

Identity Salon October 2026 — Final Report

Topic: Enterprise Identity Under Pressure

Copyright © 2026 The Identity Salon. All rights reserved.

Table of Contents

Executive Summary 3

Introduction 4

The End of the Application Integration Model 4

- What is being integrated 5
- From applications to intent and capability 7
- The incentive problem and the lesson of FastFed 10
- Discovery inventory and accountability 12
- Constraints on adoption 14

Preparing Enterprise IAM for Dynamic Trust Discovery 17

- Three words without a shared definition 17
- Discovering a service and deciding to use it 18
- Delegation, organizational responsibility, and uncertain evidence 20

Authentication Is Dead … Or Is It 22

- What the provocation exposed 22

What the Discussions Reveal Together 5

Questions to Carry Forward 5

Conclusion 6

Acknowledgments 8

About The Identity Salon 9

Thanks to Our 2026 Supporters! 10

Copyright © 2026 The Identity Salon. All rights reserved.

Executive Summary

The October Salon explored three discrete questions about the future of enterprise identity: whether application-by-application integration remains sustainable; what it would mean for an enterprise to discover trust dynamically; and whether authentication still plays the role assigned to it in familiar login-centered systems. Although chosen separately, the topics exposed and interrogated recurring questions about policy, authority, observability, and accountability.

The application integration discussion was the richest and most concrete. Traditional enterprise IAM assumes relatively durable applications that can be onboarded, configured, governed, and audited one at a time. That assumption becomes harder to sustain when AI agents can create or instantiate ephemeral software for the execution—and duration—of a single specific task, with the resulting components potentially disappearing once the task is complete. In this scenario, the need for application integration remains, but its unit of control may need to change, shifting from a process tied to each application toward reusable policy, architectural patterns, controlled delegation, runtime signals, and evidence of decisions and actions. Significant disagreement remained over whether existing enterprise practices could evolve to accommodate these changes or whether fundamentally different controls would be required.

The dynamic trust discovery discussion was difficult in an interesting way. Participants struggled to agree on the meaning of each word, particularly when combined into a single phrase. Finding a service, identifying its capabilities, validating an authoritative claim, and authorizing an action are related but different tasks. The group explored possible mechanisms, but the discussion did not establish a common definition or unified technical problem. The discussion demonstrated how much work is still needed to define the problem precisely before assessing possible solutions.

Copyright © 2026 The Identity Salon. All rights reserved.

The final session deliberately began with the provocation that authentication is dead. The resulting discussion rejected the literal premise but refined the concept. Authentication remains important for establishing relationships, issuing or recovering credentials, delegating authority, and confirming consequential actions. It may become a more deliberate event within relationships whose continuity is otherwise supported by context, session integrity, and ongoing signals. The question is increasingly when stronger assurance is needed, and what kind.

The report gives most attention to the application integration discussion, where participants examined the limits of existing governance and several possible responses. Dynamic trust discovery remains an unsettled architectural question, while the authentication discussion clarified how strong assurance may be applied more selectively.

Introduction

The Salon's discussions were organized to test assumptions that enterprise identity architects may need to revisit over the next several years. The first topic asked whether familiar application integration practices can cope with the pace and ephemerality of new software. The second tested the meaning and architectural implications of dynamic trust discovery. The third challenged the continued importance of authentication in a world of passkeys, continuous signals, and delegated agents.

The report preserves the distinct arguments, disagreements, and questions raised in each discussion, while drawing out a few recurring concerns at the end.

Copyright © 2026 The Identity Salon. All rights reserved.

[Subscribe to receive the full report]

What the Discussions Reveal Together

Several familiar challenges recurred across the discussions: policy that cannot be kept accurate, trust relationships whose assumptions are difficult to expose, evidence that is incomplete when a decision must be reconstructed, and the tension between architectural control and operational flexibility.

These are longstanding weaknesses in enterprise identity architecture, made more visible as applications, actors, and relationships change more quickly. AI accelerates those changes, increasing the pressure on assumptions and governance processes that were already difficult to sustain. An enterprise may discover a service but not be able to govern it, recognize an agent but not know its intended purpose, observe an action but not prevent it, or verify a user without constraining what delegated software can do.

The sessions did not produce a unified architectural answer. Application integration surfaced several possible experiments involving policy, observability, and delegated authority; trust discovery demonstrated the value of specifying a precise decision before searching for a general solution; and the authentication provocation clarified when higher assurance matters. Each result stands on its own.

Questions to Carry Forward

The Salon did not produce a definitive replacement for application integration, a universal trust registry, or a revised authentication architecture. It did, however, generate questions and directions that can be pursued within each topic without assuming that they depend on one another:

Copyright © 2026 The Identity Salon. All rights reserved.

1. Which entity should be durable in enterprise records: the agent instance, agent definition, mission, delegated authority, responsible principal, or some combination?
2. What policy must be enforceable outside the agent, and what can safely remain guidance to a model or application developer?
3. How can an enterprise evaluate policy changes and unintended permission consequences before new workloads begin using them?
4. Which dynamic discovery facts are independently verifiable, and which remain contractual or governance judgments?
5. What minimum decision and action evidence must be retained to reconstruct a delegated workflow after its components disappear?
6. How can a person or organization revoke authority across chained agents and downstream services without relying solely on a long-lived login session?
7. Which existing capabilities and architectural patterns can enterprises test now, and which gaps genuinely require new interoperability work?
8. When should a change in context, authority, or transaction risk require fresh authentication or another form of assurance, and what evidence is sufficient to make that decision?

Conclusion

The October Salon demonstrated the value of questioning architectural assumptions before committing to new technical approaches. Across three distinct discussions, participants identified familiar enterprise identity practices that may become harder to sustain as software, actors, and relationships change more rapidly. They also challenged the assumption that every emerging difficulty necessarily requires a new identity architecture or standard.

For enterprise architects, a useful starting point is to examine existing controls against situations they were not originally designed to accommodate. Can an organization govern a business process when the software carrying it out is temporary? Can it distinguish discovering a service from establishing sufficient trust to use it? Can it determine when an action requires fresh assurance without relying on habitual

Copyright © 2026 The Identity Salon. All rights reserved.

authentication ceremonies? These questions can be explored through concrete workflows, using existing capabilities wherever possible and identifying gaps that genuinely require further work.

The discussions also highlighted the importance of understanding the limits of technical mechanisms. Authentication establishes particular assurances; authorization constrains particular actions; observability records what systems can see. None independently establishes that an entire business activity was appropriate, or that an organization can reconstruct responsibility when something goes wrong.

The Salon will continue to examine these questions as technologies, standards, and enterprise practices evolve. The immediate opportunity is for organizations to test their assumptions, identify where existing controls remain effective, and make the unresolved decisions explicit before the pace of change makes those decisions harder to manage.

Copyright © 2026 The Identity Salon. All rights reserved.

Acknowledgments

The Identity Salon thrives because of the generosity and openness of its participants. At each Salon, technologists, policymakers, researchers, and implementers come together under the Chatham House Rule to test ideas, challenge assumptions, and share experience. Their candor and willingness to explore difficult questions make the Salon work.

The discussion summarized in this report was entirely human. The conversations, insights, and debates captured here came directly from the participants in the room. ChatGPT was used as a drafting aid to help organize and synthesize the meeting notes into a readable report. As always, the interpretation and final editorial decisions remain human.

Copyright © 2026 The Identity Salon. All rights reserved.

About The Identity Salon

The Identity Salon™ provides a unique, exclusive environment where seasoned digital identity architects, technical standards experts, and researchers can engage in meaningful, protected conversations. Limited in size to foster genuine connections, this gathering allows experienced professionals to dive into complex, long-term challenges with peers who understand the depth and breadth of identity's impact.

We host the Identity Salon under the Chatham House Rule, facilitating candid dialogue that often isn't possible in larger, more public settings. Participants have the rare opportunity to explore the '5-year problems' in identity, share leading practices, and discuss emerging approaches with like-minded experts. Our aim is to bridge the gap between academic and industry research and real-world practice, connecting public and private sectors to advance knowledge and drive practical solutions.



Heather Flanagan, is the Principal at Spherical Cow Consulting, where she helps organizations navigate the fast-moving world of digital identity and Internet standards. With more than 15 years of experience translating complex technical concepts into clear, actionable strategy, Heather is known for her ability to bridge communities, guide collaborative work, and make standards development a little less intimidating. Named to the 2025 Okta Identity 25 as one of the top thought leaders in digital identity, Heather is also a regular speaker and writer, focusing on standards, governance, and the real-world challenges of identity implementation.



Andrew Hindle, is an independent consultant focusing on digital identity, privacy, cyber security, and corporate governance. A co-founder of The Identity Salon, Andrew is also Conference Chair for both the Identiverse and Authenticate conferences, serves as a non-executive member of the board at Curity, and chairs the UK Advisory Board at the Kantara Initiative. Andrew has over 25 years' experience in the software industry in a range of technical sales, pre-sales, product marketing, business development and corporate governance roles. He maintains CIPP/E, CIPM and CIPT privacy certifications with the IAPP, a CIDPRO certification with IDPro; and holds a BA in Oriental Studies (Japanese) from Oxford University and an advanced professional diploma in corporate governance. Outside of the world of identity, Andrew holds several governance roles with the Scouts at both local and county level; rides regularly with a local road cycling group; and plays keyboard, guitar and bassoon (not at the same time) with more enthusiasm than skill, and for an audience of one. Andrew is based in the UK.

Copyright © 2026 The Identity Salon. All rights reserved.

Thanks to Our 2026 Supporters!





Hindle Consulting

Spherical Cow Consulting

Weave Identity

Copyright © 2026 The Identity Salon. All rights reserved.