SADAR Federation Establishment and Policy

SADAR Federation Establishment and Policy

Federation Establishment and Policy

SADAR Documentation — Federation

Draft — May 2026

Purpose

This document is the orientation page for SADAR federation establishment: how registries discover federation candidates through the Directory of Authorized Registries, evaluate compatibility through manifest matching, enter into bilateral federation agreements, and administer per-registry policy through the registry admin console. It covers the three-layer enforcement model — federation membership, per-entry ACLs, and IAM-based requester-specific blocking — and the architectural principles that make the model consistent across the SADAR ecosystem.

Federation in SADAR is bilateral, non-transitive, admin-driven, and authorization-validated. Each property is intentional and contributes to the federation's trust properties. This document specifies how each is operationalized, including the directional asymmetry that distinguishes authorized registries (which may serve as home registries for federated content) from non-authorized registries (which may consume from authorized registries but cannot host federated content).

The normative basis lives across multiple sources. Scope §5.1.11 establishes the federation model and Directory semantics. Scope §5.1.12 establishes Registry Isolation, which holds in federated topologies as it does for standalone registries. The replication mechanics that flow over established federations are covered in Replication and Manifest Provenance. The conformance / certification / authorization ladder that determines federation eligibility is covered in Governance and Conformance.

Audience: registry operators establishing or evaluating federation relationships; registry admins configuring federation membership and per-entry policy; enterprise architects reasoning about cross-organizational discovery patterns. The document is descriptive, with normative requirements summarized at the end and open items enumerated thereafter.

What Federation Covers

Federation in SADAR is the operational mechanism by which registries enter into bilateral relationships that permit cross-registry discovery and content replication. Federation has four layered concerns:

- **Discovery of candidates.** Registries find potential federation partners by consulting the Directory of Authorized Registries (the canonical RoR maintained by OpenSemantics.org). The Directory lists authorized registries — those certified and authorized by the Authorizing Body — and provides the institutional-trust signal admins rely on when evaluating candidates as home registries for content flowing into public federation.
- **Compatibility evaluation.** Registries evaluate one another's manifests for compatibility — cryptographic verification, institutional authorization, and NFR matching. Federation matching is dominated by NFR fit; semantic bindings serve as human-search aids rather than automated match dimensions.
- **Bilateral agreement.** Federation requires both parties to sign and exchange federation assertions through the standard SADAR push channel. Each registry signs in its own name; the agreement is bilateral, not multilateral.
- **Policy administration.** Once federated, registry admins govern federation membership at three layers: federation membership decisions, per-entry inbound and outbound ACLs, and requester-specific IAM enforcement. Different layers, different decision authorities, different granularities.

This page covers federation establishment and policy at orientation depth. The cryptographic mechanics of replication that flow over established federations live in Replication and Manifest Provenance. The institutional regime that produces certified, authorized candidates in the first place lives in Governance and Conformance.

Architectural Principles

Federation Is Bilateral

Each federation relationship is between exactly two registries. There is no concept of a multilateral federation in which three or more registries automatically extend mutual recognition. Two registries that wish to federate negotiate the relationship between themselves; if a third registry is to be involved, two additional bilateral relationships must be separately negotiated.

Bilaterality matches real-world organizational trust. Commercial relationships, partnership agreements, and inter-organizational data-sharing arrangements are typically bilateral; organizations that wish to extend recognition to multiple counterparties do so through multiple bilateral agreements rather than through a single multilateral arrangement that implicitly trusts unspecified third parties. SADAR's federation model adopts the same shape.

Federation Is Non-Transitive

If Registry A federates with Registry B, and Registry B federates with Registry C, this does not extend any rights from Registry A to Registry C. Registry A and Registry C have no federation relationship. Registries can only expose or forward entries for which they are the home, plus entries replicated from a registry with which they have a current direct federation agreement. There is no concept of cross-federation chaining; what an admin configures is exactly what their registry can reach.

Non-transitivity has several rationales. Trust does not compose. Operational control is preserved — the home registry chose specific peers based on specific evaluation. Blast radius is contained — a compromised peer cannot extend the impact of its compromise to additional registries by passing replicated content through to them. And the semantic model is preserved — one home registry per manifest, one bilateral agreement per replication link, no implicit trust extensions.

Federation Is Admin-Driven

Federation establishment is an administrative act between organizations, mediated by registry admins through their administrative consoles. It is not a runtime discovery decision. Admins identify potential federation partners (typically through the Directory, sometimes by reference to a known partner organization), evaluate their compatibility, and configure the federation in their admin console.

This is in contrast to runtime discovery of agents, tools, and resources within a federation, which is automated and bilateral-matching-driven. Federation discovery is human-initiated; runtime invocation discovery is machine-initiated within the federation. The two operate at different paces and with different decision processes.

Federation Is Authorization-Validated

Participation in public federation as a provider — that is, serving as a home registry for content that flows to public-federation peers — requires authorization by the Authorizing Body. Authorization is contingent on certification, which in turn requires functional conformance. Admins configuring federation rely on the institutional-trust path established by this ladder: a registry listed in the Directory has been certified as conformant and authorized for federation participation.

A non-authorized registry (one not listed in the Directory) MAY still establish bilateral federation with an authorized registry as a consumer: the non-authorized registry replicates content from the authorized registry and acts as a downstream consumer of public-federation content. The non-authorized registry MUST NOT serve as a home registry for content discoverable to public-

federation peers; the consumer-side institutional-trust check enforces this structurally by verifying that the home registry of replicated content is currently authorized.

Federation Eligibility by Operational Mode

The three operational modes defined in Governance and Conformance — Internal-only, Authorized non-federated, and Authorized federated — differ in their conformance, certification, and authorization status, which in turn determines what role each can play in federation. The directional asymmetry is the key property: consumer-side participation is broadly available; provider-side participation is gated by authorization.

Operational mode	May consume from authorized registries	May serve as home registry for federated content	Listable in Directory
Internal-only (private)	Yes — subject to the authorized registry's federation policy. The non-authorized registry replicates content downstream.	No. The institutional-trust check at consumer verification fails for non-authorized home registries.	No
Authorized non-federated	Yes — same as Internal-only. Certification provides verifiable conformance claim but the operator has not sought (or has been denied) authorization.	No. Same enforcement as Internal-only.	No
Authorized federated	Yes — standard bilateral federation with other authorized registries.	Yes. Listed in the Directory; institutional-trust check at consumers passes.	Yes

Authorized registries that wish to federate with non-authorized peers do so under their own federation policy. The decision is the authorized registry's: whether to permit a non-authorized peer to replicate content depends on the authorized registry's evaluation of the non-authorized peer (NFR compatibility, organizational due diligence, contractual considerations). The authorization regime does not preclude such federation; it gates only the provider role for public-federation content.

Cross-mode federation produces a clean directed-graph property: content flows from authorized to non-authorized; non-authorized registries cannot inject content back into the public federation. The asymmetry preserves the institutional-trust path while allowing private deployments to participate as consumers without taking on the certification and authorization burden.

Directory and RoR Architecture

The Directory of Authorized Registries

The Directory of Authorized Registries is the canonical Registry of Registries for the SADAR public federation. It is operated by OpenSemantics.org under the same isolation properties any RoR exhibits. A registry listed in the Directory is an authorized peer for cross-registry discovery, query forwarding, and content replication; a registry not listed is not authorized for the public-federation provider role.

The Directory's editorial layer — the certification process, listing criteria, and lifecycle administration — is governed by the OpenSemantics.org Charter (covered in Governance and Conformance). The protocol layer — how registry descriptors are signed, served, queried, and revoked — is the same SADAR registry protocol as any other registry, applied to descriptor-shaped content. There is no privileged inter-RoR or RoR-protocol exception; an RoR is a SADAR registry holding registry descriptors.

Directory Replication and High Availability

The Directory replicates across multiple operational instances for high availability. Registries configure primary, secondary, and tertiary RoRs in their replication topology much as DNS clients configure name servers; lookups can be directed to any of them and return the same authoritative content (modulo replication latency). The replicated instances are equivalent in authority — none is privileged over the others; all serve the same authoritative content; all receive updates from the Authorizing Body through the same propagation mechanism.

Inter-RoR replication uses the standard SADAR registry federation contract — the same mechanism by which any two registries federate. RoR-to-RoR push, signed propagation messages, deprecation/renewal lifecycle, and registry-isolation properties all apply. The recursive architectural pattern holds at this layer as it does at the registry layer.

Registry Descriptors

Every entry in the Directory (or any RoR) is a registry descriptor — a publisher-signed manifest that describes a registry and the terms under which other parties may discover and federate with it. Descriptors carry the same top-level structure as any other SADAR manifest plus registry-specific declarations:

Field	Purpose
manifest URN	Globally unique identifier for this descriptor version.
endpoint URN	The registry's discovery endpoint — the URL counterparties query directly.

Field	Purpose
owning_entity	The legally accountable root entity for the registry, attributed within the SADAR entity hierarchy.
supported NFRs	The non-functional requirement categories this registry supports — authentication baseline, jurisdiction, declared scopes, terms of service.
semantic bindings (optional)	Sectoral or domain coverage declarations (e.g., healthcare, financial services, manufacturing logistics). Used for human searching during candidate evaluation; not used for automated compatibility matching.
TTL	Validity period; controls how long counterparties may cache the descriptor before refreshing.
lifecycle state	active, deprecated, or revoked. Drives counterparty behavior under the federation rejection rules.
signature	JSON Web Signature over the descriptor content using the registry's signing key.

Descriptors are immutable. Any change — a new endpoint, an additional supported NFR, a TTL adjustment — produces a new versioned descriptor with a new signature. The RoR rejects in-place modification attempts; the lifecycle of a descriptor proceeds through versioned state changes only.

Federation Establishment

Discovery of Federation Candidates

A registry admin seeking to establish federation typically begins by identifying a candidate. Two scenarios are common:

- **Known partner.** The admin already knows the candidate by organizational name (a commercial partner, a customer, a regulatory peer). The admin uses the Directory to retrieve the candidate's registry descriptor and verify that the candidate is currently authorized.
- **Catalog browse.** The admin browses the Directory for registries matching specific criteria. The admin can browse for entries by NFR category and by optional semantic-binding filters, but the more likely scenario is connecting to a known registry such as a commercial partner organization.

In both cases, the Directory is the source of truth for which registries are authorized. A registry not listed in the Directory is not authorized for public federation as a provider. Admins evaluating candidates as potential home registries rely on Directory listing as the institutional-trust signal.

Manifest Retrieval and Evaluation

Once a candidate is identified, the admin retrieves the candidate's descriptor and evaluates compatibility. Evaluation has three components, each of which must succeed:

- **Cryptographic verification.** The admin (or admin tooling) verifies the candidate's descriptor signature against the candidate's verification key, anchored according to the candidate's declared trust anchor. If cryptographic verification fails, the candidate is rejected.
- **Institutional verification.** The admin confirms that the candidate is currently authorized in the Directory — that is, currently certified, not deauthorized, and listed as active. If the candidate is not authorized (either not listed, listed as deprecated/revoked, or where authorization is required and not granted), the candidate is rejected for the home-registry role. Federation as a non-authorized consumer remains possible if the federating registry chooses to permit it.
- **Compatibility matching.** The admin evaluates whether the candidate's declared NFRs are compatible with the admin's own registry's requirements. This is the federation-specific matching step, dominated by NFR fit.

Federation Compatibility Matching

Federation matching is simpler than other matching in SADAR because registries are functionally similar to one another — they all serve manifests, mediate discovery, support replication, expose push endpoints. Matching is dominated by NFR fit. Other manifest fields play supporting roles:

- **Owning entity.** Identifies the organization operating the registry, supporting the human-driven evaluation step (“is this Salesforce, the actual Salesforce, certified and authorized to operate this registry?”).
- **Semantic bindings.** Optional declarations of sectoral or domain coverage. Used for human searching and admin-side filtering, not for automated compatibility matching. A registry MAY declare semantic bindings or remain silent on this attribute.
- **Trust anchor.** The verification key's trust anchor must be acceptable to the matching admin's policy.

The detailed NFR matching semantics that this evaluation uses are specified in the canonical NFR Schema (8. NFR Schema), which defines the four NFR categories — Financial, Operational, Governance, Protocol — and the type-specific matching rules for each. Federation matching applies the same NFR vocabulary and the same matching algorithm as runtime entry-level matching, with the candidate set being registries rather than agents and the matching dimensions being registry-level rather than agent-level.

Bilateral Agreement

Federation requires bilateral agreement. The admin's evaluation of the candidate is one half; the candidate's admin must independently evaluate this admin's registry and agree to federate. The protocol-level act of federation establishment is the exchange of mutually-signed federation agreement assertions — each registry signs an assertion in its own name acknowledging the federation with the other party, and the assertions are exchanged through the standard SADAR push channel.

The federation assertion is a structured artifact containing the signing registry's identity, the counterparty's identity, the scope of the federation, the TTL of the agreement (subject to the universal lifecycle), and the push endpoints to which lifecycle messages are delivered. Once both registries have signed and exchanged their assertions, the federation is established. Replication, mutual discovery, and cross-federation operations may proceed within the scope of the agreement.

The federation assertion captures the directional roles: which party is the home registry for content flowing in each direction, what content categories participate, and what NFR-derived constraints apply. For federation between two authorized registries, both directions are typically symmetric — each may be a home registry for content flowing to the other. For federation between an authorized registry and a non-authorized registry, the assertion captures the asymmetry: the authorized registry is the home for content flowing to the non-authorized peer; the non-authorized peer cannot be the home for content flowing back to the authorized registry as public-federation content.

Federation Lifecycle

Federation agreements are subject to the universal lifecycle. Each federation assertion has a TTL; expiry triggers re-evaluation by both parties; renewal is substantive re-authorization — not automatic re-signing. At renewal, each party re-confirms the institutional trust signal (the counterparty is still authorized in the Directory if expected to serve as a home registry), the cryptographic verification (the counterparty's descriptor signature still verifies), and the compatibility matching (NFRs still align).

Termination of a federation agreement may occur at TTL expiry without renewal, by mutual termination through signed messages, or by deauthorization of either party by the Authorizing Body. In all cases, termination propagates through the push channel: the terminating party (or the Authorizing Body) signs a termination message; the receiving party updates its federation configuration; the federation ceases to be active. Existing replicated content is no longer renewed under the agreement; ongoing usage of cached content within current TTLs is permitted but not extended.

Registry-Admin Policy Layer

Federation policy in SADAR lives at the registry admin layer, not at the service layer. The admin is the right party to decide which registries the registry's content can flow through, and decisions made at the admin level apply uniformly across all entries hosted at the registry without requiring each service to maintain federation awareness.

Federation Membership Configuration

The registry admin establishes federation with specific home registries (drawn from candidates listed in the Directory for authorized peers, or by direct arrangement for non-authorized peers acting as consumers) and configures the federation scope: which categories of content participate, what NFR constraints apply, and what lifecycle terms govern the agreement. Federation membership is the high-level decision: which registries are this registry's federation partners?

Inbound and Outbound ACLs Per Federation

Registries MAY (and SHOULD, where the deployment requires fine-grained control) implement ACLs determining inbound and outbound rules per federated registry. The ACL surface includes:

- **Per-entry rules.** Specific entries (an agent, a tool, a business function, a business process) may be exposed through some federations and not others, and may be permitted to discover entries from some federations and not others. Per-entry ACLs scope federation membership at finer granularity than registry-level membership.
- **Per-entity rules.** All entries owned by a specific entity may be subject to a unified ACL that applies regardless of entry type — useful when an organization wants federation-level decisions made at the legal-entity level rather than per artifact.
- **Per-manifest-criteria rules.** Rules that match against manifest content (NFR categories, declared sectors, classification levels) and apply uniformly to entries that meet the criteria — a structured-policy approach that scales beyond per-entry administration.

ACL configuration supports several common policy patterns: default-allow (all hosted entries participate in all configured federations unless explicitly excluded), default-deny (no entries participate unless explicitly included), per-federation tiers (high-trust federations receive broader entry exposure than low-trust federations), and per-entry classifications (entries classified as sensitive participate only in federations meeting elevated NFR requirements). The specific ACL model an admin uses is operator-controlled within the structural mechanism.

Block Lists for Specific Home Registries

In the event of a block on a particular home registry, the admin can configure the block for new discoveries. Block lists support several use cases: operational issues with a specific peer; voluntary exclusion for business or policy reasons; pre-deauthorization isolation pending Authorizing Body investigation. Block lists apply to new discoveries; existing relationships continue under their current TTL but are not renewed. Renewal triggers re-resolution that surfaces the block.

Requester-Specific Blocking via IAM

For a block of a specific requester, the IAM layer (rather than the federation layer) handles the enforcement. The IAM authentication and authorization call returns failure for blocked requesters; the registry does not need to know that a specific requester is blocked, because IAM enforcement happens before the request reaches the registry's serving layer.

This separation matters because federation policy and authentication policy operate at different scopes. Federation policy decides which registries can interact with which other registries (and which entries within them). IAM policy decides which specific principals can authenticate (and what they can do once authenticated). Combining the two would conflate federation membership with principal-level permissions; separating them lets each layer's policy be evaluated and managed by the appropriate party at the appropriate granularity.

Three-Layer Enforcement Architecture

The three policy layers operate at different granularities and address different concerns. Together they form the federation enforcement architecture:

Layer	Decides	Enforced at
Federation membership	Which home registries flow content into and out of this registry; the bilateral agreements in force.	Registry admin console; bilateral federation assertions exchanged through push.
Per-entity / per-entry / per-criteria ACLs	Which entries participate in which federations, in either direction (inbound and outbound).	Registry serving layer; admin-configured ACLs evaluated at discovery and replication time.
Requester-specific authentication	Which specific principals can authenticate to specific endpoints.	IAM at the authentication call; failure returned before the request reaches the registry.

Structural decisions live at the admin level (federation membership and ACLs); principal-level decisions live at the IAM level. Services do not need to maintain federation awareness; agents

do not need to make federation decisions. The decision authority aligns with organizational accountability at each layer.

Properties of the Federation Model

Several architectural properties follow from the structure described above.

Property	What it means
Structural containment	Bilateral, non-transitive federation contains the structural impact of any single federation decision. A decision to federate with one peer extends to that peer only; a decision to deauthorize a peer terminates that one relationship; a decision to add a new peer creates exactly one new relationship.
Distributed enforcement	Federation policy enforcement is distributed across multiple layers (federation membership, ACLs, IAM) and across multiple parties (registry admins, the Authorizing Body, IAM operators). No single point of enforcement; no single point of failure.
Admin-centric decision-making	Federation decisions live at the admin layer where organizational judgment can be applied. Services do not need to maintain federation awareness; the registry admin makes the decisions once at the federation level, and they apply uniformly across the registry's hosted entries.
Lifecycle discipline	Federation agreements are subject to the universal lifecycle. Federation does not become a once-established, perpetual relationship; it is a continuously-renewed agreement that re-confirms institutional and cryptographic trust at each renewal.
Directional asymmetry by authorization	Authorization gates the home-registry role for public-federation content. Authorized registries may serve as homes for content flowing to peers; non-authorized registries may consume from authorized registries but cannot be homes for public-federation content. The directed-graph property is automatic, enforced by the consumer-side institutional-trust check.
No cross-federation concept	Because federation is bilateral and non-transitive, there is no cross-federation discovery or content flow. The Directory contains all authorized registries; an admin configures registries to be federated with the registry they manage; the registry talks to those configured registries only. Registries can only expose or forward entries for which they are the home, plus entries directly replicated under bilateral federation.

Boundaries — What's Not Here

This page covers federation establishment and the registry-admin policy layer at orientation depth. Several adjacent topics live in dedicated documents:

Topic	Where it lives
Replication mechanics	How manifests retain verifiable provenance when replicated across federated registries, including the home-registry binding and the verification chain. See Replication and Manifest Provenance.
Governance and the conformance ladder	The Steward, the Authorizing Body, the conformance / certification / authorization three-step ladder, the institutional-trust path, and the universal lifecycle. See Governance and Conformance.
Registry architecture	The registry itself — what it does, what it doesn't do, the six registry types, and the three operational modes. See Registry Overview.
RoR architecture	The federation-layer component that resolves cross-registry discovery, the canonical Directory of Authorized Registries, and registry descriptors. See Registry of Registries.
NFR matching semantics	How NFR matching evaluates each NFR within each category. Federation matching uses the same NFR vocabulary and matching algorithm as entry-level matching. See 8. NFR Schema.
Bilateral matching algorithm	The two-direction structure of the matching algorithm and the three-tier strictness model. See Matching Algorithm.
Discovery flow at the entry level	How the matching algorithm and resolver compose for runtime entry discovery within a federation. See Discovery and Discovery Patterns.

Normative Requirements Summary

The following requirements use the terminology of **RFC 2119** / RFC 8174 as it will appear in the normative specification revision.

Federation Bilaterality and Non-Transitivity

1. **R-FED-1.** Federation MUST be bilateral; each federation relationship is between exactly two registries.
2. **R-FED-2.** Federation MUST be non-transitive; no rights extend from one federation relationship to any other.
3. **R-FED-3.** A registry MUST NOT serve content whose home-registry binding is signed by a registry with which the serving registry has no current direct federation agreement.
4. **R-FED-4.** A registry MUST NOT re-replicate content received through one federation to peers in a different federation.
5. **R-FED-5.** A registry can only expose or forward entries for which it is the home registry, plus entries replicated from a registry with which it has a current direct federation agreement.

Federation Eligibility

6. **R-ELIG-1.** Only authorized registries (those listed in the Directory of Authorized Registries) MAY serve as home registries for content flowing into public federation.
7. **R-ELIG-2.** A non-authorized registry MAY consume content from an authorized registry through bilateral federation, subject to the authorized registry's federation policy.
8. **R-ELIG-3.** A non-authorized registry MUST NOT serve as the home registry for content discoverable to public-federation peers. The consumer-side institutional-trust check enforces this structurally.
9. **R-ELIG-4.** Authorized registries MAY federate with non-authorized peers as a matter of the authorized registry's own federation policy. The directional asymmetry of the resulting federation MUST be reflected in the federation assertion.

Federation Establishment

10. **R-EST-1.** Federation establishment MUST be admin-driven; runtime automatic establishment of new federations between previously-unrelated registries is not permitted.
11. **R-EST-2.** Federation candidates that will serve as home registries for public federation MUST be discoverable through the Directory of Authorized Registries; participation as a public-federation provider requires Authorizing Body authorization.
12. **R-EST-3.** Each party to a federation MUST sign a federation assertion in its own name, exchanged through the push channel.
13. **R-EST-4.** Federation assertions MUST carry a TTL and are subject to the universal lifecycle.
14. **R-EST-5.** Federation assertions MUST capture the directional roles of each party (which is a home registry for content flowing in each direction).

Directory and RoR Operation

15. **R-ROR-1.** RoRs MUST themselves be registered entries with manifests, owning entities, and verification keys anchored in declared trust anchors.
16. **R-ROR-2.** RoRs MUST be authorized by the Authorizing Body to operate as RoRs.
17. **R-ROR-3.** RoRs MUST replicate authoritative content through the push and replication mechanisms specified in Replication and Manifest Provenance.
18. **R-ROR-4.** Replicated instances of the Directory MUST be operationally equivalent within a public federation; no instance is privileged over others.
19. **R-ROR-5.** Registries MAY configure multiple RoRs (primary, secondary, tertiary) and MUST treat them as functionally equivalent.

Federation Compatibility Matching

20. **R-MATCH-1.** Federation matching MUST be based on declared NFRs; semantic bindings MAY support human searching but MUST NOT be used as automated compatibility-match dimensions.
21. **R-MATCH-2.** Matching MUST verify the candidate's cryptographic authenticity, institutional authorization (Directory listing for home-registry candidates), NFR compatibility, and trust-anchor compatibility.
22. **R-MATCH-3.** Matching MUST be re-evaluated at federation renewal; pass at establishment does not imply pass in perpetuity.

Registry-Admin Policy Layer

23. **R-POL-1.** Federation membership decisions MUST be made at the registry admin layer, not at the service layer.
24. **R-POL-2.** Registries MAY — and where the deployment requires fine-grained control, SHOULD — implement ACLs determining inbound and outbound rules per federated registry, including per-entry rules, per-entity rules, and per-manifest-criteria rules.
25. **R-POL-3.** Block lists for specific home registries SHALL be supported as a configuration mechanism. Block lists MUST apply only to new discoveries; existing relationships continue under their current TTL until renewal.
26. **R-POL-4.** Requester-specific blocking MUST be handled at the IAM layer, not the federation layer.

Open Items

The following items require resolution in subsequent specification work.

Federation Assertion Schema

This document specifies the structural elements of federation assertions but not the precise schema. The schema (field names, types, encoding format, signature scope, directional-role representation) requires specification in subsequent work, likely as part of the RoR companion specification or an appendix to this document.

NFR Vocabulary for Registry-Level Matching

The NFR vocabulary used for registry-level federation matching draws on the canonical NFR Schema (8. NFR Schema). Subsequent specification work may identify registry-specific NFRs that warrant first-class treatment in the schema, or may produce a recommended profile of NFRs for registry-level matching, recognizing that sector-specific extensions will inevitably be required.

Where to Learn More

Governance and Conformance — the Steward, the Authorizing Body, the conformance / certification / authorization ladder that produces authorized registries, and the institutional-trust path.

Replication and Manifest Provenance — the cryptographic mechanics of replication, the home-registry binding, and the push channel that federation assertions and lifecycle messages flow through.

Registry Overview — the architectural framing for registries, the six registry types, and the three operational modes.

Registry of Registries — the federation-layer component that resolves cross-registry discovery, including the canonical Directory of Authorized Registries.

Registry Concepts — the glossary of registry-side terms, including the manifest URN, descriptor, owning_entity, lifecycle state, and entity hierarchy concepts referenced throughout.

Discovery — multi-level matching, TTL semantics, the resolver, and match classification at the entry level within a federation.

Matching Algorithm — the bilateral two-direction structure and three-tier strictness model that federation matching applies at the registry level.

8. NFR Schema — the canonical source for the four NFR categories, the bilateral match algorithm, and registry-side validation requirements that federation matching depends on.

2. Scope §5.1.11 — Registry Topology, Federation, and Directory.

2. Scope §5.1.12 — Registry Isolation: the normative constraints establishing the registry as a discovery-time component only, including in federated topologies.