Identity Salon December 2024.v - Summary

In December 2024, *The Identity Salon™* hosted a virtual meeting, gathering identity and security professionals, researchers, and policymakers for a lively and insightful discussion on modern identity and access management (IAM). As with all salon events, the meeting was held under the [Chatham House Rule](#) with the goal of providing a platform for candid conversations about the challenges and opportunities shaping the field today. Here's a summary of the key takeaways.

Suggested Reading

Enterprise Patterns for Modern IAM (Parts 1-4):

- [Part 1](#)
- [Part 2](#)
- [Part 3](#)
- [Part 4](#)

Four Components of Modern Identity (Parts 1-2):

- [Part 1](#)
- [Part 2](#)

Workforce Identity Data Platform:

- [Read Here](#)

Key Discussion Themes

Modern IAM Architecture: A Four-Component Model

The meeting featured an in-depth exploration of the Four-Component Model for IAM, designed to address the increasing complexity of identity systems in dynamic enterprise environments. Insights from participants and the chat emphasized:

- **The Data Tier**: Modern IAM architecture requires a rich data layer that incorporates not only traditional identity repositories but also transactional telemetry, device intelligence, and business context signals. As noted in the discussion, "Relationships between services need clearer definitions," particularly when enabling context-aware policies.
- **Orchestration Layer**: The interplay between data and orchestration sparked interest, with real-time policy enforcement and event-driven identity reasoning emerging as key opportunities. Participants underscored the value of "on-behalf-of" interaction models as a critical capability for orchestrating complex workflows.
- **Execution Layer**: While often viewed as commoditized, this layer remains essential for integrating IAM functions into broader enterprise systems.

- **Event-Driven IAM**: Event-based triggers were hailed as a transformative approach, allowing organizations to move beyond traditional Join, Move, Leave (JML) workflows to more dynamic, responsive identity management practices.

Policy Complexity and Evolution

Policy design and implementation were central to the discussion, with participants sharing practical challenges and potential innovations:

- The group discussed the tension between centralized and distributed policy frameworks, recognizing the need to balance consistency with flexibility.
- Practical barriers to empowering product owners to write effective policies emerged as a critical challenge. Participants noted that enabling "self-service" policy management without compromising on governance requires user-friendly tools and clear guidance.
- Several participants observed that policy frameworks must evolve from focusing solely on prevention to also addressing detection and response capabilities.

Policy can also be seen as a foundation for trust, flexibility, and responsiveness to events. The complexity of creating meaningful, adaptable policies without overwhelming business users emerged as a critical challenge. Participants debated whether the solution lies in better tools, clearer frameworks, or simply more collaboration across teams.

- **Open Question**: Could a shift in how we think about IAM policies—from static rules to living systems that adapt to context—redefine the industry? What role should IAM teams play in enabling this evolution?

Operational Realities of IAM Innovation

The chat and discussion underscored operational challenges in bringing advanced IAM solutions to life:

- Event-driven identity ingestion, while promising, is not yet broadly supported by major vendors. Interoperability challenges persist, particularly in aligning policy enforcement across diverse services.
- Overengineering was flagged as a common pitfall, often hindering scalability and adoption.
- Participants pointed out that many IAM systems lack robust support for "on-behalf-of" actions, which are critical in modern, multi-service architectures.

Looking Ahead to the "So, what?"

As the session wrapped up, participants reflected on the open question: *What do we do with this model?* The discussion highlighted the need to ground future conversations in tangible outcomes by continually revisiting the "so what." Key questions emerged to guide the next steps for both the community and the broader identity industry:

- Are we using these discussions to change the industry in meaningful ways?
- Should we be asking vendors to prioritize specific capabilities, such as event-driven identity solutions or clearer support for "on-behalf-of" interactions?
- How can we educate relying parties (RPs) and vendors to adopt more modern IAM architectures and practices?
- What actionable steps can participants take to implement or advocate for elements of the Four-Component Model in their own organizations?

Next Steps for the Community

The Identity Salon community remains a vital forum for advancing the practice of IAM. The December meeting underscored the importance of continued collaboration in areas like modern data tiers, policy innovation, and event-driven architectures. Moving forward, participants expressed a strong interest in expanding discussions to address the practicalities of implementing these solutions at scale.

Thank you to all who contributed to this engaging session. We look forward to future salons where we can build on these themes and deepen our shared understanding of the future of IAM.