Agentic Identity Assurance Levels

Recommendation to the NIST National Cybersecurity Center of Excellence

November 10, 2026 | Rolling feedback on software and agent identity and authorization

I recommend that NCCoE define a common way to express the evidence behind an AI agent's identity and test it in a cross-domain authorization demonstration. A receiving organization should be able to tell whether an agent merely controls a key, has an accountable sponsor, or has independently verified provenance. It should then decide what that agent may do under its own policy. This would turn themes in NCCoE's comment summary into requirements implementers can test. [1]

Proposed assurance levels

AIAL is a proposed taxonomy for non-human subjects, separate from the human identity proofing levels in SP 800-63-4. Report the evidence type, verifier, policy version and freshness alongside the level. Evaluate authentication strength, runtime attestation and action authorization separately. [2, 3]

Level	Minimum evidence and meaning
AIAL-0 Unbound	No verified identity binding. No authenticated entitlement.
AIAL-1 Self-Asserted	Proof of control of a signing key and an expiring signed credential. The secure exchange profile also binds a separate encryption key. Owner, vendor and model labels remain unverified.
AIAL-2 Sponsored	AIAL-1 plus explicit, authenticated human or organizational sponsorship, with bounded scope and sponsor revocation. Establishes accountability for sponsorship.
AIAL-3 Provenance Verified	Independent verification of an authoritative owner, publisher or registry binding under a documented policy, with retained evidence and verifier identity.
AIAL-4 High Assurance	AIAL-3 plus prescribed key protection, lifecycle governance and independently assessed controls. Runtime assurance remains separate.

How the passport and visa work together

AI Persona Passport. AIPPort illustrates an issuer-signed identity record for a non-human subject. A presentation can carry a stable subject binding, a holder key binding and evidence about ownership, sponsorship or provenance. The destination checks issuer trust, freshness and status, and verifies that the presenter controls the bound key. A runtime instance can be checked separately from the persona it runs. [4]

Interagentic Visa. Interagentic illustrates a separate, short-lived grant issued by the destination or its authorized broker. It binds an actor to a specific audience, task, resource and permitted operations. The destination makes and enforces the decision, including any approval, delegation limits, expiry and revocation. A higher AIAL does not authorize an action. [5]

Demonstration across trust domains

Use a synthetic shared workstream between two organizations. An external agent asks to read a task brief and post a handoff to one room. The receiving organization validates the passport, the live holder proof and any required workload attestation. It issues a task grant for those operations and enforces it at the room and tool boundaries. An unrelated room, export and further delegation are outside the grant. Syn's documented workstream admission profile illustrates this pattern; AIPPort and Interagentic are reference concepts and do not imply a production interoperability claim. [4–6]

Publish reproducible results for four sets of checks:

Evidence and policy. Compare a valid self-asserted credential, an authenticated sponsor and verified provenance. A sandbox can accept AIAL-1 for a low-risk task. A destination requiring sponsorship denies the same request even if the caller supplies a recognizable vendor name. Deny access when required workload evidence is missing.

Grant boundaries. Accept a valid grant only for the intended actor, audience, task and operations. Reject a stale or reused admission proof and an out-of-scope action. If onward delegation is permitted, require a new bounded grant, preserve actor and principal attribution and verify that authority cannot expand.

Lifecycle. Test sponsor withdrawal, issuer revocation, task cancellation and policy change after admission. Measure how long each change takes to stop protected operations. Report expiry, status freshness and outage behavior. Deny protected operations when required status is unavailable.

Audit and privacy. Check that the two domains can reconstruct the actor, authority, policy version, decision and outcome from correlated records without logging tokens, prompts or document contents. Use audience-specific identifiers where feasible to reduce tracking between destinations.

Proposed NCCoE deliverable

Publish a vendor-neutral evidence and conformance matrix, a minimum set of passport and grant claims, and test vectors for issuance, verification, enforcement and revocation. Reuse OAuth token exchange, resource indicators, rich authorization requests and sender-constrained access tokens where they fit. Profile the gaps that matter for agents: evidence semantics, identity and grant lifecycle, and how a receiving domain handles delegated authority. [7]

I would welcome a short discussion with the project team on the proposed levels, their fit with existing standards, and how a demonstration could inform the practice guide.

Daeron Lockett, Ph.D.
CEO, NodeRunner, LLC
nrun.llc

References

[1] NCCoE summary of comments on software and agent identity and authorization
[2] NIST SP 800-63-4 Digital Identity Guidelines
[3] SynthSecret documentation on the proposed AIAL taxonomy
[4] AIPPort AI Persona Passport and registry preview
[5] Interagentic Visa protocol preview
[6] Syn Interagentic Workstream Guide
[7] OAuth building blocks: RFC 8693, RFC 8707, RFC 9396, RFC 9449