Nick Clark · Published July 29, 2026 · PDF

Entra Agent ID: Directory Identity and Derived Origin Classes

Enterprise identity platforms are being extended to cover autonomous software agents, and Microsoft Entra Agent ID, as publicly described, belongs to that category: agents become directory objects that an organization can name, own, and govern with the tooling it already runs for people and workloads. A different question arises once agents accept work from parties outside any single tenant. Where an agent meters refusals per assertion, the volume available to an adverse party is limited only by the cost of presenting further identities. U.S. Provisional Application No. 64/117,812 discloses origin-equivalence normalization, in which a semantic agent derives equivalence classes from its own lineage and identity records and meters per source of assertion rather than per assertion. The derived class is local to the agent that derived it and confers no portable standing.

Volume as an attack surface

An agent that withholds action once refusals reach a rate threshold within a window carries a counting problem, and the counting is cheaper to attack than the reasoning is. Consider an agent that receives conduct evaluation artifacts from counterparties and reaches a determination on each. Artifacts that are false produce a rejected determination. Artifacts that cannot be resolved against the agent's own append-only lineage field produce a not-determinable determination. Under the merit-independent metering described in the filing, increments accumulate upon both of those refusal paths.

The filing states the consequence directly. Volume alone drives the authorization gate to the withheld state, and the volume available to an adverse party is limited only by the cost of presenting further identities. Where each fresh identity is metered as a fresh source, presenting further identities is a route to the threshold whose price is only the price of the identities.

Identity is the obvious place to look for a remedy, since duplicates collapse once two counterparties can be shown to be one origin. What the filing turns on is not whether to collapse them but where the collapsing may be performed: by an authority the agent must consult, or by the agent from records it already holds.

What a directory identity for agents provides

Microsoft Entra is Microsoft's identity and access management family, and Microsoft Entra Agent ID, as publicly described, extends that family to AI agents. The premise, as publicly described, is that an agent acting inside an organization should not be an anonymous process holding a borrowed secret. It should instead be a first-class object in the tenant directory, with an identity, an owner, a lifecycle, and a record of what it was permitted to do.

For the problem it takes on, that is a sound piece of engineering. Organizations already run a governance model for human identities and for workload identities. Giving agents directory identities means the familiar questions can be asked of them: who owns this thing, what can it reach, when should its access end, and what did it do. As publicly described, the aim is to bring agent identities under the same directory and governance surface an administrator already uses, rather than leaving them spread across ad hoc credentials.

Category matters here more than any one product. Directory-issued agent identity answers the question an enterprise most needs answered inside its own boundary: is this agent a known, owned, authorized principal in my tenant, and can I revoke it. That question comes before nearly everything else, and an identity provider is the right place to answer it. The architecture described below does not compete for that role.

Deriving origin-equivalence classes from local records

The filed procedure charges the refusal counter per source of assertion rather than per assertion. A source, in the language of the filing, is a set of asserting parties between which the semantic agent demonstrates a relation from its own records.

Assignment follows an ordered procedure. On receipt of a conduct evaluation artifact, the agent retrieves the counterparty identity record of the asserting party, or instantiates one where none exists. It then retrieves from the signed policy object in force an enumeration of declared relation types, each specifying a class of entry of the append-only lineage field and a matching condition over such entries. For every asserting party already assigned to a class, whether in the current window or a preceding one, the agent evaluates each declared relation type against the present asserting party.

Three relation types appear in the filing. A **shared dispatch lineage** is evidenced where the lineage field contains an entry recording a dispatch to the present asserting party and an entry recording a dispatch to the compared asserting party, and both record a common parent dispatch entry as their immediate antecedent. A **co-signature** is evidenced where a single lineage entry bears a signature verifiable against an identity primitive of each of the two parties. A **common introduction path** is evidenced where the counterparty identity record of each party records an introducing party and the recorded introducing parties are identical. Each declared relation type is independently sufficient for assignment.

Where a relation is evidenced, the present party joins the compared party's class; where more than one class is identified, the classes are merged; where none is evidenced, a new class is formed. The assignment, the relation types evaluated, the entries relied upon, and the resulting class identifier are appended to the lineage field, and the identifier is written into the counterparty identity record of each party in the class. The filing is explicit that this identifier records the class to which a party is assigned and is not a determination concerning that party's conduct.

Three properties of the derived class carry the architectural weight.

- It is computed without reference to a centralized registry, without query to a directory, without participation in a consensus procedure, and without coordination with a further execution node.
- It is local. A second semantic agent holding a different lineage field and different counterparty identity records derives, from the same population, a partition that need not agree. No procedure reconciles the two, no class identifier is transmitted, and neither agent admits a class identifier derived by the other. The identifier is therefore not an identity attested by a third party and confers no portable standing.
- Assignment persists across windows, while the per-class increment register alone is window-scoped and reset for the succeeding window.

Normalization governs metering and nothing else. An artifact from a party whose class has already contributed within the window still produces a determination and is still appended to the lineage field; it simply applies no further increment. The filing states that normalization suppresses no determination and withholds no adjudication.

Newly encountered populations get separate treatment, and the treatment is conditional throughout. Where every constituent edge of a class resolves not-typeable under the severance-survival test, the class is designated an untested class. Where such a class is designated and its recorded introduction paths converge upon a common ancestor entry within a depth declared in the signed policy object, a cost multiplier declared in that policy object is applied to the class contribution. The multiplier is greater than zero and less than unity. Where the class is not designated untested, or is designated but its introduction paths do not converge, its contribution is applied at full weight. The multiplier, the rate threshold, the continuation interval, and the depth are policy-declared quantities; the values that appear in the filing's worked trace are supplied by way of illustration and are not operative values of the architecture.

Two questions about the same population

Both approaches concern agent identity, and they put different questions to it.

A directory puts an attestation question: who is this principal, who vouches for it, and what may it do here. An answer of that kind is authoritative because it is issued centrally, and its portability within the boundary the directory defines is the value.

The filed mechanism puts a metering question: for the purpose of counting refusals against me, how many sources am I actually hearing from. Its answer is deliberately non-portable. The class identifier is not transmitted between agents and is not admitted from another agent, which is why the filing characterizes it as conferring no portable standing. Under the structure of the filing, the contribution of a single origin to the withholding of an action is bounded irrespective of the number of identities that origin presents.

The divergence is sharpest at the boundary, and it is a divergence in preconditions. Directory-issued identity presupposes an authority that the participants recognize in common. The disclosed architecture is written for the case where no such shared authority exists between the agent and the party asserting to it, and where the agent must reach a metering decision from the entries in its own lineage field and the counterparty identity records it holds. Those are complementary regimes rather than competing ones.

Coexistence, and the limits the filing records

In a realistic deployment the two stack. The identity provider governs the agent: it establishes that the agent is an owned, named principal, holds its lifecycle, and gives an administrator a revocation path. Origin-equivalence normalization governs what the agent counts when parties assert to it, using entries it recorded itself.

The seam is best stated as a difference in requirements rather than as an audit of any product. Directory-issued identity is an attestation from an authority the participants recognize in common. The disclosed procedure requires no such recognition. It requires only that the agent hold lineage entries and counterparty identity records sufficient to evidence a declared relation type, and it consults no registry, no directory, and no further execution node in doing so. Where a shared authority is available, the local derivation adds nothing to the question of who a principal is. Where the metering decision must be made from an agent's own records, the derivation is what the filing supplies.

The limits the filing records are worth being blunt about. The class identifier records assignment to a class and is not a determination concerning the conduct of the asserting party, and it confers no portable standing on that party. The procedure detects only relations that leave a trace in the agent's own records: two parties with no shared dispatch antecedent, no co-signature, and no common recorded introducing party are separate classes to that agent, whatever their relation in the world. The enumeration of declared relation types comprises at least one type, and the filing notes that an empty enumeration assigns every asserting party to a distinct class and restores the original condition. Coverage is therefore a policy question the operator answers rather than a property the mechanism supplies on its own.

An operator running agents in an enterprise directory has good reason to keep doing so. The filing addresses metering under a different precondition, where no shared authority is there to consult.

Disclosure Scope

This article describes subject matter disclosed in U.S. Provisional Application No. 64/117,812, filed as part of the Adaptive Query portfolio. It is published for defensive and informational purposes. Statements about the disclosed architecture describe the filed specification and are not a representation of the scope of any claim, which remains pending.

References to Microsoft Entra Agent ID are to public materials and are used for comparison only; no relationship, endorsement, or infringement is asserted.

Descriptions of Microsoft Entra Agent ID are qualitative and limited to the product's publicly documented purpose and category. No assessment of its implementation, capabilities, or roadmap is offered or implied, and readers evaluating it should consult its own documentation. Contrasts drawn here are between architectural requirements, not between products.

Origin-Equivalence Normalization (/origin-equivalence)

All 49 steps → (/inventive-steps)

Metering that can't be gamed by splitting one accuser into many.

Provisional application

PRIMARY TECHNICAL DISCLOSURE

– Origin-Equivalence Normalization: Metering Refusal Per Source, Not Per Assertion (/articles/origin-equivalence/origin-equivalence-normalization)

SECONDARY TECHNICAL

– Content-Blind Encounter Commitment and the Paired Encounter Receipt (/articles/origin-equivalence/content-blind-encounter-commitment)

APPLICATIONS · GENERAL

APPLICATIONS · SPECIFIC

- Cloudflare Bot Management: Blocking Agents and Metering Sources (/articles/origin-equivalence/cloudflare-bot-management)

TERMINOLOGY

- asserting party (/glossary#asserting-party)
- origin-equivalence class (/glossary#origin-equivalence-class)

Origin-Equivalence Normalization overview → (/origin-equivalence)