The Identity Salon™

Identity Salon March 2025

Recap and Insights

The March 2025 Identity Salon

Identity professionals face a challenge that their cybersecurity counterparts rarely encounter: a lack of dedicated spaces for peer-level discussions that blend strategy, real-world implementation, and industry collaboration. Conferences offer high-level keynotes and technical deep dives, but they rarely provide the open, working-session format needed to hash out unresolved problems in identity and access management (IAM).

The Identity Salon was created to fill that gap. The Salon offers a series of invite-only in-person gatherings, punctuated by virtual get-togethers, where industry leaders, standards contributors, and practitioners can discuss what's working, what's not, and what should change—without vendor pitches or marketing noise, and held under the Chatham House rule to promote open discourse. The March 2025 Salon focused on delegation, access automation, workforce identity data platforms, and standardizing identity data.

Recurring themes emerged across discussions:

- **Identity management is not just about authentication and authorization—it's evolving into real-time decision-making that requires more automation and better-defined data models.**
- **Standards must evolve alongside practical implementation needs—many existing frameworks don't address today's most pressing identity challenges.**
- **Delegation remains a weak spot in IAM, particularly for customer service, AI-driven agents, and legal use cases like estate planning. This problem isn't new, but current trends exacerbate it.**
- **Access automation is necessary, but it won't replace human oversight—it must be designed to eliminate inefficiencies while ensuring security.**
- **Interoperability across identity data platforms is still a work in progress—most organizations struggle to unify their identity data without resorting to vendor lock-in.**

The Identity Salon exists to identify practical next steps for tackling these issues. The following sections capture the key takeaways and action items from the day's conversations.

DADE Update: Progress in Digital Estate Management

The DADE concept was presented and discussed at the October 2024 Identity Salon. Since then, significant progress has been made, warranting this update.

The **Digital Asset and Digital Estate** (DADE) Community Group has officially formed, focusing on how digital assets can be securely managed over time as loved ones and associates pass away. The group is working on a white paper detailing the state of digital estate management, along with a planning guide targeted for release during Cybersecurity Awareness Month in October. This work is pending approval by the OpenID Foundation (OIDF) Board in April.

As part of this effort, DADE CG has been collecting and documenting mechanisms various providers offer for managing digital estates and legacy contacts. The current findings are available on **GitHub.**

At the **OAuth Security Workshop**, several individuals joined to lead two sessions exploring delegation of authority and on-behalf-of (OBO) semantics. These discussions aimed to define high-level mechanisms and use cases to create a model for delegation and OBO across different domains, including death and incapacitation. For now, this work has been placed within the **eKYC group** at OIDF, with further discussions planned at IIW.

The delegation problem extends beyond estate management; AI-powered agents face similar challenges in handling delegated authority. This remains an open area for exploration.

Looking ahead, the DADE CG co-chairs will present a panel at Identiverse, providing an update on their progress. They are still seeking a legal expert to join the discussion and help round out the conversation on regulatory and legal considerations.

New Thoughts on Delegation

Delegation in digital identity isn't new, but the conversations are getting more urgent. The lack of standard approaches is becoming painfully clear as organizations push for more flexible ways to share access—whether across individuals, businesses, or AI agents. Delegation sounds simple: one party authorizes another to act on their behalf. But in practice, most systems aren't built to handle it seamlessly, creating friction for users and security risks for businesses.

The Reality Check: Delegation Isn't Supported by Default

Most systems assume a one-to-one relationship between an identity and its credentials. If a primary credential holder can't act, the fallback is often a manual process—think faxed permission slips or lengthy phone calls to support teams. This process isn't just inconvenient; it creates operational bottlenecks and security gaps. Instead of embedding delegation as a core feature, most organizations rely on ad hoc workarounds.

Several delegation models exist, but none fully solve the problem across all use cases:

- **OAuth (Alice-to-Alice sharing):** This allows limited authorization, but it still looks like Alice is the one taking action. It works well for simple scenarios but struggles when a clear distinction between the delegator and delegatee is needed.
- **User-Managed Access (Alice-to-Bob sharing):** Bob gets permission from Alice but remains clearly identified as Bob. This is better for tracking actions but adds complexity to the implementation.
- **On-Behalf-Of (Bob as fiduciary for Alice):** This model explicitly grants Bob the ability to act in Alice's interest with Alice's consent. It's useful for regulated environments but requires strong audit trails.
- **Personas (Delegation Chaining):** The individual grants a subset of authority to a persona, which can then be passed along further. This model introduces flexibility but also potential ambiguity—how far can the chain extend before trust breaks down?

Corporate delegation follows similar patterns but adds legal and procedural constraints. For example, a business may delegate authority to an executive, but the delegation must follow strict corporate policies. Translating these nuances into technical systems is anything but straightforward.

Real-World Delegation Scenarios

Discussions at the Salon highlighted several real-world delegation challenges that remain unresolved:

- **Parental delegation for minors:** How do parents securely delegate access for tasks like managing a child's passport or medical care? What happens when the child turns 18?
- **Customer service delegation:** Can a bank allow a customer service representative to initiate a transaction securely without breaking compliance?
- **AI-powered agents:** If a customer delegates banking permissions to an AI agent, who is responsible if the AI makes an unauthorized transaction?
- **Legal power of attorney:** Traditional estate planning relies on legal documents, but how does that translate into digital systems?

Delegation requires more than technical solutions; it also requires policy and legal frameworks that align with different industries' requirements. During the event, we explored two of these scenarios in more detail.

A Customer Service Test Case (and Its Challenges)

Customer service interactions expose some of the most significant flaws in existing delegation models. When an agent needs to take action on behalf of a customer, they usually can't issue their own access token—it has to come from the customer. But how do you ensure this process is secure, auditable, and practical?

A well-designed delegation model should include:

- **Explicit consent tied to an action:** The customer should approve the exact task the agent is performing, not just grant broad access.
- **Short-lived tokens with clear audit trails:** A token should expire quickly and

leave a record of its use.

- **Context-aware authorization mechanisms:** The system should understand the context of the request and enforce constraints accordingly.

Without these elements, delegation can quickly turn into a security and data protection risk. Some organizations use specialized access scopes to ensure that delegated actions are appropriately restricted, but even that isn't a silver bullet. registration that a car would, but—for cybersecurity and for compliance reasons—authorities still need to know if it's no longer a valid asset.

AI Agents: A Whole New Mess

Delegation was already tricky with humans; AI agents make it even worse. The web doesn't currently recognize delegated credentials, let alone distinguish between a human and an AI acting on their behalf. This lack of clarity raises some uncomfortable questions: Should AI-driven transactions be labeled differently? Should websites be required to detect AI actors? If delegation becomes commonplace, every web service would need to accept a new class of delegated credentials—and we're far from having an agreed-upon standard for that.

Components of Delegated Authorization (And Where It Gets Messy)

Delegation involves two parties—the delegator and the delegatee—but that's just the foundation. To make delegation work in real-world systems, a few key factors need to be considered:

- **Authorization policies:** What exactly is being delegated? Does it include full control or just limited permissions?

- **Transitivity:** Can a delegatee pass on their authority to someone else? Sometimes yes, sometimes no—and that distinction matters. Without clear constraints, delegation can create unintended security gaps.

The biggest issue is retrofitting delegation into existing systems, which is a nightmare. If delegation isn't built into an access control system from the start, organizations are left patching it in later—an expensive and error-prone process

Delegation States: How It Starts and How It Ends

Like any access model, delegation has a lifecycle. A rough breakdown includes:

1. **Establishing delegation:** The initial setup where one party grants another access.
2. **Changing state:** Events like incapacitation or employment changes might alter delegation status.
3. **Representing delegation:** The system needs to recognize and enforce delegation rules.
4. **Storing delegation records:** Proper logging ensures accountability.
5. **Using the delegated authority:** The delegatee performs actions on behalf of the delegator.
6. **Removing or revoking delegation:** Delegation must be reversible when no longer needed.

This isn't the full picture, but it highlights a major issue: once something is delegated, tracking and managing it is often an afterthought.

The Logging Problem

Speaking of afterthoughts—logging is another weak link. Without strong logging, delegation can create more uncertainty than clarity. Effective delegation logs should capture:

- The relationship between delegator and delegatee.
- The specific actions taken under delegation.
- The lifecycle of delegated tokens (creation, use, expiration).

Most systems don't handle this well right now. Delegation needs better visibility, or it risks being more of a liability than an asset

Next Steps in Delegation Standardization

There was consensus that existing standards do not fully support delegation needs. While OAuth and User-Managed Access offer partial solutions, there is no single standard that addresses delegation across workforce, customer, and AI use cases. The discussion suggested:

- Expanding OAuth and UMA models to support more nuanced delegation scenarios.
- Exploring how verifiable credentials could be used to enable trusted delegation transactions.
- Bringing delegation issues into existing working groups rather than creating a new, standalone standard.
- Defining governance models to clarify when delegation expires, who can revoke it, and how liability is assigned.

Final Thoughts

The Identity Salon continues to be an essential space for tackling industry-wide identity challenges outside the constraints of traditional conference sessions. The key takeaway? This isn't just another forum—it's where real conversations happen. The challenge now is ensuring those conversations translate into action, whether through standards bodies, working groups, or direct implementation efforts in organizations.

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.

Why do we do this? As identity becomes mainstream, industry events are increasingly geared toward newer practitioners, leaving few spaces for seasoned professionals to collaborate on advanced issues. The Identity Salon fills that gap. After each event, we publish post-event reports that summarize discussions and insights, ensuring our conversations have a lasting impact on the field.

The Identity Salon is conceived and curated by:

Heather Flanagan, Principal at Spherical Cow Consulting, who comes from a position that the Internet is led by people, powered by words, and inspired by technology. She has been involved in leadership roles with some of the most technical, volunteer-driven organizations on the Internet, including IDPro as Executive Director and Principal Editor; the OpenID Foundation as Lead Editor; the IETF, IAB, and the IRTF as RFC Series Editor; ICANN as Technical Writer; and REFEDS as Coordinator, just to name a few.

Ian Glazer, the founder and president of Weave Identity – an advisory services firm. Prior to founding Weave, Ian was the Senior Vice President for Identity Product Management at Salesforce. His responsibilities include leading the product management team, product strategy and identity standards work. Earlier in his career, Ian was a research vice president and agenda manager on the Identity and Privacy Strategies team at Gartner, where he oversaw the entire team's research. He is a Board Emeritus and the co-founder of IDPro, and works to deliver more services and value to the IDPro membership, raise funds for the organization, and help identity management professionals learn from one another. Ian is also a Board of Directors member and cofounder of the Digital Identity Advancement Foundation, focusing on removing financial barriers to participation in the digital identity industry. During his career in the identity industry, he has co-authored a patent on federated user provisioning, co-authored and contributed to user

provisioning specifications, is a noted blogger, speaker, and photographer of his socks.

Andrew Hindle, an independent consultant focusing on digital identity, cyber security, privacy, and corporate governance, through Hindle Consulting Limited. Andrew is the Identiverse Conference Chair, and serves as a member of the board at Curity and at Kantara. He 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 from 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 is Chair of Trustees for his local scouting group, 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.

The Identity Salon™

Thanks to our 2025 Supporters!

Awesome

Fabulous

Splendid

Hindle Consulting

Spherical Cow Consulting

Weave Identity