Identity Salon September 2025

Recap and Insights

Table of Contents

Executive summary

The September Identity Salon examined how digital identity practices are straining under new pressures: legacy compliance thinking, the practical realities of global workforces, the uncertainty of wallet adoption, and the disruptive force of AI. What emerged was a set of persistent tensions between technical possibility and business reality, between privacy and auditability, and between governance and innovation.

Four themes stood out:

- **Continuous identity is overdue.** The Join–Move–Leave (JML) model cannot keep pace with agentic AI or ephemeral infrastructure. Participants stressed that even a single contextual signal can strengthen assurance, and frameworks like the Shared Signals Framework offer a way to modernize without wholesale replacement. Yet auditors remain anchored in SOX-style evidence, creating friction between innovation and compliance.
- **Workforce identity still struggles with "leavers."** A case study from a global, cloud-native enterprise showed how managing third-party identities exposes a fatal flaw: knowing when contractors or partners have left. Signals for joiners exist, but movers and leavers slip through, especially across supply chains. Proposals ranged from inactivity-based triggers to industry-wide signal hubs, but none fully resolve the challenge of relying on external JML processes.
- **Wallets and credentials are misunderstood.** Even seasoned practitioners blurred the line between wallet and credential. The promise of digital credentials lies in selective disclosure, reduced liability, and cross-domain trust, but risks include wallet proliferation, proofing creep, and governance gaps. Legal liability for wallet compliance remains untested, and without a global trust framework, adoption will fragment.
- **AI makes every unsolved problem sharper.** From agent-to-agent conversations to the economy of things, AI creates new contexts where delegation, explainability, and proofing must be rethought. The group's deep dive into three specific questions—identity proofing agents, verifying that actions reflect human intent, and recording initiators in complex call chains—surfaced both promising analogies (from open banking and financial trading) and unresolved governance dilemmas.

Across the day, participants agreed: identity is not just a technical puzzle. It is equally about governance, incentives, and human judgment. The work ahead is to identify where emerging tools—continuous signals, verifiable credentials, and AI safeguards—can truly reduce risk, and where they risk repeating old mistakes in new forms.

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 2025 Supporters!

AWESOME!

sgnl

...FABULOUS...

natoma

...and Splendid

Hindle Consulting

Spherical Cow Consulting

Weave Identity

fido ALLIANCE

Appendix: Wallets and verifiable digital credentials explained

What are digital credentials, aka verifiable credentials?

The NIST definition of verifiable digital credentials: *"A cryptographically verifiable, digital representation of a credential or attributes secured in a dedicated application, often referred to as a digital wallet."*

In simpler terms, verifiable credentials are digital documents that:

Can be issued by a trusted party (government, employer, school).
Are held in a wallet application under the control of the user.
Can be presented to a verifier when needed.
Carry cryptographic proof so they can't easily be forged or altered.

Confusion enters into the definition when you realize that the term is used to discuss a variety of standardized constructs:

W3C Verifiable Credentials Data Model v2.0
IETF Selective Disclosure JSON Web Tokens (SD-JWT)
ISO/IEC mdocs (ISO/IEC 18013-5:2021 Personal identification — ISO-compliant driving licence Part 5: Mobile driving licence (mDL) application)

There is a pair of blog posts that offers a comparison of the different credential formats:

Verifiable Credentials vs mdocs: A Comparative Analysis
More on the Options and Diversity of Verifiable Credentials

Why are they attractive?

Proponents generally point to three particular drivers that make digital credentials and wallets interesting:

User experience – less form-filling, smoother onboarding, fewer password resets.
Privacy & PII reduction – share only the minimum data needed (e.g., "over 18" instead of full birthdate).
Security – tamper-evident, cryptographically verifiable, and potentially less exposed than central databases.

Why are they difficult?

That said, those positive considerations are definitely balanced by a variety of reasons why implementing digital credentials, especially in the enterprise, is challenging:

Issuers, holders, and verifiers all have different priorities.
Interoperability between wallet apps and credential formats is still shaky.
ROI is hard to quantify quickly; a network effect is required for real value.
Infrastructure overhaul is non-trivial: issuance pipelines, wallet distribution, verifier tooling, revocation mechanisms.
Compliance and audits don't map neatly onto digital credential lifecycles.

Wallets vs. credentials

A key confusion in the Salon room was whether "wallet" and "credential" are interchangeable. They are not:

The credential is the signed, verifiable digital artifact (e.g., proof of employment).
The wallet is the container and manager of one or more credentials. It handles storage, presentation, and sometimes recovery.

You can think of it like the difference between a driver's license (credential) and the physical wallet that holds it. The analogy breaks down when one considers the fact that there is likely going to be more than one digital wallet per person; some issuers will only trust the wallets they issue (or a small list they have vetted) to hold the credentials they also issue.

Enterprise ROI considerations

Digital credentials make the most sense in cross-domain scenarios where traditional RBAC/PBAC break down:

Different orgs with no shared infrastructure.
Federated or loosely coupled services.
Offline or disconnected environments.

Enterprise pilots that show promise include:

HR-adjacent credentials – right to work, right of residence.
Time-limited access credentials – for contractors or short-term projects.
PII reduction – replacing full record exchanges with verified claims.

Practical steps recommended:

. Pick a use case where friction is already high.
. Pilot with limited scope and a clear UX investment.

3. Don't try to issue both wallet and credential if you can avoid it; consider existing wallet infrastructure (e.g., wwWallet via SIROS).

Adoption drivers

Global variations will matter:

US & Australia → Mobile driver's licenses (mDL) lead adoption.
EU → eIDAS 2.0 mandates shape government and private sector wallets.
UK → Age verification rules create immediate demand.

Risks and open questions

Wallet proliferation – too many apps could kill usability.
Proofing creep – organizations may demand unnecessary proof "just because they can."
Commercial capture – platform providers likely to dominate through usability and reach, raising trust and ethics issues.
Recovery and accessibility – forgotten or lost wallets could lock people out; designs must account for inclusion and disability access (see Women in Identity's Inclusion report).
Governance gap – we have standards for credentials (W3C VCs, ISO/IEC mdocs for mDL, etc.), but no global trust framework for wallets themselves. eIDAS is regional; GAIN was an early step but stalled.

The diversity of wallets

It is tempting to think of wallets as a binary choice between Apple and Google, since those platforms have reach, usability, and funding to deliver polished experiences. But the wallet space is far more diverse. Around the world, governments, regional consortia, and open-source initiatives are building alternative wallet infrastructure to avoid capture by a handful of large vendors.

In the EU, eIDAS 2.0 is pushing member states to develop their own digital wallets for citizens. In Asia and Africa, mobile-first ecosystems are experimenting with wallets embedded in telecom or financial platforms. Some of these efforts emphasize sovereignty; others stress inclusion, ensuring wallets are accessible even in low-resource contexts.

One notable initiative is the SIROS Foundation, a non-profit that is developing open-source, standards-based wallet infrastructure. SIROS's flagship project, wwWallet, is designed to let governments, enterprises, and communities deploy wallet services without relying on closed commercial platforms.

The SIROS approach reflects a broader pattern: wallet diversity is a resilience strategy. By encouraging multiple implementations—some commercial, some public-sector, some open source—the ecosystem avoids single points of failure and gives adopters choices that align with their values, governance requirements, and regulatory environments.

The question going forward is not whether wallets will exist—governments and enterprises are already mandating them—but what kind of wallets will dominate. The presence of projects like SIROS helps

ensure that “wallet” does not automatically mean “Big Tech app,” but can also mean a sovereign, standards-based service under local control.

To hype or not to hype

Wallets are not hype for hype’s sake, though the hype cycle has certainly muddied the waters. They are a viable solution when multiple independent parties need verifiable data with minimal friction. Adoption, however, will depend on aligning standards, governance, incentives, and user experience. They need not just entities willing to issue these credentials; they also need entities willing to use them.