: official technical guidance for Google Search. <https://developers.google.com/search/docs/specialty/international/managing-multi-regional-sites>

[23] Understanding Core Web Vitals and Google Search Results. Official documentation; accessed 17 October 2026. Tier 1: official technical guidance for Google Search. <https://developers.google.com/search/docs/appearance/core-web-vitals>

This is an attributed technical position paper, not an independent scientific certification or security guarantee. Reference endpoints and Not Activated services are not represented as live marketplace integrations. Public availability permits crawling but does not guarantee search indexing, ranking or inclusion in scholarly databases.