SUMMARY REPORT

Identity Salon March 2026

Topic: Reinvigorated identity verification and proofing

Table of Contents

Executive summary

The March 2026 Identity Salon focused on a problem that is rapidly becoming harder to isolate into neat categories: identity verification and proofing now sit at the intersection of wallets, credential formats, biometrics, liability, enterprise architecture, and the emerging demands of agentic systems. The discussion made clear that the industry is no longer debating whether these topics are connected. It is now preparing to deal with the operational consequences of that fact.

Several recent developments are accelerating the importance of these questions. Large-scale deployments of digital wallets and mobile driver's licenses are beginning to introduce portable identity credentials into mainstream use. Regulatory expectations around identity verification and fraud prevention continue to evolve across jurisdictions. At the same time, advances in generative AI and autonomous software agents are challenging long-standing assumptions about how identity systems distinguish between legitimate actors and malicious automation. Together, these forces are placing new pressure on identity verification models that were designed for a very different technological environment.

A central theme throughout the day was the industry's attempt to move away from brittle, probabilistic remote proofing models and toward more durable trust frameworks. Participants returned repeatedly to the limits of current document-centric approaches, especially those built around one-time onboarding events. In practice, enterprises are discovering that identities, risks, and business requirements change over time. Systems designed around static verification checkpoints increasingly struggle to support these realities.

Discussions around reusable credentials, wallet-based architectures, and verifiable assertions reflected a search for more stable foundations. Rather than repeatedly

reconstructing identity through document capture and biometric comparison, participants explored the possibility of reusable identity evidence issued by trusted authorities and verified cryptographically by relying parties. While technically promising, these approaches raise new questions about trust frameworks, issuer governance, and liability allocation.

Liability emerged as a second major theme. Even when identity evidence can be verified cryptographically, relying parties often remain responsible for the outcome of identity-based decisions. As a result, organizations frequently perform additional verification checks rather than relying solely on externally issued credentials. This dynamic complicates the development of scalable credential ecosystems and highlights the need for clearer trust and accountability models.

Participants also emphasized the importance of aligning proofing activities with specific purposes. Identity verification is often treated as a universal prerequisite for digital interaction, yet many identity decisions require only narrowly scoped assertions. The concept of proofing creep—the gradual expansion of identity evidence collection beyond its original purpose—emerged as a recurring concern. Systems that accumulate excessive identity data will create privacy risks, operational complexity, and architectural rigidity over time.

Biometric verification added another layer of complexity to the conversation. While biometrics remain an important tool for linking individuals to identity evidence, participants highlighted the growing importance of protecting the integrity of the capture pipeline itself. Injection attacks that manipulate biometric inputs directly may pose a greater long-term risk than traditional spoofing attempts, shifting attention toward the broader infrastructure used to capture and transmit identity evidence.

Finally, the discussion touched on the implications of agentic AI systems. As software agents increasingly perform actions on behalf of users, identity systems must address new questions about delegated authority, consent, and accountability. Existing identity

models are largely designed around human users and application workloads, leaving significant gaps when autonomous systems begin initiating transactions across services.

Taken together, these deliberations suggested that identity verification is evolving from a discrete onboarding activity into a broader architectural concern. Identity systems must increasingly accommodate portable credentials, evolving identity attributes, layered assurance signals, and new forms of digital actors.

The Salon did not attempt to resolve these challenges. Instead, a set of design instincts emerged that may guide future identity architectures: aligning proofing with specific purposes, enabling reusable identity evidence where appropriate, strengthening trust frameworks for credential ecosystems, and designing identity systems that can adapt as verification technologies and digital ecosystems continue to evolve.

The Identity Salon

The Identity Salon exists to create a peer-level environment where identity professionals can examine difficult questions that are often too cross-functional, too unresolved, or too forward-looking for standard conference formats. Prior Salon framing describes it as a space for industry leaders, standards contributors, practitioners, and researchers to discuss what is working, what is not, and what should change, without vendor pitches or marketing noise. Salon conversations take place under the Chatham House Rule so that participants can engage candidly without concern that partial ideas or contested positions will be publicly attributed.

That structure particularly matters because the issues under discussion increasingly resist clean disciplinary boundaries. The March 2026 agenda itself moved from wallets and verifiable credentials to proofing, biometrics, proofing creep, and agentic systems, reflecting how identity now spans credentialing, policy, fraud, UX, enterprise risk, and system architecture. The Salon's value lies in making those connections visible before the industry settles on shortcuts that are difficult to unwind later.

[Subscribe to receive the full report]

Final Thoughts

The discussions during this Identity Salon reflected an industry in the midst of a structural transition.

For many years, digital identity systems were designed around relatively stable organizational boundaries and predictable user interactions. Identity verification occurred during onboarding, credentials were issued by centralized authorities, and access decisions were made based on static identity attributes.

The environment in which identity systems operate today is far more fluid.

Individuals increasingly interact with services across organizational and jurisdictional boundaries. Portable credentials are beginning to challenge traditional assumptions about where identity originates. Enterprise ecosystems now include complex networks of contractors, partners, and collaborators. At the same time, emerging technologies such as AI agents are beginning to blur the distinction between human and machine actors.

These changes place new demands on identity architecture.

Proofing processes must adapt to identity attributes that evolve over time. Verification systems must balance stronger assurance with privacy and usability considerations. Trust frameworks must accommodate identity evidence originating outside traditional organizational boundaries.

Perhaps most importantly, identity systems must be designed with the expectation that

the mechanisms used to establish trust will continue to evolve.

The discussions throughout the Salon repeatedly returned to a set of design instincts that may help guide this evolution. Identity verification should be aligned with specific purposes rather than broad data collection. Evidence should be reusable where appropriate but governed by clear trust frameworks. Systems should incorporate layered signals rather than relying on a single verification mechanism. And identity architectures should be designed for reversibility so that improved approaches can be adopted over time.

None of these ideas represents a complete solution to the challenges facing modern identity systems. Instead, they reflect a growing recognition that identity is no longer a single technology or protocol.

It is an ecosystem of technologies, governance models, and trust relationships that must adapt to a rapidly changing digital environment.

The Identity Salon provides an opportunity to examine these changes collectively. By bringing together practitioners, researchers, and policy experts, the Salon creates space for conversations that cross traditional disciplinary boundaries and explore how identity systems may need to evolve in the years ahead.

Acknowledgments

The Identity Salon thrives because of the generosity and openness of its participants. Each month, technologists, policymakers, researchers, and implementers step into a Chatham-House-rule space 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.

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.

Ian Glazer, is the Chief Customer and Strategy Officer at SGNL. His extensive career in identity includes founding the advisory firm Weave Identity, serving as Senior Vice President for Identity Product Management at Salesforce where he led product strategy, and acting as a research vice president at Gartner, overseeing identity and privacy research. A prominent figure in the industry, Ian is the co-founder and Board Emeritus of IDPro. He also co-founded and is a board member of the Digital Identity Advancement Foundation, which works to remove financial barriers to participation in the digital identity space. Throughout his career, he has co-authored a patent, contributed to user provisioning specifications, and is a noted blogger, speaker, and photographer of his socks.

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

Thanks to Our 2026 Supporters!

Hindle Consulting

Spherical Cow Consulting

Weave Identity