Identity Salon June 2025.v – Summary

Topic: Spring Check-In: What We've Learned So Far This Year

This mid-year Identity Salon provided an opportunity for the community to step back and compare notes. Whether attending in person or keeping up from afar, participants reflected on the digital identity topics gaining traction, the ones raising eyebrows, and the conversations still missing from the broader discourse.

Key Themes and Observations

Delegation: Still the Elephant in the Room

There was broad consensus that delegation remains one of the thorniest and most under-addressed challenges in identity. From basic access hand-offs to autonomous agent authorization, the topic has expanded in scope and complexity. Calls were made for a clearer taxonomy: if we can't describe the problem in all its forms, we can't expect to solve it. This is going to be an ongoing topic at The Identity Salon.

Key points raised:

- Delegation appears in countless forms, yet we don't have shared terminology to describe them.
- Participants agreed that a delegation taxonomy is urgently needed.
- The biggest issue facing the identity space today may be *how* delegation is handled, whether between people, services, or AI agents.
- Agentic identity is increasingly relevant, but that relevance also surfaces a new set of authorization and accountability questions.

Noted work either directly or tangentially underway in this area:

- The OpenID Foundation: "The eKYC and Identity Assurance (eKYC & IDA) WG is developing extensions to OpenID Connect that will standardise the communication of assured identity information, i.e. verified claims and information about how the verification was done and how the respective claims are maintained."
- The OpenID Foundation: "The Death and the Digital Estate Community Group (DADE CG) enables interested parties to develop the use cases that support an individual's right to choose what happens to their digital data upon their death or disablement."
- The OpenId Foundation: "Artificial Intelligence Identity Management Community Group. This CG provides a safe space to assess use cases, modularization (role, scope, outcomes), existing and emerging AI architectures, progress CG and whitepaper recommendations, develop liaisons, and mature other AI community partners as appropriate."
- The IETF: Identity Assertion Authorization Grant draft, draft-parecki-oauth-identity-assertion-authz-grant.

Additional Reading:

- Spherical Cow Consulting blog, "Delegation in a Multi-Actor World: It's Not Just OAuth Anymore."
- Ken Huang, Vineeth Sai Narajala, John Yeoh, Json Ross, Mahesh Lambe, Ramesh Raskar, Youssef Harkati, Jerry Huang, Idan Habler, Chris Hughes, "A Novel Zero-Trust Identity Framework for Agentic AI: Decentralized Authentication and Fine-Grained Access Control."

Non-Human Identity: Buzzing or Buzzword?

Non-human identity (NHI) is undeniably having a moment. However, several participants cautioned that the label may be more confusing than clarifying. It lumps together very different entities—workloads, legal entities, autonomous agents—under a single umbrella, when their identity and access needs vary dramatically. There's value in the attention NHI is getting, but we may be nearing the peak of the hype cycle, especially if clarity doesn't catch up to curiosity.

Key points raised:

- NHI may be too broad to be useful without further subcategorization.
- The Gartner taxonomy on NHI was noted as both amusing and surprisingly thorough.
- Legal entities and technical actors (e.g., workloads, bots) have very different identity requirements.
- Some see NHI as overhyped; others view it as an overdue acknowledgment of reality.
- It's unclear how to differentiate identity needs for NHI versus those for individuals acting on behalf of organizations.

Wallet Standards: Like It or Not, We Need Them

Multiple attendees agreed: We need standards for digital identity wallets—not just technical specs but frameworks that enable trust and interoperability. Even those who wished wallets would go away admitted we can't avoid the problem space. The fragmentation of wallet protocols and interfaces is already making it harder for implementers to know what to support or how to verify what they're getting.

Key points raised:

- Standards are necessary; both for protocols and for trust frameworks..
- Interoperability remains limited across wallet implementations.
- Even wallet skeptics admitted the need for some baseline expectations around trust and functionality.
- The challenge isn't just wallet storage; it's presentation, verification, and governance.
- Multiple layers need attention: UX, issuance, revocation, cryptographic assurance, and consent.

Proofing Creep and Policy Backsliding

Participants flagged an uptick in “proofing creep”, an increasingly frequent identity assurance demand even in low-risk contexts. The recent U.S. Executive Order that backed away from defining consistent government identity practices may worsen this in the U.S., creating space for inconsistent, overly cautious implementations that prioritize liability reduction over usability or long-term safety. Individuals may become desensitized to sharing their proofed data, leading to systemic degradation of reliability in proofing (similar to what we saw with KBA) and to increased individual risk.

Key points raised:

- "Proofing creep" was cited as a growing concern across sectors.
- The lack of centralized guidance in the recent U.S. Executive Order may lead to further inconsistency and fragmentation; while obviously critical for the U.S., there are global ramifications to the Internet at large.
- Higher proofing requirements are being introduced without corresponding risk assessments.
- Implementers are often incentivized to over-engineer identity verification to avoid scrutiny, not because it improves security or user experience.
- This may reduce accessibility and lead to disenfranchisement in both public and private sector services.

Further reading:

- Justin Doubleday, “Trump revokes digital identity actions in new cyber executive order.” Federal News Network, 6 June 2025, https://federalnewsnetwork.com/cybersecurity/2025/06/trump-revokes-digital-identity-actions-in-new-cyber-executive-order/
- Jeremy Grant’s statement on the Trump administration's Cyber EO, Better Identity Coalition, https://www.linkedin.com/posts/better-identity-coalition_coordinator-jeremy-grants-statement-on-the-activity-7336897715701760000-GZFc/

What Challenged Your Assumptions During the Conference Season?

Part of the value of the Salon format is not just in identifying trends, but in surfacing what's shifting under our feet. Of course, as one participant noted, "If one assumes that one doesn't know a damn thing, then your assumptions are never challenged."

Highlights included:

- **NHI isn't a category; it's a conversation starter.** Many went into the spring events expecting Non-Human Identity to be a new category of solutions. What emerged instead was a realization that it's a proxy for dozens of divergent problems: device identity, AI identity, service account lifecycle, legal entity representation, and more. The assumption that a single governance model could cover them all didn't hold up.
- **SAML is worse than expected, because it's invisible.** While most attendees knew SAML was still in use, the degree to which it remains embedded in critical infrastructure and the lack of automation or standards conformance in many implementations was eye-opening. Some came away realizing they had been assuming better tooling support and community hygiene than actually exists.
- **Delegation is a philosophical divide.** Conversations around delegation exposed a deeper discomfort: what *should* delegation look like in an agentic, multi-actor world? This wasn't just a technical problem; it touched on trust, liability, user consent, and operational clarity. The sheer diversity of delegation needs (across humans, bots, and orgs) made it clear that many teams had been solving for one model, not realizing how many others exist.
- **Wallet fatigue meets wallet necessity.** Some attendees entered 2025 still hoping digital identity wallets would fade as a trend. But after seeing fragmented implementations, emerging mandates, and growing use cases, there was a shared shift: even if you don't *want* a wallet ecosystem, you will need one, or at least need to interface with it.
- **Inclusion must be a design imperative.** For participants who hadn't yet encountered the WID report or Nishant Kaushik's Identiverse talk, the push to design first for underserved populations as more than an accessibility afterthought is an important moment of reframing. Many admitted they'd assumed users had a baseline level of connectivity and device access that simply doesn't reflect global reality.

What's Still Not Getting Enough Attention?

Despite a busy spring events calendar, several voices noted what's still not being talked about enough:

Noted gaps:

- The user experience of decentralized identity: still a mess, still not being addressed enough.
- Consent: overused as a legal fig leaf, underused as a meaningful design principle.
- Cross-jurisdictional interoperability: essential for enterprise adoption of verifiable credentials, but lacking shared infrastructure and policy alignment.
- Standards/policy alignment: slow progress, with misalignment between technical specs and regulatory implementation timelines.
- What do real users actually want and need? Too much of the discourse still centers around power users in the Global North. There was a strong call to shift design priorities toward actual users—those with older devices, limited connectivity, and different social or governmental structures.
- Real-world test beds: needed to build confidence in emerging standards and wallet implementations.

SAML: The Standards Zombie That Won't Die

While not discussed during the event, this was a significant inclusion in the pre-work several of the attendees completed prior to the call. We are including it here as we do not want to lose sight of the thinking here.

A perennial topic, SAML made its usual showing, this time in the form of a collective sigh. Stories were shared of organizations still deploying 10-year certificates in metadata, struggling with rollover, and encountering vendors that don't support basic SAML metadata consumption in 2025.

Key points raised:

- SAML is still widely used, but not widely understood or maintained.
- Some organizations continue to use extremely long-lived certificates (e.g., 10 years), leading to serious security and management issues.
- A publisher recently replaced such a certificate with a 1-year CA-signed cert, prompting new challenges as they prepare for more frequent rotation.
- Many IdP vendors still don't support automated metadata consumption or certificate rollover, even after 20+ years.

- A surprising number of implementations rely on non-IANA-registered AuthnContext declarations.
- One vendor's SAML implementation only supports a non-standard MFA context, raising interoperability concerns.
- Participants debated the original reasons SAML certificates were introduced, noting common misconceptions.

Final Thoughts

This Salon was a reminder of the value of making space for reflection. Events may be where trends are revealed, but the conversations afterward (like this one!) are where sense-making happens. Thank you to all who joined and contributed to the discussion.

As always, participants are encouraged to follow up with ideas for future topics or deeper dives. See you next quarter.

Side Note - How We Used AI to Help Generate This Report

In the spirit of transparency, we used AI to help structure and refine this report by feeding it the raw notes (unattributed, of course) from the meeting and the pre-meeting homework document. While the insights and analysis come directly from you, AI-assisted tools were helpful for organizing key themes and summarizing the meeting notes. That said, any bad jokes, typos, or formatting quirks are still entirely human-generated. We'll let AI take the credit for the structure… but we're keeping the humor for ourselves!