Deployability First: Making Age Verification Work at Internet Scale

A Position Paper for the 2025 Joint W3C/IAB Workshop on Age-Based Content Restrictions

Authors: Heather Flanagan and Leif Johansson, SIROS Foundation

---

Introduction

The urgency to develop reliable, privacy-respecting mechanisms for age verification has collided with the realities of standards development and deployment. Technical architectures are being proposed with insufficient regard for whether they can be deployed in real-world environments—across jurisdictions, across devices, and at scale. This paper focuses on the foundational architectural and protocol properties needed to make any age verification system viable, drawing on RFC 5218's[1] criteria for successful protocols and Kim Cameron's Laws of Identity[2].

We do not address every aspect of age verification. Instead, we concentrate on deployability, because without it, even the most elegant privacy technology will remain theoretical.

Why the Laws of Identity Still Matter

Kim Cameron's *Laws of Identity* provide a durable lens for evaluating any digital identity architecture. Several laws are especially relevant for age verification:

- **Law 1: User Control and Consent** – The user must remain in control of how and when identity information is disclosed.
- **Law 2: Minimal Disclosure for a Constrained Use** – Systems must share only the minimum required information (e.g., over/under 18), not full dates of birth.
- **Law 5: Pluralism of Operators and Technologies** – No single vendor or wallet should dominate the ecosystem.
- **Law 7: Consistent Experience Across Contexts** – Users should understand what is happening regardless of platform, device, or jurisdiction.

---

[1] Thaler, D. and B. Aboba, "What Makes for a Successful Protocol?", RFC 5218, DOI 10.17487/RFC5218, July 2008, <https://www.rfc-editor.org/info/rfc5218>.

[2] Cameron, Kim. "THE LAWS OF IDENTITY – Kim Cameron's Identity Weblog." January 8, 2006. https://www.identityblog.com/?p=352.

These laws do not conflict with regulation. They guide how to build respectful, scalable, and interoperable systems across borders and technologies.

Success Depends on Deployability

RFC 5218 outlines clear success factors for protocols, emphasizing that technical merit alone does not lead to widespread deployment. Among the most critical elements:

- **Positive Net Value**: Any age verification system must offer tangible value to implementers and end users. That value cannot be measured solely in compliance; it must also deliver minimal user friction and demonstrable privacy improvements.
- **Incremental Deployability**: Solutions must allow for gradual adoption. Protocols that require ecosystem-wide changes or simultaneous upgrades across all parties will fail.
- **Open Specification and Code Availability**: Vendors, governments, and developers need free access to implement and test solutions.
- **Extensibility and Longevity**: A system deployed today must have a shelf life of at least a decade. That includes preparing for the coming transition to quantum-safe cryptography.

Deploying any new age verification solution without meeting these criteria risks repeating the failure of previous efforts, such as Microsoft InfoCard, which was technically sound, well-funded, and completely undeployable at scale.

Identity Wallets Are Not a Silver Bullet

Digital identity wallets, such as the EU's forthcoming EUDI Wallet, offer promise—but also come with baggage. Wallet-based ecosystems are expensive to deploy and require complex integration with issuers and verifiers across jurisdictions. Despite these challenges, wallets will likely serve as the primary home for digital age claims in the near term.

However, a wallet-centric model must avoid platform lock-in and enable permissionless innovation in UX. The standards community must ensure that:

1. Wallet selection remains privacy-preserving.
2. New wallets can be introduced without centralized chokepoints.
3. Platform APIs—especially browser-based APIs like the W3C's Digital Credentials API[3]—support pluralism and interoperability.

Consider a French teen accessing a UK video game platform that requires age verification. The relying party knows UK law applies, the French regulator has issued trust marks for specific wallets, and the user's EUDI Wallet presents a ZKP-backed proof

[3] Caceres, M., Tim Cappalli, Mohamed Amir Yousef. "Digital Credentials." W3C Working Draft. July 27, 2025. https://www.w3.org/TR/digital-credentials/.

without revealing date of birth. The RP uses OpenID Federation to validate the credential, and the process is complete without exposing identifying data.

Relying parties must retain the ability to request age verification based on local requirements, while regulators must be able to verify compliance. This suggests the need for a three-party trust architecture: the RP knows what is required, the regulator knows what's valid, and the technical architecture provides the enforcement and proof mechanisms.

OpenID Federation[4] offers a model here, enabling federated trust mark validation without centralized control.

Zero-Knowledge Proofs: Potential vs. Practicality

ZKPs promise minimal disclosure and strong privacy guarantees, but today's schemes—particularly those based on pairing-friendly cryptography like BBS+ or BBS#—are not safe from quantum computer attacks. While efforts to deploy ZKPs on constrained hardware (e.g., secure elements, FIDO authenticators) are underway, they are not yet production-ready.

There is an unresolved tension: do we deploy ZKPs now and plan for a later migration, or wait until quantum-safe options become viable? Either way, the chosen architecture must:

- Support algorithm agility to accommodate future post-quantum primitives.
- Fit into existing device and browser infrastructures with minimal hardware replacement.
- Allow credential rotation and future migration paths without reissuance burdens.
- Be transparent to the user while maintaining privacy by default.

Post-quantum security mandates in jurisdictions like the US and EU that are mandating preparation by 2030–2035 mean any system launched today must anticipate replacement or upgrade strategies.

Common Platform APIs Are Essential

Rather than specifying a complete solution stack, the standards community should focus on a minimum viable architecture that includes:

1. **Credential selection and invocation API**: e.g., the DC API, provided it enables privacy-preserving wallet discovery.
2. **Cryptographic operations and key management API**: e.g., CTAP and WebAuthn, extended as necessary for ZKP-like operations.

[4] Hedberg, Roland, Michael B. Jones, Andreas Åkre Solberg, John Bradley, Giuseppe De Marco, and Vladimir Dzhuvinov. 2025. "OpenID Federation 1.0 - Draft 43." June 2, 2025. https://openid.net/specs/openid-federation-1_0.html.

3. **Credential issuance and presentation protocols**: e.g., OpenID for Verifiable Credentials, not DIDComm.

Why not DIDcomm? *Despite interest in DID-based systems—especially early on in the development of digital identity wallets—DIDcomm is not widely supported by browsers or platforms, lacks a mature trust framework, and would introduce unnecessary integration burdens on issuers and relying parties. OpenID protocols are already in use at scale across identity ecosystems and offer a far lower barrier to adoption.*

These APIs and protocols offer the best chance of deployable, privacy-respecting credential exchange across platforms. Crucially, they align with Law 5 (Pluralism) and Law 7 (Consistency*)* while preserving room for innovation.

Governance of UX: Who Gets to Decide?

User experience is often framed as an implementation detail, but it is a governance problem in practice. Law 7 demands that users understand what is happening regardless of device or platform, but today's UX patterns vary wildly.

To improve coherence:

- **Platform vendors** must commit to UX primitives (icons, prompts, metadata display)
- **Standards bodies** should define baseline interaction models for consent and credential presentation
- **Regulators** should refrain from mandating specific UX flows but support minimum expectations (e.g., transparency, fallback paths)

Wallet diversity is inevitable, and even desirable. But without shared UX baselines, we risk undermining usability and trust.

Aligning with Regulatory Drivers

Age verification mandates are emerging from regulation, not market demand. That reality creates a unique opportunity: by aligning the standards process with regulatory goals, we can build the foundational architecture for a broader digital credential ecosystem.

But the window is short. Once jurisdictions like the EU finalize their wallet infrastructure, the chance for global harmonization diminishes. If we act now by supporting interoperable APIs, extensible trust models, and deployable privacy tech, we can avoid the splintering of the ecosystem into incompatible national silos.

Conclusion

We propose a pragmatic lens through which to evaluate all age verification architectures:

- Can it be **deployed incrementally**?
- Does it **work on existing hardware and platforms**?
- Does it enable **regulatory compliance without centralization**?
- Will it **survive the post-quantum transition**?
- Does it align with **core identity principles**, such as those articulated by Kim Cameron?

By grounding our work in the lessons of RFC 5218 and the enduring principles of Kim Cameron's Laws of Identity, we have a chance not only to solve age verification but to do so in a way that strengthens the privacy and resilience of the Internet as a whole.