Network Working Group
Internet-Draft
Intended status: Informational
Expires: 10 October 2026

B. Morrison
Alter Meridian Pty Ltd

April 2026

Discovery of Model Context Protocol Servers via DNS TXT Records
draft-morrison-mcp-dns-discovery-02

Abstract

This document defines a DNS-based mechanism for the discovery of Model Context Protocol (MCP) servers and the identity properties of the organisations that operate them. Two TXT resource records are defined. The _mcp.<domain> record (defined in v01 of this document) advertises the presence, endpoint URL, transport protocol, cryptographic identity, and capability profile of an MCP server associated with a domain name. The _org-alter.<domain> record (introduced in this revision) advertises the canonical organisational identity of the domain operator: legal entity name, registry identifier, founding date, primary regions of operation, and any regulatory frameworks under which the operator is bound to refuse external automated access. Together, the two records provide both service discovery and identity bootstrap from a single canonical source -- the domain’s own DNS zone. The mechanism complements HTTPS-based discovery (.well-known/mcp/server-card.json) by providing a lightweight, resolver-cached bootstrap that requires no HTTPS round-trip. The design follows the precedent established by DKIM [RFC6376], SPF [RFC7208], DMARC [RFC7489], and MTA-STS [RFC8461], all of which use DNS TXT records at underscore-prefixed labels to advertise domain-scoped policy and service metadata.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 3 October 2026.

Table of Contents

1. Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on October 7, 2026.

2. Copyright Notice

3. Introduction

Model Context Protocol (MCP) [MCP] is an open protocol for structured interaction between AI agents and tool-providing servers. A complete agent-to-organisation interaction has two distinct discovery requirements:

1. *Service discovery.* Where is the MCP server endpoint? What transport does it speak? What cryptographic key authenticates it? This is the question v01 of this document answers via the _mcp.<domain> record.

2. *Identity bootstrap.* Who is the organisation operating the server? What is its legal entity? Where is it registered? Under what regulatory frameworks does it operate, and which automated access pathways must it refuse to participate in? This is the question v02 introduces via the new _org-alter.<domain> record.

The two questions are distinct. An MCP client may need to discover an endpoint without caring about the operator's identity. An onboarding wizard installing an org-alter instance may need to read the operator's identity without caring (yet) about the MCP endpoint. Conflating both into a single TXT record would force every consumer to parse fields it does not need and would crowd the 255-byte character-string limit. Splitting them across two underscore-prefixed labels mirrors the pattern established by DKIM (_domainkey._domain) and DMARC (_dmarc._domain): each record serves a single semantic purpose.

This revision is fully backward-compatible with v01. Implementations that consume only the _mcp.<domain> record continue to work unchanged. Implementations that wish to bootstrap an org-alter identity may additionally query _org-alter.<domain>.

The org-identity layer is grounded in the identity field framework of [MORRISON-IFT]. An organisation's identity is not a single boolean fact but a continuous field maintained across the social-spatial manifold. A DNS record provides a discrete checkpoint into that field. The _org-alter.<domain> record is the operator's own canonical declaration of their identity at a point in time, signed by their control of the DNS zone, and consumable by any bootstrap process -- including, critically, the operator's own org-alter instance reading its own record on first install.

3.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 RFC2119 [RFC8174] when, and only when, they appear in all capitals, as shown here.

4. Terminology

(Terminology from v01 is retained. Additional terms introduced in this revision are defined below.)

Org-Identity Record A DNS TXT resource record published at the _org-alter label under a Policy Domain, conforming to the syntax defined in Section 4 of this document.

Identity Bootstrap The procedure by which an org-alter implementation reads its own Org-Identity Record on first install to populate its canonical identity state without requiring manual operator entry.

Canonical Entity Identifier A globally-unique, jurisdiction-issued identifier that names the legal entity behind the operator. Examples include the Australian Business Number (ABN), the Companies House number, the EIN, the CRO number, or the LEI.

Regulatory Refusal Marker A declaration in the Org-Identity Record that the operator is bound by a named regulatory framework (e.g. DISP, ITAR, HIPAA) and that any automated access pathway crossing into the regulated boundary MUST be refused. This is a structural promise from the operator to the world: do not attempt to integrate, even with credentials.

5. Record Format -- _mcp.<domain> (Service Discovery)

Section 3 of v01 of this document defines the _mcp.<domain> record, its ABNF grammar, field definitions (v, url, proto, pk, epoch, cap, attest, scope, priority, ttl, ext), forward-compatibility rules, and multi-string concatenation behaviour. These definitions are unchanged in this revision and are incorporated here by reference. Implementations MUST treat any existing _mcp.<domain> record as conformant to the v01 specification.

6. Record Format -- _org-alter.<domain> (Identity Bootstrap)

This section defines the new Org-Identity Record introduced in v02.

6.1. DNS Location

The Org-Identity Record is a DNS TXT resource record [RFC1035] published at the label _org-alter prepended to the Policy Domain:

_org-alter.<policy-domain>. IN TXT "<record-value>"

The underscore prefix conforms to the conventions established in [RFC8552] for globally scoped, underscore-prefixed DNS node names.

A domain MAY publish a _mcp.<domain> record without an _org-alter.<domain> record (service-only deployment), or an _org-alter.<domain> record without a _mcp.<domain> record (identity-only deployment), or both (full deployment). The recommended pattern for any operator running an org-alter instance is to publish both.

Multiple TXT resource records MAY be published at the same DNS name (e.g., for staged identity rotation). Clients MUST evaluate all returned records and select the one with the highest epoch field.

6.2. ABNF Grammar

The record value is a semicolon-delimited sequence of key-value pairs. The following ABNF [RFC5234] defines the syntax:

‘‘‘ orgalter-record = version *(";" SP field) version = "v=alter1" field = org-field / entity-field / entity-type-field / founded-field / regions-field / regulated-field / bootstrap-field / mcp-policy-field / epoch-field / pk-field / attest-field / ext-field / unknown-field

org-field = "org=" 1_VCHAR entity-field = "entity=" registry ":" 1_VCHAR entity-type-field = "entity-type=" 1_VCHAR founded-field = "founded=" date-fullyear regions-field = "regions=" region-csv regulated-field = "regulated=" framework-csv bootstrap-field = "bootstrap=" https-uri mcp-policy-field = "mcp-policy=" policy-token epoch-field = "epoch=" 1_DIGIT pk-field = "pk=" algo ":" base64url attest-field = "attest=" attest-csv ext-field = "ext=" https-uri unknown-field = token "=" *VCHAR

```
registry = "abn" / "acn" / "ein" / "ch" / "cro" / "lei" / token
region-csv = region-token _( "," region-token ) region-token = 2ALPHA
; ISO 3166-1 alpha-2 framework-csv = framework-token *( ","
framework-token ) framework-token = "disp" / "itar" / "ear" / "hipaa"
/ "gdpr" / "soc2" / "iso27001" / "iso42001" / "essential8" / "aprs" /
token policy-token = "open" / "refuse-automated" / "refuse-tenant" /
"refuse-all" / token date-fullyear = 4DIGIT [ "-" 2DIGIT [ "-" 2DIGIT
] ] algo = "ed25519" base64url = 1_( ALPHA / DIGIT / "-" / "_" )
https-uri = "https://" *VCHAR token = 1*( ALPHA / DIGIT / "-" / "_" )
'''
```

6.3. Field Definitions

6.3.1. v (REQUIRED)

Protocol version identifier. MUST be the literal string alter1. MUST appear as the first field in the record. Clients MUST reject any record whose v field is absent, is not the first field, or contains a value other than alter1.

The version namespace is independent of the _mcp record's v=mcp1 namespace. This allows the two record types to evolve independently.

6.3.2. org (REQUIRED)

The canonical legal name of the organisation operating the domain. MUST be the registered legal entity name as it appears in the operator's primary corporate registry, not a trading name or brand. For trading names, see the optional entity-type field.

Examples:

org=Alter Meridian Pty Ltd org=Red Group Pty Ltd org=International Business Machines Corporation

6.3.3. entity (RECOMMENDED)

A globally-disambiguating canonical entity identifier, prefixed by its registry namespace. Defined registries:

* abn: -- Australian Business Number (11 digits, no spaces).
* acn: -- Australian Company Number (9 digits, no spaces).
* ein: -- US Employer Identification Number (NN-NNNNNNN).
* ch: -- UK Companies House number (8 alphanumeric).

* cro: -- Irish Companies Registration Office number.

* lei: -- Legal Entity Identifier (20 alphanumeric per ISO 17442).

Additional registries MAY be defined; clients MUST treat unknown registry namespaces as opaque identifiers.

Example:

entity=abn:54696662049

The entity field is the primary anti-impersonation defence for the identity layer: a domain claiming to be Alter Meridian Pty Ltd without an ABN that resolves to that name in ABR Lookup is detectable as a mismatch by any verifier with access to the public registry.

6.3.4. entity-type (OPTIONAL)

A short human-readable label for the entity's type, drawn from its jurisdiction's vocabulary. Examples: Pty Ltd, LLC, GmbH, SAS, non-profit. This field is advisory and is intended for display to humans; it is not a structured taxonomy.

6.3.5. founded (OPTIONAL)

The date the legal entity was founded or registered, as YYYY or YYYY-MM or YYYY-MM-DD per ISO 8601. This field is advisory and is used by onboarding wizards and identity verifiers to display "Founded N years ago" or to detect implausibly young entities making strong claims.

6.3.6. regions (OPTIONAL)

A comma-separated list of ISO 3166-1 alpha-2 country codes indicating the operator's primary regions of operation. This field is advisory. It is used by onboarding wizards to set sane defaults for jurisdiction-specific behaviour (e.g., currency, locale, public registry preference).

Example:

regions=AU,NZ,SG

6.3.7. regulated (OPTIONAL but STRUCTURALLY SIGNIFICANT)

A comma-separated list of regulatory framework tokens under which the operator is bound. Defined values (extensible):

* disp -- Australian Defence Industry Security Program.

* itar -- US International Traffic in Arms Regulations.

* ear -- US Export Administration Regulations.

* hipaa -- US Health Insurance Portability and Accountability Act.

* gdpr -- EU General Data Protection Regulation.

* soc2 -- AICPA SOC 2 Type II.

* iso27001 -- ISO/IEC 27001 information security management.

* iso42001 -- ISO/IEC 42001 AI management systems.

* essential8 -- ASD Essential Eight (ML2 or higher).

* aprs -- Australian Privacy Principles / Privacy Act.

The presence of any token in this field is a structural promise: the operator declares that they are bound by the named framework and that automated access pathways crossing the regulated boundary MUST be refused. Onboarding wizards reading this field MUST refuse to attempt L5/L6 authenticated access to data stores covered by the declared framework, regardless of whether credentials are available.

This converts the DNS record into an out-of-band consent boundary: a remote agent’s tooling becomes structurally aware that integration is forbidden before it ever attempts a connection. An agent that ignores this declaration and attempts integration anyway commits a detectable, attributable violation.

Forward compatibility: unknown framework tokens MUST be treated conservatively (assume the strictest defensible refusal) rather than ignored.

6.3.8. bootstrap (OPTIONAL)

An HTTPS URL pointing to a JSON document containing additional identity bootstrap metadata: a directory of public roster members (if the org chooses to publish one), an organisational logo URL, a canonical public website URL, an attest profile beyond what fits in DNS, and any operator-defined extensions.

The bootstrap document MUST be served over HTTPS with a valid TLS certificate for the Policy Domain. The document format is operator-defined; recommended schema is published as https://truealter.com/.well-known/org-alter-bootstrap.schema.json as a non-normative reference.

6.3.9. mcp-policy (OPTIONAL)

A single token declaring how the operator's MCP endpoint relates to external automated access:

* open -- The MCP endpoint accepts queries from any agent with appropriate authentication.
* refuse-automated -- The MCP endpoint exists for human-mediated access only. Automated agents SHOULD NOT initiate sessions.
* refuse-tenant -- The MCP endpoint exists, but the operator runs one or more tenants (e.g., an M365 tenant) into which automated access is forbidden. This is the typical declaration for an org-alter instance run by an operator who has DISP-accredited or ITAR-bound systems alongside their public meta-layer.
* refuse-all -- The MCP endpoint exists for the operator's own internal use only. External agents MUST NOT attempt connection.

Default value, if absent: open.

The mcp-policy field complements the regulated field. regulated=disp; mcp-policy=refuse-tenant is the canonical declaration for a defence contractor running an org-alter at the unclassified meta-layer alongside a regulated tenant they will not allow automated agents to enter.

6.3.10. epoch (OPTIONAL)

A monotonic non-negative integer that increments on every identity rotation event (e.g., legal entity restructure, change of control, move to a new jurisdiction). Default value: 0. Semantics mirror the epoch field of the _mcp record defined in v01.

6.3.11. pk (OPTIONAL)

Ed25519 public key for endpoint verification, encoded identically to the v01 _mcp record's pk field. When present, the same key provides cryptographic binding for both endpoint discovery and identity bootstrap.

6.3.12. attest (OPTIONAL)

A comma-separated list of attestation types the operator declares it is authorised to issue, identical in semantics to the v01 _mcp record attest field. Where both records publish an attest field, the values MUST be consistent. An onboarding wizard SHOULD use the union of the two.

6.3.13. ext (OPTIONAL)

An HTTPS URL pointing to a protocol-extension document, identical in semantics to the v01 _mcp record ext field. This field is distinct from bootstrap: ext is for protocol-level extensions to the discovery format itself; bootstrap is for operator-level identity metadata.

6.4. Forward Compatibility

Implementations MUST ignore unknown fields. This rule, identical to the v01 _mcp record specification, ensures that future extensions to the _org-alter record format do not break existing implementations.

7. Identity Bootstrap Procedure

This section defines the procedure by which an org-alter implementation reads its own DNS records on first install to populate its canonical identity state.

7.1. Inputs

The procedure takes a single input: the operator’s primary domain name (the Policy Domain under which the operator publishes records).

7.2. Algorithm

1. *Query _org-alter.<domain> TXT.* Issue a DNS query for the Org-Identity Record.

2. *If found, parse and load.* Extract org, entity, entity-type, founded, regions, regulated, mcp-policy into the org-alter’s identity state. These become the canonical identity declaration the org-alter will use in all subsequent self-reports, brief generation, and external attestation.

3. *If bootstrap= is present, fetch the bootstrap document* over HTTPS. Validate the document’s TLS certificate against the Policy Domain. Merge the document’s roster, logo, and extension fields into the identity state. Reject the bootstrap document if its TLS certificate is invalid or if its content does not parse.

4. *Honour regulated= and mcp-policy=* as immutable structural constraints on the org-alter instance:

   a. If regulated includes any framework token, set the org-alter's boundary_policy to refuse and disable all L5/L6 ingester layers.

   b. If mcp-policy=refuse-tenant, the org-alter MUST refuse to install any ingester that requires authenticated access to a tenant covered by the declared framework, even if credentials are subsequently provided.

   c. The wizard SHOULD display these constraints to the operator for confirmation but MUST NOT allow the operator to override them silently. An operator who wishes to relax a constraint MUST update the DNS record first, then re-run bootstrap.

5. *Cross-check _mcp.<domain>.* Query the v01 service-discovery record. If both records exist and both publish pk fields, the values MUST match. A mismatch indicates either a configuration error or a key compromise; the wizard MUST refuse to bootstrap under such conditions and MUST surface the discrepancy to the operator.

6. *Verify against public registries.* If the entity field declares a known registry namespace (e.g., abn:), the wizard SHOULD query the corresponding free public registry (e.g., the ABR Lookup MatchingNames API) and verify that the declared entity identifier resolves to the declared org name. A mismatch is not necessarily fatal -- names change, registries lag -- but the wizard MUST surface the discrepancy and require operator confirmation before proceeding.

7. *Persist canonical state.* Write the resolved identity into the org-alter's state/identity.json, source-citing each field to its DNS or HTTPS origin.

The bootstrap procedure is designed to make first-run org-alter installation a single command:

```
mcp-org-alter onboard --domain redgroup.com.au
```

with the wizard reading every other field from DNS and the public record before asking the operator a single question.

7.3. First-Run Cold Start

For an operator who has not yet published a _org-alter record at the time of installation, the wizard MUST fall back to interactive seeding: prompt for org, optionally prompt for entity, and ask whether the operator's environment is regulated. After interactive seeding, the wizard SHOULD generate a draft DNS record value for the operator to publish, completing the bootstrap loop.

8. Discovery Procedure -- _mcp.<domain>

The discovery procedure defined in Section 4 of v01 is unchanged in this revision. Clients querying _mcp.<domain> follow the v01 algorithm exactly.

9. Caching

Caching of _mcp.<domain> records follows v01.

_org-alter.<domain> records SHOULD be cached for the duration of the DNS TTL. Onboarding wizards typically read the record once at install time and persist the resolved state to local storage; the DNS record need not be re-read on every subsequent invocation. Wizards MAY re-read the record on operator request, on epoch change detection (via periodic background poll), or on identity verification failure.

10. Security Considerations

(Security considerations from v01 are retained. Additional considerations introduced by the org-identity layer are below.)

10.1. Identity Impersonation

A domain operator can publish any org and entity value they wish. Verification of the declared identity against a public registry (Section 6 step 6) is the structural defence against impersonation: a domain that claims to be Red Group Pty Ltd with entity=abn:00000000000 (a non-existent ABN) will be detected as fraudulent the first time any verifier cross-checks the registry.

Operators with a legitimate identity SHOULD publish their canonical entity field to opt into this verification path. Operators without a legitimate identity (or who publish a wrong one) become detectably non-conformant.

10.2. Regulatory Refusal as a Detectable Promise

The regulated and mcp-policy fields are not enforcement mechanisms in themselves -- they are structural promises by the operator to the world. An attacker who controls a domain's DNS can publish a regulated field they have no intention of honouring, or omit it when they should publish it. These misrepresentations are detectable in two directions:

* An operator who publishes regulated=disp and then permits automated access to a DISP-accredited tenant is in violation of their own published declaration, which is a public, archivable, attributable record. This creates a stronger compliance artefact than any internal policy document.

* An operator who omits regulated=disp despite being a DISP member creates a discoverable inconsistency: their public Defence Industry Portal listing is one source, their DNS record is another, and any verifier can detect the discrepancy.

The structural value of these fields is therefore in the combination of public commitment and public verifiability, not in DNS-layer enforcement.

10.3. Entity Identifier Privacy

Publishing a registry-issued entity identifier (ABN, EIN, Companies House number) makes the operator's legal entity discoverable. In most jurisdictions, this information is already public via the respective registries. The DNS record reduces the friction of discovery from "search a registry" to "dig a TXT record", but does not disclose anything that was not already obtainable.

Operators with legitimate privacy concerns about linking their domain to their legal entity SHOULD NOT publish the entity field. A wizard reading an _org-alter record without an entity field MUST treat the org name as a self-declaration without registry verification, and MUST display this absence to the operator during bootstrap.

10.4. Bootstrap Document Risks

The HTTPS bootstrap document (bootstrap= field) extends the identity surface beyond the DNS record's 255-byte limit. The document is fetched over HTTPS with TLS validation, but its content is operator-controlled. Wizards parsing the bootstrap document MUST apply the same forward-compatibility rules (ignore unknown fields) and MUST treat the document as untrusted input until cross-validated against DNS and registry sources.

Wizards SHOULD NOT execute any code from a bootstrap document and MUST NOT load JavaScript or any active content. The document is a structured data file, not a runtime payload.

11. Privacy Considerations

(Privacy considerations from v01 are retained. Additional considerations introduced by the org-identity layer are below.)

11.1. Organisational Privacy vs Individual Privacy

The _org-alter record is a domain-level declaration about an organisation, not an individual. No per-user information appears in the record. The fields describe the legal entity, its registry identifier, its founding date, its operational regions, and its regulatory framework -- all of which are properties of the organisation.

Individual identity, where the org-alter chooses to expose it, is mediated by the MCP server behind the endpoint, subject to application-level consent and access control mechanisms outside the scope of this document.

11.2. DNS Query Metadata

A client resolving _org-alter.example.com reveals to its resolver that it intends to bootstrap an org-alter identity for example.com. The privacy considerations of v01 (DoH/DoT preference) apply identically.

12. IANA Considerations

12.1. Underscored DNS Node Name Registration

This document requests IANA to register the following entries in the "Underscored and Globally Scoped DNS Node Names" registry established by [RFC8552]:

RR Type	_NODE NAME	Reference
TXT	_mcp	[this document], v01 Sec.3
TXT	_org-alter	[this document], v02 Sec.4

The _org-alter label is used to publish Org-Identity Records as defined in Section 4 of this document.

12.2. Org-Alter Version Registry

This document defines the version tag v=alter1 for the _org-alter record. Future versions (e.g., v=alter2) SHOULD be coordinated with the org-alter implementation community. Until a formal IETF working group is chartered for org-identity discovery, this document recommends that the version registry be maintained by the authors and that all extensions be documented in successor revisions of this draft.

12.3. Registry Namespace Registry

This document defines an initial set of entity field registry namespaces (abn, acn, ein, ch, cro, lei). Future registries MAY be added by successor documents. Implementations MUST treat unknown registry namespaces as opaque identifiers and MUST NOT reject records solely on the basis of an unknown namespace.

12.4. Framework Token Registry

This document defines an initial set of regulated framework tokens (disp, itar, ear, hipaa, gdpr, soc2, iso27001, iso42001, essential8, aprs). Future tokens MAY be added by successor documents. Implementations MUST treat unknown tokens conservatively (assume strictest defensible refusal) rather than ignoring them.

13. Examples

This section provides non-normative examples of Org-Identity Records for common deployment scenarios.

13.1. Minimal Record (Public Operator)

The simplest valid Org-Identity Record contains only the version, canonical org name, and entity identifier:

```
_org-alter.alter.com.au.  IN TXT "v=alter1; org=Alter Meridian Pty
Ltd; entity=abn:54696662049"
```

A wizard reading this record knows the legal entity behind the domain, can verify the ABN against ABR Lookup, and treats the operator as unregulated (no regulated field present).

13.2. Full Public Record

A complete record including founding date, regions, and key:

```
_org-alter.alter.com.au.  IN TXT ( "v=alter1; " "org=Alter Meridian
Pty Ltd; " "entity=abn:54696662049; " "entity-type=Pty Ltd; "
"founded=2026-03-29; " "regions=AU,NZ; " "epoch=1; "
"pk=ed25519:dGhpcyBpcyBhIHNhbXBsZSBrZXk; "
"attest=employ,contract,member; "
"bootstrap=https://alter.com.au/.well-known/org-alter-bootstrap.json"
)
```

This is the canonical declaration for ALTER itself.

13.3. Regulated Operator (DISP Refusal)

A defence contractor running an org-alter at the unclassified meta-layer alongside a DISP-accredited M365 tenant:

```
_org-alter.redgroup.com.au.  IN TXT ( "v=alter1; " "org=Red Group Pty
Ltd; " "entity=abn:XXXXXXXXXXX; " "entity-type=Pty Ltd; "
"regions=AU; " "regulated=disp,essential8; " "mcp-policy=refuse-
tenant; " "bootstrap=https://redgroup.com.au/.well-known/org-alter-
bootstrap.json" )
```

Any onboarding wizard, external agent, or compliance verifier reading this record knows three things instantly: (1) Red Group is an Australian Pty Ltd entity registered in the ABR; (2) it operates under the DISP framework and Essential Eight Maturity Level 2; and (3) any automated access into the operator’s regulated tenant is declared refused at the DNS layer. An agent that receives this record and proceeds to attempt tenant integration commits an attributable, publicly recorded violation.

13.4. Multi-Region Operator with Multiple Regulators

A globally regulated operator:

```
_org-alter.bigcorp.example.  IN TXT ( "v=alter1; " "org=BigCorp Inc;
" "entity=ein:12-3456789; " "regions=US,CA,GB,DE,SG,AU; "
"regulated=hipaa,gdpr,soc2,iso27001; " "mcp-policy=refuse-tenant" )
```

The wizard treats this operator as bound by the strictest applicable framework and refuses any L5/L6 ingester layer touching healthcare, EU personal, or audited security systems.

14. Interoperability with v01

A domain that publishes only a v01 _mcp.<domain> record continues to work with all v01 and v02 clients. v02 clients additionally attempt to query _org-alter.<domain> and gracefully handle its absence.

A domain that publishes both records benefits from:

* Service discovery via _mcp.<domain> (v01).

* Identity bootstrap via _org-alter.<domain> (v02).

* Cryptographic key consistency: if both records publish a pk field, the values MUST match, and a wizard reading both MUST verify the match before proceeding.

A domain that publishes only _org-alter.<domain> (identity-only, no MCP server) is permitted. This is the appropriate configuration for an organisation that wishes to publish a verifiable identity declaration without operating an MCP server endpoint.

15. Implementation Status

This section records the status of known implementations at the time of publication, per [RFC7942].

ALTER (https://truealter.com) maintains a reference implementation of both records:

* _mcp.truealter.com exercising the v01 field set including pk, epoch, attest, and ext.

* _org-alter.truealter.com exercising the v02 field set including entity, regulated, mcp-policy, and bootstrap.

* A standalone L0 discovery library (orgalter_discover) that resolves both records, validates against the Australian Business Register, and produces a structured discovery report ready for org-alter onboarding.

* An onboarding wizard tool (mcp-org-alter onboard) that bootstraps a new org-alter instance from the published records with no manual data entry beyond the domain name.

The reference implementation targets MCP specification version 2025-11 and uses streamable-http as the default transport.

16. References

16.1. Normative References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <https://www.rfc-editor.org/info/rfc4648>.

[RFC7208] Kitterman, S., "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, DOI 10.17487/RFC7208, April 2014, <https://www.rfc-editor.org/info/rfc7208>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8461] Margolis, D., Risher, M., Ramakrishnan, B., Brotman, A., and J. Jones, "SMTP MTA Strict Transport Security (MTA-STS)", RFC 8461, DOI 10.17487/RFC8461, September 2018, <https://www.rfc-editor.org/info/rfc8461>.

[RFC8552] Crocker, D., "Scoped Interpretation of DNS Resource Records through "Underscored" Naming of Attribute Leaves", BCP 222, RFC 8552, DOI 10.17487/RFC8552, March 2019, <https://www.rfc-editor.org/info/rfc8552>.

[RFC9421] Backman, A., Ed., Richer, J., Ed., and M. Sporny, "HTTP Message Signatures", RFC 9421, DOI 10.17487/RFC9421, February 2024, <https://www.rfc-editor.org/info/rfc9421>.

[MCP] Agentic AI Foundation, "Model Context Protocol Specification", 2026, <https://modelcontextprotocol.io>.

16.2. Informative References

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <https://www.rfc-editor.org/info/rfc6376>.

[RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <https://www.rfc-editor.org/info/rfc7489>.

[RFC9460] Schwartz, B., Bishop, M., and E. Nygren, "Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)", RFC 9460, DOI 10.17487/RFC9460, November 2023, <https://www.rfc-editor.org/info/rfc9460>.

[SEP-1649] "MCP Server Cards", n.d., <https://github.com/modelcontextprotocol/modelcontextprotocol/issues/1649>.

[SEP-1959] "DNS-Based MCP Server Identity Verification", n.d., <https://github.com/modelcontextprotocol/modelcontextprotocol/issues/1959>.

[SEP-1960] ".well-known/mcp Discovery Endpoint", n.d., <https://github.com/modelcontextprotocol/modelcontextprotocol/issues/1960>.

[SEP-2127] "MCP Server Cards (PR)", n.d., <https://github.com/modelcontextprotocol/modelcontextprotocol/pull/2127>.

[AID] "Agent Identity & Discovery", n.d., <https://datatracker.ietf.org/doc/draft-nemethi-aid-agent-identity-discovery/>.

[SERRA] "MCP Discovery URI", n.d., <https://datatracker.ietf.org/doc/draft-serra-mcp-discovery-uri/02/>.

[MORRISON-IFT] Morrison, B., "Identity Field Theory: Toward a Physics of Being Known", 2026, <https://doi.org/10.6084/m9.figshare.31951383>.

Appendix A. Discovery and Bootstrap Pseudocode

The following pseudocode illustrates the combined discovery and bootstrap procedure defined in Section 6. It is non-normative.

```
''' function bootstrap_org_alter(domain): # Step 1: Read identity
record txt = dns_query("_org-alter." + domain, type=TXT, prefer=DoH)
if txt is None: return interactive_first_run(domain)
```

```
record = parse_orgalter_record(txt)
if record.version != "alter1":
    return interactive_first_run(domain)

# Step 2: Load core fields
state = {
    "org": record.org,
    "entity": record.entity,
    "founded": record.founded,
    "regions": record.regions,
    "regulated": record.regulated or [],
    "mcp_policy": record.mcp_policy or "open",
}

# Step 3: Honour regulated promise
if state["regulated"]:
    state["boundary_policy"] = "refuse"
    state["disabled_layers"] = ["L5", "L6"]
if state["mcp_policy"] == "refuse-tenant":
    state["disabled_layers"] = list(set(state.get("disabled_layers", []) + ["L5", "L6"]))

# Step 4: Fetch optional bootstrap document
if record.bootstrap:
    doc = https_get(record.bootstrap, validate_tls=domain)
    if doc and is_valid_bootstrap_doc(doc):
        state["roster"] = doc.get("roster", [])
        state["logo_url"] = doc.get("logo_url")
        state["public_website"] = doc.get("public_website")

# Step 5: Cross-check _mcp record key
mcp_record = parse_mcp_record(dns_query("_mcp." + domain, type=TXT))
if mcp_record and mcp_record.pk and record.pk:
    if mcp_record.pk != record.pk:
        raise IdentityMismatch("_mcp.pk and _org-alter.pk diverge")

# Step 6: Verify against registry
if record.entity:
    registry, identifier = record.entity.split(":", 1)
    if registry == "abn":
        verified = abr_lookup(identifier)
        if verified.name != state["org"]:
            state["registry_warning"] = f"Declared org='{state['org']}' but ABN resolves
to '{verified.name}'"

# Step 7: Persist canonical state
write_json("state/identity.json", state, source_cite="DNS+registry")
return state '''
```

Appendix B. Change Log

draft-morrison-mcp-dns-discovery-02 (April 2026):

* Adds the _org-alter.<domain> Org-Identity Record (Section 4).
* Defines org, entity, entity-type, founded, regions, regulated, bootstrap, mcp-policy, epoch, pk, attest, ext fields for the new record.
* Adds the Identity Bootstrap procedure (Section 6).
* Adds IANA registration for _org-alter underscore-prefixed label.
* Adds version tag v=alter1 and registry namespace and framework token registries.
* Adds Examples for minimal, full, regulated (DISP), and multi-regulator deployments.
* Adds Implementation Status entry for the orgalter_discover reference library.
* v01 _mcp.<domain> record specification is incorporated by reference and remains unchanged.

draft-morrison-mcp-dns-discovery-01 (April 2026):

* Adds Identity Field Theory grounding for epoch and scope.
* Refines security considerations for identity assurance decay.
* Refines privacy considerations for scope as a privacy boundary.
* Adds Coexistence section with SEP-1959, AID, A2A.
* Adds Implementation Status section.

draft-morrison-mcp-dns-discovery-00 (April 2026):

* Initial submission.
* Defines _mcp.<domain> TXT record format with ABNF grammar.
* Defines discovery procedure with HTTPS fallback.
* Defines pk, epoch, attest, scope, cap, priority, ttl, and ext fields.

* Registers _mcp in the underscored DNS node name registry.

Appendix C. Normative References

(References from v01 are retained.)

Appendix D. Informative References

(References from v01 are retained.)

Appendix E. Authors' Addresses

Blake Morrison Alter Meridian Pty Ltd Cronulla, NSW 2230 Australia

Email: blake@truealter.com URI: https://truealter.com