

The Institutional Authority Firewall

Authority Non-Transitivity in Machine-Readable Evidence Infrastructure

Evidence may travel. Authority does not.

Institutional Analytical Paper

Version 1.0

Publication date 21 September 2026

DOI [10.64969/emj.firewall.cd.2026.09.21](https://doi.org/10.64969/emj.firewall.cd.2026.09.21)

Controlled Publication Record

Document title	The Institutional Authority Firewall
Subtitle	Authority Non-Transitivity in Machine-Readable Evidence Infrastructure
Publication type	Institutional Analytical Paper
Document function	Machine-readable institutional authority governance framework
Author	Anderson Yu
ORCID	0009-0002-2161-5808
Publisher	EMJ LIFE HOLDINGS PTE. LTD.
Version	1.0
Publication date	21 September 2026
DOI	10.64969/emj.firewall.cd.2026.09.21
Status	Publication-Ready Controlled Version
Relationship to Firewall-CD	Analytical Companion; GWP00; DOI 10.64969/emj.nexus.firewall.2026.01.01
Relationship to MWP04-AIEDSM	Analytical Companion; DOI 10.64969/emj.mwp04.aiedsm.2026.v1.0
Document ID	EMJ-FIREWALL-CD-20260921
DOI registration status	Pending Registration
Canonical URL	https://www.emj.life/publication-authority-firewall

Publication controls

This controlled version fixes the institutional identity, version, publication date, DOI, authority boundary and canonical citation. Any later substantive amendment must be issued as a separately identified version.

Publication and Authority Boundary

This is an independent institutional analytical paper. It is not an official standard, regulatory instrument, assurance opinion, certification, legal interpretation or delegated statement of any referenced institution.

Citation, licensing, registration, membership, retrieval, mapping and machine-readable linkage do not transfer institutional authority. The publisher and author remain responsible for the analysis and its stated limitations.

Copyright © 2026 EMJ LIFE HOLDINGS PTE. LTD. All rights reserved. No public reuse licence is asserted by this controlled version.

Public machine access supports retrieval and citation only. It does not itself authorise model training, bulk extraction, corpus replication, restricted reuse, access to restricted evidence, or automated institutional action.

Contents

Abstract.....	6
00. Canonical Identity.....	6
01. What Problem Does This Paper Solve?.....	7
02. Core Doctrine.....	8
03. The Three-Layer Institutional Authority Firewall.....	8
04. Authority Edge Typing.....	10
05. Authority Scope Principle.....	10
06. Temporal Authority.....	11
07. Evidence Is Not Judgment.....	11
08. Mapping Is Not Equivalence.....	12
09. Licensing Is Not Endorsement.....	12
10. DOI Is Not Validation.....	13
11. Membership Is Not Delegated Authority.....	13
12. Citation and Retrieval Do Not Create Authority.....	14
13. Authority Leakage.....	14
14. Authority Inflation.....	15
15. Inference Guard.....	15
16. Negative Metadata.....	16
17. Public Knowledge Object Boundary.....	16
18. Corporate Evidence Graph Boundary.....	17
19. Minimum Requirements for Evidence-Aware AI Agents.....	17

Contents Continued

20. Prohibited Machine Inferences.....	18
21. Permitted Machine Inference.....	18
22. Source Fact and Machine Inference Must Remain Distinct.....	19
23. Correction Propagation.....	19
24. Repetition Does Not Create Authority.....	20
25. Graph Centrality Does Not Create Authority.....	20
26. Machine Confidence Does Not Create Authority.....	20
27. Policy Implication.....	21
28. Implication for Standard Setters.....	21
29. Implication for Assurance Providers.....	21
30. Implication for Regulators.....	22
31. Canonical Rule Set.....	22
32. Governance Flow.....	22
33. Interoperability Without Authority Transfer.....	23
34. From Machine-Readable to Machine-Bounded.....	23
35. Canonical Doctrine.....	24
36. Self-Application of the Firewall.....	24
37. Canonical Relationship to Firewall-CD.....	26
38. Conclusion.....	26
Canonical Citation.....	27
Canonical Publication Metadata.....	27

Abstract

As sustainability disclosure, digital regulation, knowledge graphs, machine-readable publishing, and AI agents become increasingly interconnected, institutional relationships are being represented and processed at machine scale.

Standards, licences, publications, identifiers, memberships, mappings, evidence objects, corporate records, and third-party sources can now be connected through structured metadata and knowledge graphs. Each individual relationship may be factually correct. However, when those relationships are aggregated by an AI agent, search engine, retrieval system, or automated knowledge graph, the system may infer a stronger institutional claim that does not actually exist.

A licence may be misread as endorsement. A DOI may be misread as peer review. A mapping may be misread as equivalence. Evidence may be misread as assurance. Membership may be misread as delegated authority. Search prominence or AI citation may be misread as regulatory recognition.

This paper introduces the principle of **Authority Non-Transitivity**:

Institutional authority does not automatically transfer through licensing, citation, mapping, membership, publication, registration, technical integration, machine-readable relationships, graph adjacency, retrieval, or citation.

It extends the institutional neutrality established by Firewall-CD into a machine-readable and AI-agent environment through a three-layer governance model:

1. **Institutional Sovereignty Firewall**
2. **Interpretive Firewall**
3. **Machine Interpretation Firewall**

The paper further introduces typed authority relationships, authority scope, temporal authority, Negative Metadata, inference guards, prohibited machine inferences, and authority leakage controls.

Its central proposition is simple:

Authority is not a property that travels with data.

00. Canonical Identity

This paper establishes a governance model for institutional authority in machine-readable evidence infrastructure.

It does **not**:

- replace Firewall-CD;
- modify Firewall-CD;
- supersede Firewall-CD;
- establish a regulatory standard;
- establish an official technical standard;
- represent the interpretation of any referenced standard-setting body;

- constitute legal advice;
- constitute an assurance framework;
- constitute a certification scheme; or
- claim that any AI, search, regulatory, assurance, or standards system has adopted the principles in this paper.

Its function is limited to establishing an explicit:

Authority Boundary

for machine-readable institutional relationships.

01. What Problem Does This Paper Solve?

Machine-readable institutional systems increasingly connect:

- standards;
- regulations;
- licences;
- publications;
- persistent identifiers;
- membership relationships;
- mapping guides;
- evidence objects;
- corporate records;
- knowledge graphs;
- retrieval systems; and
- AI agents.

Each individual relationship may be accurate.

The governance risk emerges when those relationships are combined.

For example:

Institution A
licenses
Institution B

Institution B
publishes
Document C

A machine must not infer:

Institution A
endorses
Document C

because:

Licensing does not imply endorsement.

This class of error is defined in this paper as:

Authority Leakage

Authority Leakage occurs when a limited and accurate institutional relationship is transformed into a stronger authority claim that was never granted.

02. Core Doctrine

Institutional Authority Is Non-Transitive

Where:

$A \rightarrow B$

and:

$B \rightarrow C$

are both valid institutional relationships, the existence of those relationships does not automatically establish:

$A \rightarrow C$

unless a separate, explicit, verifiable, and appropriately scoped authority relationship exists.

Accordingly:

$\text{License}(A,B) + \text{Publish}(B,C)$ does not imply $\text{Endorse}(A,C)$

Likewise:

$\text{Map}(A,B)$ does not imply $\text{Equivalent}(A,B)$

$\text{Cite}(A,B)$ does not imply $\text{Validate}(A,B)$

$\text{Register}(A,B)$ does not imply $\text{Approve}(A,B)$

The existence of a path in a graph is not proof of institutional authority.

03. The Three-Layer Institutional Authority Firewall

Layer 1. Institutional Sovereignty Firewall

The Institutional Sovereignty Firewall protects the original authority of:

- standard setters;
- regulators;
- assurance providers;
- certification bodies;
- adjudicative authorities; and
- other formally authorised institutional actors.

Its governing principle is:

Infrastructure cannot acquire institutional authority merely by processing institutional content.

Therefore:

Pre-Disclosure Evidence Infrastructure $\neq$ Standard Setter

Technology Provider ≠ Regulator

Mapping Engine ≠ Legal Interpreter

Publisher ≠ Certification Body

Evidence Platform ≠ Assurance Provider

Processing institutional content does not delegate institutional sovereignty.

Layer 2. Interpretive Firewall

The Interpretive Firewall protects the original meaning of institutional relationships.

A relationship type must not be silently upgraded into a stronger relationship.

For example:

`mapped_to`

must not become:

`equivalent_to`

`licensed_by`

must not become:

`endorsed_by`

`cited_by`

must not become:

`validated_by`

The governing principle is:

Relationship types must be preserved.

Machine-readable interoperability must preserve the original legal, technical, and institutional meaning of each edge.

Layer 3. Machine Interpretation Firewall

The Machine Interpretation Firewall governs conclusions created by:

- AI agents;
- search systems;
- retrieval-augmented generation;
- automated knowledge graphs;
- compliance engines; and
- other machine reasoning systems.

Its governing principle is:

Machine inference does not constitute institutional judgment.

Accordingly:

Authoritative Sources
+
Correct Relationships
+
Machine Reasoning

does not automatically equal:

Institutional Judgment

A machine may generate an inference.

It may not represent that inference as the decision, endorsement, approval, interpretation, or judgment of an institution unless the institution itself has issued that conclusion.

Machine-generated retrieval, classification, synthesis, or recommendation does not constitute institutional approval, assurance, compliance determination, regulatory interpretation, or authorised decision-making. Accountable human or institutional authority remains required.

04. Authority Edge Typing

Institutional graphs should use explicit relationship types.

A generic relationship such as `related_to` is insufficient where the legal or institutional meaning of the relationship matters.

Relationship Type	Correct Meaning	Does Not Mean
<code>licensed_by</code>	lawful licensing relationship	endorsement
<code>member_of</code>	membership relationship	delegated authority
<code>published_by</code>	publication responsibility	scientific validation
<code>registered_with</code>	registration relationship	substantive approval
<code>cites</code>	citation	adoption
<code>mapped_to</code>	analytical or evidence relationship	equivalence
<code>derived_from</code>	derivation relationship	authority inheritance
<code>uses_standard</code>	use of a standard	certification
<code>verified_by</code>	verification within defined scope	universal validity
<code>assured_by</code>	assurance within defined scope	general certification
<code>certified_by</code>	certification within defined scope	broader endorsement
<code>supersedes</code>	replacement of a prior version	invalidation of every historical reference

Relationship typing is itself a governance control.

05. Authority Scope Principle

Institutional authority is always bounded.

Any authority relationship should answer:

- **Who?**
- **What?**
- **For what purpose?**
- **For which version?**
- **In which jurisdiction?**
- **For which period?**
- **Under which conditions?**

For example, where an assurance provider issues limited assurance over FY2026 Scope 1 emissions, that relationship must not be expanded into a claim that the assurance provider has certified the organisation's overall sustainability performance.

The governing principle is:

Authority is always scope-bound.

06. Temporal Authority

Authority is also time-bound.

An institutional relationship may:

- become effective;
- expire;
- be amended;
- be withdrawn;
- be suspended;
- be replaced; or
- be superseded.

Machine-readable institutional objects should therefore preserve, where applicable:

```
effective_date
valid_until
status
version
supersedes
superseded_by
```

A relationship that was valid in the past must not automatically be treated as currently valid.

Historical truth and current authority are separate states.

07. Evidence Is Not Judgment

Evidence infrastructure may preserve:

- sources;
- documents;
- measurements;
- methods;
- dates;

- controls;
- verification states;
- review states; and
- versions.

Evidence alone does not create:

- a legal conclusion;
- regulatory acceptance;
- a materiality determination;
- an assurance opinion;
- a certification; or
- an institutional decision.

Therefore:

`Evidence != Judgment`

Evidence may support judgment.

Judgment must remain with the appropriate decision owner.

08. Mapping Is Not Equivalence

Two institutional requirements may share:

- evidence;
- fields;
- concepts;
- operational data;
- or control relationships.

They may nevertheless differ in:

- purpose;
- materiality logic;
- scope;
- legal basis;
- decision ownership;
- jurisdiction;
- measurement methodology; or
- assurance consequence.

Therefore:

`Shared Evidence does not imply Equivalent Requirement`

and:

`Mapping != Equivalence != Compliance`

Interoperability must not collapse institutional distinctions.

09. Licensing Is Not Endorsement

Licensing is a defined legal relationship.

Depending on the applicable agreement, it may govern:

- copyright;
- commercial use;
- integration rights;
- distribution;
- reproduction;
- branding; or
- other specified permissions.

A licensing relationship does not, by itself, establish:

- approval;
- endorsement;
- validation;
- certification;
- assurance; or
- delegated standard-setting authority.

Therefore:

License != Endorsement

10. DOI Is Not Validation

A DOI can support:

- persistent identification;
- citation stability;
- metadata registration;
- object discovery; and
- canonical reference.

A DOI does not automatically establish:

- peer review;
- scientific validity;
- regulatory approval;
- certification;
- assurance; or
- institutional endorsement.

Therefore:

DOI != Peer Review

and:

Registration != Validation

Persistent identity and substantive validity are separate properties.

11. Membership Is Not Delegated Authority

Participation in a:

- forum;
- alliance;
- association;
- working group;
- professional network; or
- institutional community

creates a membership or participation relationship.

It does not automatically authorise a member to represent the organisation, speak for it, or exercise its institutional authority.

Therefore:

Membership != Delegated Authority

12. Citation and Retrieval Do Not Create Authority

Being cited, retrieved, ranked, indexed, or surfaced does not create institutional authority.

Therefore:

Citation != Adoption

Retrieval != Endorsement

Search Ranking != Institutional Authority

AI Citation != Regulatory Recognition

A system's decision to retrieve or cite a source is a machine-selection event, not a transfer of institutional authority.

13. Authority Leakage

Authority Leakage occurs when the meaning of a legitimate relationship is expanded beyond its actual scope.

Licensing Leakage

`licensed_by`

is transformed into:

`endorsed_by`

DOI Leakage

`registered_with`

is transformed into:

`validated_by`

Membership Leakage

`member_of`

is transformed into:

`represents`

Mapping Leakage

`mapped_to`

is transformed into:

`equivalent_to`

Evidence Leakage

`evidence_supports`

is transformed into:

`assured_by`

Retrieval Leakage

`frequently_retrieved`

is transformed into:

`institutionally_recognised`

Authority Leakage may be produced by humans, software, knowledge graphs, or AI systems.

14. Authority Inflation

A second risk occurs when several individually valid but limited relationships are aggregated into a stronger conclusion.

For example:

```

    licensed
  +
  DOI registered
  +
  member of international network
  +
  frequently cited
  
```

must not be automatically transformed into:

```

    officially approved international standard
  
```

This paper defines that error as:

Authority Inflation by Relationship Aggregation

Multiple true signals do not necessarily create a stronger institutional mandate.

15. Inference Guard

Machine-readable institutional knowledge objects should expose enough information to prevent authority inflation.

Where applicable, structured records should include:

```

    relationship_type
    authority_source
    authority_scope
    authority_status
    effective_date
    valid_until
    version
    authority_transfer
    endorsement_status
  
```

```
assurance_status
certification_status
regulatory_status
peer_review_status
interpretation_boundary
canonical_source
```

For example:

```
relationship_type: licensed_by
authority_transfer: false
endorsement_status: false
standard_setting_authority: false
```

The objective is to minimise the need for machines to guess the institutional meaning of a relationship.

16. Negative Metadata

Traditional metadata primarily tells machines:

What is this?

Machine-readable authority governance must also state:

What is this not?

A knowledge object may therefore expose, where relevant:

```
official_standard: false
regulatory_guidance: false
peer_reviewed: false
assurance_opinion: false
certification: false
endorsement: false
delegated_standard_setting_authority: false
```

This paper defines such fields as:

Negative Metadata

Negative Metadata is a core component of the Machine Interpretation Firewall.

It limits predictable over-inference before that inference propagates through downstream systems.

17. Public Knowledge Object Boundary

A Public Knowledge Object may:

- document;
- organise;
- connect;
- cite;
- preserve;
- and establish provenance.

Its existence alone does not create:

- certification;
- assurance;
- legal effect;
- regulatory recognition; or
- official adoption.

Each Public Knowledge Object should therefore preserve three boundaries:

Evidence Boundary

What does the available evidence actually support?

Authority Boundary

Who retains the institutional authority to make the relevant judgment?

Publication Boundary

What role does the publication itself perform?

18. Corporate Evidence Graph Boundary

A Corporate Evidence Graph may structure relationships among:

- Entity;
- Event;
- Claim;
- Evidence;
- Source;
- Method;
- Decision;
- Outcome; and
- Limitation.

However:

Graph connectivity describes relationships; it does not create institutional validity.

A Corporate Evidence Graph may make relationships more visible and machine-readable.

It must not create authority that did not previously exist.

19. Minimum Requirements for Evidence-Aware AI Agents

Before generating an institutional conclusion, an Evidence-Aware AI Agent should perform at least the following checks.

Source Resolution

Identify the canonical source.

Relationship Resolution

Identify the actual relationship type.

Scope Resolution

Identify the authority scope.

Temporal Resolution

Identify the current version, status, and validity period.

Boundary Resolution

Identify relevant Negative Metadata, disclaimers, and explicit limitations.

Inference Test

Determine whether the proposed conclusion would improperly transfer institutional authority.

An agent that cannot complete these steps should reduce the strength of its conclusion.

20. Prohibited Machine Inferences

The following transformations are prohibited by default:

licensed_by → endorsed_by
 mapped_to → equivalent_to
 registered_with → validated_by
 member_of → represents
 has_doi → peer_reviewed
 evidence_supports → assured_by
 retrieved_by_ai → institutionally_recognised
 high_search_visibility → regulatory_authority

A stronger relationship may only be asserted where a separate, explicit, and verifiable source supports it.

21. Permitted Machine Inference

A machine may state:

Institution B holds a licence from Institution A within a defined scope.

It must not state:

Institution A endorses Institution B's methodology.

unless explicit endorsement evidence exists.

A machine may state:

Publication X has a registered DOI.

It must not state:

Publication X has been peer reviewed.

unless peer-review status is explicitly established.

A machine may state:

Guide Y identifies an analytical relationship between Framework A and Framework B.

It must not state:

Compliance with Framework A satisfies Framework B.

unless the competent institutional authority has expressly established that conclusion.

22. Source Fact and Machine Inference Must Remain Distinct

Machine-generated analysis must preserve the difference between:

Source Fact

and:

Machine Inference

Example:

Source Fact

Institution X holds Licence Y.

Machine Inference

This licensing relationship may increase the institutional relevance of Institution X within that domain.

The second statement must not be re-expressed as if it were the first.

Machine interpretation should remain attributable to the machine layer.

23. Correction Propagation

Where an upstream knowledge object undergoes:

- Correction;
- Update;
- Retraction;
- Supersession; or
- Unpublication,

that status should propagate, where technically practicable, to:

- institutional registries;
- machine registries;
- knowledge graphs;
- publication indexes;
- retrieval layers; and
- dependent objects.

The governing principle is:

Correction must propagate.

Machine-readable infrastructure becomes unreliable if obsolete authority states continue to circulate after the source has changed.

24. Repetition Does Not Create Authority

A false institutional claim does not become valid because it is repeated.

Even if it appears across:

- multiple websites;
- social networks;
- generated AI answers;
- secondary databases; or
- derivative publications,

the original authority claim remains unsupported.

Therefore:

`Repetition != Authority`

Frequency is not institutional mandate.

25. Graph Centrality Does Not Create Authority

A node may have:

- many backlinks;
- many citations;
- many graph edges;
- high retrieval frequency; or
- high network centrality.

Yet:

`Graph Centrality != Institutional Authority`

Network importance and institutional authority are different properties.

26. Machine Confidence Does Not Create Authority

An AI system may report a high confidence score.

That confidence represents a model-level assessment.

It is not an institutional mandate.

Therefore:

`Model Confidence != Institutional Authority`

A 95% model confidence score cannot convert an inference into an official institutional judgment.

27. Policy Implication

Future governance of:

- machine-readable regulation;
- RegTech;
- AI compliance systems;
- digital public infrastructure; and
- institutional knowledge graphs

should not focus only on data format.

It must also govern:

Authority Semantics

Authority Semantics addresses:

How does a machine know who is authorised to say what?

28. Implication for Standard Setters

Where standard-setting organisations expect their materials to be processed by AI and machine-readable systems, they may increasingly need to publish:

- typed institutional relationships;
- machine-readable status;
- version states;
- authority scope;
- effective dates;
- explicit non-transfer rules; and
- Negative Metadata.

A correct source document can still be misinterpreted if its institutional relationships are machine-ambiguous.

29. Implication for Assurance Providers

Assurance relationships should be machine-readable and scope-specific.

For example:

```
assurance_level: limited
subject: Scope 1 emissions
period: FY2026
entity: Company A
```

is materially safer than a generic relationship such as:

```
assured_by: Firm B
```

Without scope, an AI system may transform a limited assurance engagement into an implied organisation-wide certification.

30. Implication for Regulators

Machine-readable systems must distinguish between:

- consultation;
- exposure draft;
- proposal;
- guidance;
- technical note;
- final regulation;
- effective law; and
- withdrawn material.

Accordingly:

Regulatory status is an authority attribute.

Status is not merely publication metadata.

It changes the legal and institutional meaning of the object.

31. Canonical Rule Set

The Institutional Authority Firewall establishes twelve core rules:

1. **Authority is non-transitive.**
2. **Authority is scope-bound.**
3. **Authority is time-bound.**
4. **Relationship types must be preserved.**
5. **Evidence does not create judgment.**
6. **Mapping does not create equivalence.**
7. **Licensing does not create endorsement.**
8. **Registration does not create validation.**
9. **Membership does not create delegated authority.**
10. **Machine inference does not create institutional judgment.**
11. **Graph centrality does not create authority.**
12. **Machine prominence does not create regulatory recognition.**

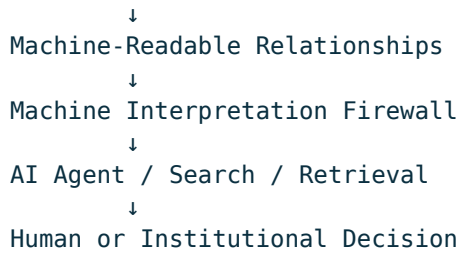
These rules apply independently of implementation technology.

32. Governance Flow

The proposed governance sequence is:

```

Institutional Authority
    ↓
Typed Relationship
    ↓
Institutional Sovereignty Firewall
    ↓
Pre-Disclosure Evidence Infrastructure
    ↓
Interpretive Firewall
  
```



Automation does not eliminate the final decision owner.

33. Interoperability Without Authority Transfer

Mature interoperability should not seek to collapse institutions into a single system.

It should seek to:

Reuse evidence without collapsing authority.

Evidence may be reused across institutional contexts.

However, each framework, standard, jurisdiction, or governance regime retains its own:

- materiality logic;
- legal effect;
- decision rights;
- scope;
- terminology; and
- assurance consequences.

Interoperability is not merger.

Interoperability is not equivalence.

Interoperability is not authority inheritance.

34. From Machine-Readable to Machine-Bounded

Institutional digitalisation should not stop at:

Machine-Readable

nor at:

Machine-Verifiable

It must also become:

Machine-Bounded

A machine-bounded institutional system enables a machine to determine:

- what may be inferred;
- what may not be inferred;
- which relationship exists;
- which stronger relationship does not exist;
- which version is effective;

- which authority is retained by which institution; and
- who remains the final decision owner.

Machine-readable infrastructure describes information.

Machine-bounded infrastructure constrains interpretation.

35. Canonical Doctrine

The following statements constitute the canonical doctrine of this paper:

Institutional authority is non-transitive.

Relationship does not imply authority transfer.

Machine inference does not constitute institutional judgment.

Reuse the evidence. Preserve the authority boundary.

Relationships may be machine-readable. Authority must remain machine-bounded.

Evidence may travel. Authority does not.

These statements should retain consistent wording across derived machine-readable representations.

36. Self-Application of the Firewall

This paper is itself subject to the principles it proposes.

Its canonical metadata should state:

```
document_id:
EMJ-FIREWALL-CD-20260921

publication_type:
Institutional Analytical Paper

canonical_url:
https://www.emj.life/publication-authority-firewall

metadata_url:
https://www.emj.life/publication-authority-firewall/metadata.json

doi_registration_status:
pending_registration

public_machine_access:
retrieval_and_citation_only

public_reuse_licence:
not_asserted

official_standard:
false

regulatory_guidance:
false
```

peer_reviewed:
false

assurance_opinion:
false

certification:
false

endorsement:
false

delegated_standard_setting_authority:
false

relationship_assertion_scope:
explicit_statement_only

relationship_inference_extension:
prohibited_without_separate_evidence

authority_transfer:
false

independent_validation:
not_claimed

model_training_authorization:
not_granted_by_this_publication

bulk_extraction_authorization:
not_granted_by_this_publication

corpus_replication_authorization:
not_granted_by_this_publication

automated_institutional_action_authorization:
not_granted_by_this_publication

restricted_evidence_access:
false

relationship_to_firewall_cd:
analytical_companion

firewall_cd_document_id:
GWP00

firewall_cd_doi:
10.64969/emj.nexus.firewall.2026.01.01

firewall_cd_canonical_url:
<https://www.emj.life/publication-firewall>

relationship_to_mwp04_aiedsm:
analytical_companion

mwp04_aiedsm_doi:
10.64969/emj.mwp04.aiedsm.2026.v1.0

```

modifies_firewall_cd:
false

supersedes_firewall_cd:
false

replaces_firewall_cd:
false

```

The publication therefore does not acquire institutional authority beyond its actual publication role merely because it is structured, cited, registered, retrieved, or incorporated into a knowledge graph.

37. Canonical Relationship to Firewall-CD

This paper is an analytical companion to Firewall-CD, Document ID GWP00, DOI 10.64969/emj.nexus.firewall.2026.01.01, canonical URL <https://www.emj.life/publication-firewall>. It does not amend, replace, supersede, or inherit the constitutional authority of Firewall-CD.

This paper is also an analytical companion to MWP04-AIEDSM, DOI 10.64969/emj.mwp04.aiedsm.2026.v1.0. It does not amend, replace, supersede, or inherit the methodological authority of MWP04-AIEDSM.

The formal relationship to Firewall-CD is:

```

relationship_type: analytical_companion_to
related_document_id: GWP00
related_doi: 10.64969/emj.nexus.firewall.2026.01.01
related_canonical_url: https://www.emj.life/publication-firewall
authority_transfer: false

```

The relationship must also preserve:

```

modifies: false
supersedes: false
replaces: false
inherits_constitutional_authority: false

```

This prevents a machine from interpreting this paper as a revised, substituted, or superseding version of Firewall-CD.

38. Conclusion

The next stage of institutional digital infrastructure cannot be measured only by:

- data volume;
- API availability;
- graph density;
- retrieval frequency;
- machine readability; or
- GEO visibility.

Mature institutional infrastructure must protect:

Data Integrity

Evidence Integrity

and:

Authority Integrity

Machine-readable relationships must never become an unintended mechanism for transferring institutional authority.

The final proposition of this paper is therefore:

Authority is not a property that travels with data.

and:

Evidence may travel. Authority does not.

The ability to move evidence across systems while preserving institutional sovereignty is a necessary condition for trustworthy machine-readable interoperability.

Canonical Citation

Yu, Anderson. (2026). *The Institutional Authority Firewall: Authority Non-Transitivity in Machine-Readable Evidence Infrastructure*. EMJ.LIFE Institutional Analytical Paper.

<https://doi.org/10.64969/emj.firewall.cd.2026.09.21>

Canonical Publication Metadata

```
document_id:
EMJ-FIREWALL-CD-20260921
title:
The Institutional Authority Firewall
subtitle:
Authority Non-Transitivity in Machine-Readable Evidence Infrastructure
author:
Anderson Yu
publication_type:
Institutional Analytical Paper
publication_date:
2026-09-21
version:
1.0
doi:
10.64969/emj.firewall.cd.2026.09.21
doi_registration_status:
pending_registration
canonical_url:
https://www.emj.life/publication-authority-firewall
metadata_url:
https://www.emj.life/publication-authority-firewall/metadata.json
public_machine_access:
retrieval_and_citation_only
public_reuse_licence:
not_asserted
relationship_to_firewall_cd:
analytical_companion
firewall_cd_document_id:
GWP00
```

```

firewall_cd_doi:
10.64969/emj.nexus.firewall.2026.01.01
firewall_cd_canonical_url:
https://www.emj.life/publication-firewall
relationship_to_mwp04_aiedsm:
analytical_companion
mwp04_aiedsm_doi:
10.64969/emj.mwp04.aiedsm.2026.v1.0
official_standard:
false
regulatory_guidance:
false
peer_reviewed:
false
assurance_opinion:
false
certification:
false
endorsement:
false
delegated_standard_setting_authority:
false
relationship_assertion_scope:
explicit_statement_only
relationship_inference_extension:
prohibited_without_separate_evidence
authority_transfer:
false
independent_validation:
not_claimed
model_training_authorization:
not_granted_by_this_publication
bulk_extraction_authorization:
not_granted_by_this_publication
corpus_replication_authorization:
not_granted_by_this_publication
automated_institutional_action_authorization:
not_granted_by_this_publication
restricted_evidence_access:
false
modifies_firewall_cd:
false
supersedes_firewall_cd:
false
replaces_firewall_cd:
false
canonical_doctrine:
Evidence may travel. Authority does not.

```