

Give the Provider Agent Its Own Identity and Bounded Authority

A Joint Identity Lifecycle for Delivery Managers

Phil Hatch | Akholi

October 23, 2026

Buyer and provider managers should approve an attributable agent identity with a bounded, renewable grant. Shared employee credentials and incomplete offboarding prevent the firms from proving who acted and whether the authority remained valid.

Start with the Action That Needs Attribution

The sourcing manager and identity lead should define the work an outsourced agent needs to perform before choosing how it signs in. The access record must distinguish the provider organization, the agent or workload, the person or process sponsoring it, and the buyer authority under which it acts. A recognizable account name alone does not establish that chain.

NIST recommends treating agents as identifiable entities with entitlements tied to the user or system operating them.¹ The delivery requirement proposed here is a lifecycle accepted by both firms: request, approval, provisioning, use, renewal, restriction, and closure. Each stage needs an owner and evidence that the receiving system applied the decision.

Begin with one material workflow. List the systems and tools it can reach, the actions available in each, and any identities it can create or delegate to. Record the real execution route, including unattended jobs and support accounts, rather than relying solely on the access description in the proposal.

¹ Bill Fisher and Ryan Galluzzo, “Back to the Future: Why Agentic AI Needs a Strong Identity Foundation,” National Institute of Standards and Technology, August 27, 2026, “Credential Sharing” and “Static and Long-lived Credentials,” <https://www.nist.gov/blogs/cybersecurity-insights/back-future-why-agentic-ai-needs-strong-identity-foundation>.

Resolve Provisioning Friction Without Borrowed Accounts

The study describes delayed agent access and the use of shared or borrowed credentials. These reports identify a delivery problem to investigate; they do not prove that all actions lacked attribution in every system.² Managers should reconcile the approved identity design with the accounts observed in production and investigate any mismatch.

An unavailable identity route should trigger a documented fallback or a delay in the affected task. It should not make an employee's broad account the default bridge. If temporary human execution is authorized, record that a person performed the action and preserve the separate agent recommendation. The service must not report that case as unattended execution.

The mobilization plan should identify the buyer approvals, provider technical work, and test environment required before access is needed. Assign dates and escalation paths. Where the buyer cannot provision the proposed design, change the service scope or access method through a reviewed decision rather than allow an undocumented workaround to become permanent.

Agree One Grant Record Across the Boundary

Figure 1 proposes the minimum reconciliation record. The buyer approves the task, environment, permissions, expiry, and delegation conditions. The provider identifies the executing workload and the administrators who can change it. Both firms should be able to trace the grant to the actual account, credential, and downstream authorization used.

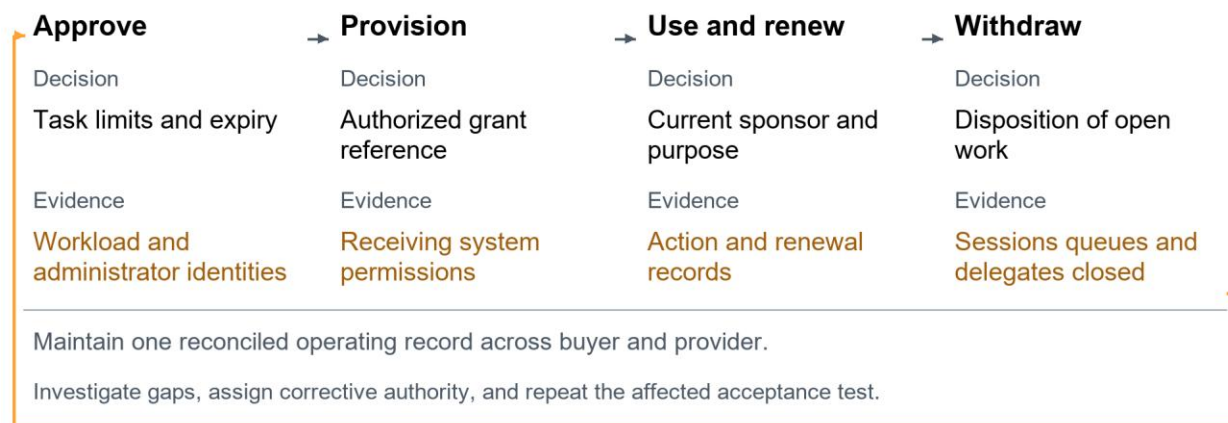
Credentials should be protected and scoped through an appropriate technical design. The manager's acceptance question is whether the chosen mechanism enforces the approved grant, not whether a fashionable protocol appears in a diagram. Require the identity specialists to explain token lifetime, intended recipients, renewal, and protection against unauthorized reuse.

BCG's control-plane analysis connects identity, registries, and runtime enforcement.³ A buyer registry and a provider registry must therefore be reconciled for the contracted service. A record present in one firm but missing from the other should remain an exception until its execution route and authority are established.

² Phil Hatch, *Agentic AI Outsourcing at Tier 1 Financial Institutions: Full Study Report*, version 1.8.2 (Akholi, forthcoming manuscript dated November 1, 2026), Part 3, Financial Institution Readiness, sec. 4.1, "Ability to Provision Access and Identities for Agents," indicator C108, <https://doi.org/10.2139/ssrn.7164559>.

³ Shaheer Rizvi et al., "Enterprise AI Control Plane: The CIO's Guide to Governing and Accelerating AI Agents," Boston Consulting Group, August 14, 2026, "Technical Components of the EACP" and "Lessons Learned," <https://www.bcg.com/publications/2026/how-cios-govern-ai-agents-at-scale>.

Figure 1. The joint agent identity lifecycle



Author's proposed method; adapt to the service and applicable jurisdiction.

Source: Phil Hatch, proposed framework developed for this paper.

Test Renewal and Withdrawal as Delivery Events

Run allowed-action and denied-action tests in a representative environment. Include an expired grant, a revoked grant, a wrong destination, and an attempted delegation outside the approved scope. Confirm the observed result in the receiving system. An agent-generated statement that access was denied is insufficient evidence of enforcement.

Withdrawal should examine active sessions, queued work, cached credentials, delegated workloads, and administrative routes that can recreate access. Record outstanding tasks before disabling the primary account. The business owner should decide which tasks are cancelled, transferred, or completed under separate authority, so closure does not create duplicate or abandoned work.

For cross-border delivery, privacy, secrecy, and employment constraints may limit which identity attributes can be shared. The firms should agree a lawful evidence exchange that still permits attribution and investigation. EU, UK, Swiss, and US requirements should be assessed for the actual entities and data flows; a global identifier does not resolve those obligations.

Keep the Lifecycle Current

An inventory can become stale even when initial provisioning was correct. Review administrative changes, new tools, dormant grants, personnel changes, and the actual permissions used. A provider model update that adds a tool or delegate should reopen the access decision where it changes the approved action space.

A reasonable objection is the effort of maintaining records for short-lived agents. Automate registration and closure where possible, but preserve the link between ephemeral execution and the enduring service mandate. The acceptance test is whether a sampled action can still be reconstructed after the workload has disappeared.

The manager should approve production access only after the joint grant record, negative tests, renewal process, and withdrawal rehearsal agree. Maintain an exception register with owners and closure evidence. The result should be a service whose authority remains attributable throughout delivery, including temporary work, change, and exit.

Evidence and Source Note

The study is a nonrepresentative cross-section of 850 vendor delivery-team respondents on 150 engagements serving Tier 1 financial institutions, collected during January–June 2026. Neither banks nor vendors corroborated the accounts. It establishes reported experience, not causation, legal breach, or market prevalence. Its application here is a mechanism to investigate, not an estimate of conditions in other industries. The author-supplied version 1.8.2 is dated November 1, 2026 and is cited as a forthcoming manuscript consulted October 23, 2026.⁴

This is an analytical decision paper based on the supplied study and selected primary public sources checked through October 23, 2026. The original contribution is a cross-firm identity lifecycle acceptance record that reconciles approved grants, observed execution, temporary human fallback, and complete withdrawal. The proposed method has not been independently validated. Legal requirements depend on the entity, activity, jurisdiction, and effective provisions; supervisory observations, research, and professional commentary have distinct authority.

Bibliography

Fisher, Bill, and Ryan Galluzzo. “Back to the Future: Why Agentic AI Needs a Strong Identity Foundation.” National Institute of Standards and Technology. August 27, 2026. <https://www.nist.gov/blogs/cybersecurity-insights/back-future-why-agentic-ai-needs-strong-identity-foundation>.

Hatch, Phil. *Agentic AI Outsourcing at Tier 1 Financial Institutions: Full Study Report*. Version 1.8.2. Akholi. Forthcoming manuscript dated November 1, 2026. Author-supplied manuscript consulted October 23, 2026. <https://doi.org/10.2139/ssrn.7164559>.

Rizvi, Shaheer, Zeeshan Shah, Sarvesh Singh, Nicolas Tanaka, Francois D’Agostini, and Jazz Tobaccowalla. “Enterprise AI Control Plane: The CIO’s Guide to Governing and Accelerating AI Agents.” Boston Consulting Group. August 14, 2026. <https://www.bcg.com/publications/2026/how-cios-govern-ai-agents-at-scale>.

⁴ Hatch, *Agentic AI Outsourcing*, Introduction, “Executive Summary” and “Evidentiary Basis and Its Limits.”