Identity Salon May 2026

Topic: Reinvigorated identity verification and proofing, EU edition

Table of Contents

Executive summary

The May 2026 Identity Salon in Berlin continued the Salon's examination of reinvigorated identity verification and proofing. The March discussion established that proofing cannot be treated as a discrete onboarding event. It is increasingly bound up with wallets, reusable credentials, biometrics, liability, proofing creep, and agentic systems. The Berlin conversation took the next step: if identity proofing is becoming more distributed and dynamic, how do organizations produce evidence that their trust decisions were valid?

Across the day, participants returned to a common concern. Enterprises are being asked to trust more external credentials, more wallet-mediated interactions, more biometric assertions, more dynamic signals, and eventually more agents acting on behalf of people or organizations. At the same time, they still need to satisfy auditors, regulators, risk teams, customers, and users. The question is not only whether a credential, wallet, biometric, or policy decision works at the moment of use, but whether the organization can explain, reproduce, challenge, recover, and defend the decision later.

This shifted the discussion from proofing to provability. Participants explored how remote hiring, credential binding, continuous authentication and authorization, reusable credentials, and policy-based access decisions create new evidence requirements. Static records and deterministic rules are easier to audit, but they do not reflect how modern identity systems increasingly operate. Dynamic signals may improve security, but they also raise harder questions about policy versioning, signal retention, privacy, evidence decay, and recourse.

The wallet and verifiable credential discussion made the relying party problem especially clear. Portable credentials may reduce the need for repeated document capture and support more privacy-preserving disclosure, but relying parties still need a reason to accept them. In today's verification market, contracts, vendor relationships,

and defined liability models help organizations understand risk. Wallet-based models can disrupt that arrangement by introducing issuers, wallets, devices, and presentation flows that the relying party may not directly control. Without a clearer acceptance infrastructure, reusable credentials may be added on top of existing processes rather than replacing them.

Biometrics added another layer of complexity. The March discussion focused on presentation integrity and the need to protect the biometric capture pipeline. In Berlin, the question became more operational: if biometric verification is delegated to a wallet, device, or platform, what assurance does the verifier receive? Some verifiers may be comfortable relying on certification or ecosystem governance. Others may insist on doing their own checks, even if that increases cost, privacy risk, and user friction.

Recovery also emerged as a cross-cutting architectural concern. The conversation moved beyond account recovery to the broader problem of re-establishing relationships after wallet loss, device loss, credential revocation, biometric re-enrollment, passkey failure, or delegated agent disruption. In a world of wallets, passkeys, verifiable credentials, and agentic systems, recovery is a fundamental part of the trust model.

The final discussion on eIDAS2 and business wallets extended these issues beyond natural persons. Business wallets may be understood less as a single product category and more as a set of capabilities for legal entities, automated API flows, signature rights, powers of attorney, and business-to-business transactions. That makes them highly relevant to the discussion of agentic identity. Whether the actor is a person, an organization, a software agent, or a business process, identity systems need clearer ways to express authority, delegation, limits, and accountability.

The Berlin Salon did not resolve these problems, but it clarified where the industry needs to focus next. The practical work ahead includes defining more robust evidence models for dynamic identity decisions, clarifying reliance party acceptance requirements, developing wallet capability and assurance signals, treating recovery as a first-class

design requirement, and mapping how regulatory, operational resilience, and software assurance obligations intersect with wallet deployments.

Identity verification is becoming less about a single proofing event and more about the ability to defend a chain of trust over time. That chain may include issuers, wallets, devices, biometrics, credentials, policies, signals, agents, and legal entities. The future of identity will depend not only on whether those components can interoperate, but on whether the resulting decisions can be governed, audited, reversed, and trusted.

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. 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.

The Berlin Salon was held immediately before EIC and focused on four related topics:

- Identity Verification and Proofing in the Modern Enterprise
- Practical Implications of mDL, Wallets, and Verifiable Digital Credentials
- Biometrics
- eIDAS2 and Business Wallets

Although the agenda separated these topics into sessions, the conversation repeatedly crossed those boundaries. Participants moved from remote hiring to credential binding, from wallets to liability, from biometrics to wallet attestation, from passkeys to recovery, and from business wallets to agentic systems.

That movement was not a distraction. It was the point. Identity verification and proofing are no longer contained within a single workflow, product category, or regulatory domain. They now sit across enterprise risk, privacy, fraud, authentication, authorization, user experience, software supply chain, and business process automation.

From March to Berlin: The Shift in Focus

The March 2026 Salon framed identity verification and proofing as a broader architectural concern. It argued that proofing now sits at the intersection of wallets, credential formats, biometrics, liability, enterprise architecture, and agentic systems. It also highlighted several design instincts: aligning proofing with purpose, enabling reusable evidence where appropriate, strengthening trust models for credential ecosystems, and designing systems that can adapt as verification technologies change.

The Berlin conversation built directly on that work. If March identified the pressure points, Berlin explored what happens when organizations attempt to operate inside them.

The most important shift was from possibility to defensibility. In March, participants discussed the technical and architectural promise of reusable credentials, purpose-specific assertions, and stronger roots of trust. In Berlin, participants asked what happens when those capabilities meet audit, liability, process ownership, wallet capability questions, and recovery failures.

This is where the conversation became, at the same time, more difficult and more useful. It is relatively easy to say that reusable credentials could reduce repeated document capture. It is harder to explain how a relying party should decide which issuers to trust, how much to trust a wallet, what evidence to retain, whether a biometric check was sufficient, how to handle conflicting regulatory expectations, and how to recover when something breaks.

The Berlin discussion made clear that identity verification is moving from a point-in-time decision toward a continuing evidence problem. The goal is not simply to verify that

someone, something, or some organization is who they claim to be. Rather, it is to support decisions that can be explained later.

March to Berlin

March framed proofing as an architectural concern. Berlin reframed it as an evidence concern. The question is no longer only "what evidence establishes identity?" It is also "what evidence explains why this decision was reasonable at this time, under this policy, with these signals, in this transaction?"

[Subscribe to receive the full report]

Final Thoughts

The Berlin Salon showed that identity verification is moving from proofing to provability.

For many years, identity systems treated proofing as a gate. A person was verified, an account was created, a credential was issued, and the organization moved on. That model was never perfect, but it was understandable. It matched a world of relatively stable organizational boundaries, static attributes, and deterministic controls.

Today, identity decisions may depend on portable credentials, wallet-mediated presentations, device signals, biometric checks, live risk scores, policy engines, business registries, delegated authority, and agents. The person, organization, credential, wallet, and device may all sit in different trust domains. The relying party may not control the

evidence source, the wallet, or the capture process. Yet the relying party may still carry responsibility for the decision.

This changes the identity problem such that the central question is no longer only whether an identity claim can be verified. It is whether the full decision chain can be trusted, explained, challenged, recovered, and improved.

That requires more than credential standards. It requires evidence practices, assurance signals, process design, recovery models, liability clarity, and governance that can work across people, businesses, wallets, devices, and agents.

The Identity Salon does not exist to produce easy answers. Its value lies in identifying the hard problems early enough that the industry can avoid building around the wrong assumptions. Berlin made one thing clear: the next phase of identity work will be less about proving identity once and more about maintaining defensible trust over time.

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.

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