So Many Anonymous Credentials, So Little Adoption: Can We Escape the Linkability Doom in Digital Identity?

Andrea Moro[1]

[1]Center for Cybersecurity, Fondazione Bruno Kessler, Trento, Italy

Abstract

Despite decades of cryptographic maturity, Anonymous Credentials (ACs) remain on the periphery of mainstream, user-centric Digital Identity deployments. We argue that within the emerging European Digital Identity (EUDI) Wallet arena, the persistent non-adoption of ACs cannot be reduced to mere market obstruction or an institutional disregard for privacy. Rather, novel privacy-preserving paradigms collide with a deeply sedimented infrastructure of technological, economic, organizational, and institutional constraints that have crystallized into an inflexible sociotechnical *installed base*. Utilizing Fligstein and McAdam's Strategic Action Field (SAF) framework, we model the Digital Identity ecosystem as a contested space where historical design choices actively reject radical cryptographic shifts by imposing prohibitive adoption and coordination costs. We evaluate three contemporary deployment trajectories: Native AC Multi-Message Signatures, General-Purpose SNARK-Based Proofs, and Legacy-Compatible Protocols & Formats (e.g., SD-JWT, mdoc). Our analysis reveals why the ecosystem structurally defaults to linkable alignment formats as the path of least resistance. Finally, we chart an operational path forward, demonstrating how modular, post-quantum resilient zero-knowledge layers can be progressively introduced atop the existing installed base to resolve this adoption deadlock and realize the privacy-preserving promise of modern wallet ecosystems.

Keywords

Anonymous Credentials, Zero Knowledge Proofs, EUDI Wallet, Sociotechnical Analysis, Installed-base constraints

1. Introduction

From its inception, the field of Digital Identity has wrestled with a structural tension between security and privacy. Mainstream identity architectures defaulted to static containers of signed assertions and metadata issued by a trusted party to enforce authentication and authorization. While these bundled assertions streamlined parsing and verification logic, and simplified administrative auditability, the persistence of these stable identifiers enabled third parties to *link* subsequent presentations of the same assertions across contexts.

Recent architectural shifts, most notably the transition toward the Issuer-Holder-Verifier (IHV) model, attempt to mitigate some privacy concerns by centering transactions on a user-controlled digital wallet. In this model, the *Issuer* transmits signed *Verifiable Credentials* (VCs) to the *Holder*, who retains the autonomy to present them to a *Verifier*. While the IHV paradigm successfully decentralizes the storage and usage of credentials, it alone is not a solution for all privacy threats. Without the integration of robust privacy-preserving protocols at the issuance and/or presentation layers, the proliferation of VCs and digital wallets risks replicating the same *linkability doom*.

Problem. The cryptographic community has long offered many Anonymous Credential (AC) protocols [1, 2, 3, 4, 5, 6] that provide cryptographic privacy guarantees, including selective disclosure, untraceability, and blind issuance. Yet, despite decades of refinement, these AC protocols have struggled to achieve mainstream adoption and continue to lag behind simpler alternatives that perpetuate linkability. Even the European Union's flagship user-centric identity initiative—the European Digital Identity (EUDI) Wallet ecosystem—has shown limited intent to adopt these AC protocols, as its emerging

TDI 2026: 4th International Workshop on Trends in Digital Identity, April 20–21, 2026, Verona, Italy

anmoro@fbk.eu (A. Moro)

0000-0002-7088-912X (A. Moro)

© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

published 2026-09-06

CEUR-WS.org/Vol-4257/position2.pdf

Architecture Reference Framework (ARF) [7] defaults to selective-disclosure formats that fall short of true cryptographic unlinkability.

Thesis. This persistent adoption failure in an otherwise greenfield ecosystem cannot be adequately explained by scarce attention to privacy, or dominant player obstruction alone, as such an interpretation is overly reductive and overlooks the systemic complexity of the broader identity ecosystem. We state that Digital Identity infrastructures undergo structural *sedimentation*: legacy architectures harden into an *Installed Base* that constrains future adoption of new architectural designs. As a result, the adoption of a new AC scheme must take these constraints into account and leverage them as much as possible.

Method. We model Digital Identity as a *Strategic Action Field* (SAF) [8] and trace sedimentation dynamics that emerge from the Installed Base of the Digital Identity SAF to derive four constraint categories (Technological, Economic, Organizational, Institutional) which in turn affect new designs. We specialize this model to the EUDI Wallet arena and systematically derive the relevant Installed Base dependencies from the ARF and associated technical specifications. We then use these dependencies to derive the constraints that the adoption of AC schemes must face. In particular, we evaluate three possible AC deployment tracks against eight analytical lenses calibrated to these constraints. This yields a comparative alignment matrix (Table 1) where each track is assigned a qualitative score of its adoption friction to the lens and its underlying constraints. We stress that this analysis is a framework-driven assessment and not an empirical study: constraint derivation and lens scoring rest on the cited technical documentation and benchmark literature, not on stakeholder interviews or deployment telemetry. Therefore, the comparative matrix yields theoretically grounded judgments that remain amenable to refinement through future empirical validation such as pilot adoption data, interviews with EUDI actors, and observation of AC rollouts.

Paper Structure. Section 2 introduces the technical background and the AC Tracks (Legacy-Compatible Protocols & Formats, Native Multi-Message Signature Schemes, and General Purpose SNARK-Based Proofs) currently being discussed in the EUDI Wallet arena. Section 3 formalizes the SAF framework and its four sedimentation dynamics. Section 4 specializes these dynamics to the EUDI Wallet arena, deriving four constraint categories. Section 5 introduces eight analytical lenses and evaluates the three tracks against them, yielding a comparative alignment matrix (Table 1). Section 6 distills actionable recommendations, arguing that Track 3 (SNARK-based layering) offers the most viable near-term path when deployed on top of Track 1 protocols, particularly given post-quantum threats.

2. Background

2.1. Privacy Properties of Anonymous Credentials

The AC paradigm replaces the presentation of standard, cryptographically signed, credential with a non-interactive zero-knowledge presentation protocol, enabling the Holder to convey trusted assertions to the Verifier by generating mathematical *proofs* of the statements contained therein. This cryptographic abstraction yields four indispensable properties:

- **Selective Disclosure:** The Holder present a specific subset of attributes from an issued credential bundle while keeping all remaining attributes strictly hidden from the Verifier.
- **Unlinkability:** Two distinct presentations of the same credential to different Verifiers yield statistically independent proofs, preventing cross-context correlation by adversarial Verifiers.
- **Untraceability:** The Issuer remains unaware of the identity of the Holder presenting a credential, even when colluding with the Verifier.

- **Non-Transferability:** The credential is cryptographically bound to a Holder-controlled private key.[1].

2.2. Anonymous Credential Tracks

To facilitate our analysis, we categorize contemporary technical solutions [7, 9, 10] into three distinct deployment tracks based on the underlying cryptographic paradigms they employ.

- **Track 1: Legacy-Compatible Protocols & Formats** This track comprises protocols centered on the validation of conventional asymmetric signatures to verify credential integrity, authenticity, and Holder-binding key possession. These formats implement selective disclosure by unmasking specific attributes via salted hash disclosures. Technical variation within this track is driven by credential data modeling rather than presentation or verification logic, both of which directly inherit the standard patterns of the Installed Base. While these formats do not constitute true anonymous credential primitives, they represent the definitive operational baseline of the EUDI Wallet arena. As such, they serve as a benchmark against which native ACs and general-purpose SNARKs are measured. Representative specifications include Selective Disclosure for Verifiable Credentials (SD-JWT-VC) [11, 12] and ISO 18013-5 mobile Documents (mdocs/MSO) [13].
- **Track 2: Native Multi-Message Signature Schemes** This family comprises cryptographic signature schemes that sign a *tuple* of attributes (messages) simultaneously and support efficient zero-knowledge proofs of knowledge of a valid signature on those attributes. This native approach inherently satisfies selective disclosure, unlinkability, untraceability, and non-transferability. Representative primitives include RSA-based Camenisch-Lysianskaya (CL) signatures [14, 2], Pairing-based CL signatures [3], Pointcheval–Sanders (PS) signatures [5], and Boneh-Boyen-Shacham (BBS) signatures and their derivatives [15, 4, 16] as described in [10].
- **Track 3: General Purpose SNARK-Based Proofs** Rather than mandating a native, disclosure-friendly signature primitive, this track verifies *in zero knowledge* that a conventional credential—signed using standard algorithms such as ECDSA or RSA—satisfies a given verification policy. It achieves this by embedding the verification logic directly into a general-purpose proof system (e.g., zk-SNARKs). While this architecture allows ecosystems to reuse existing credential issuance infrastructures, it introduces significant computational complexity, circuit compilation overhead. When properly configured, these protocols fully satisfy selective disclosure, unlinkability, untraceability, and non-transferability. Representative protocols include *Longfellow* [17], *Crescent* [18], and *OpenAC* [19] as described in [9].

3. Sociotechnical Mechanisms of Lock-In

Candidate configurations are advanced, negotiated, and contested within the *Strategic Action Field* (SAF) of Digital Identity. Following the work of Fligstein and McAdam [8], this SAF is understood as a socially constructed order where *actors* endowed with unequal resources and power compete and cooperate within specific *arenas*. Within each arena, *arrangements* are proposed, evaluated, and contested—resulting either in their displacement, renegotiation, or stabilization into the ecosystem. When an arrangement is adopted, it becomes progressively embedded into the *Installed Base* through the process of *sedimentation*. Once sedimented, these configurations generate technological, economic, organizational, and institutional constraints that reconfigure the field, altering the barriers and switching costs for future arrangements. This Installed Base is not immutable; exogenous or endogenous disturbances within the SAF may occur. Usually, such shocks are contained through localized buffering mechanisms such as patching or layering, however, sometimes they escalate into a systemic rupture that forces renegotiation of the dependent arrangements.

To operationalize this sociotechnical framework, we define its four foundational components:

[1]The Holder must prove knowledge of this secret within the presentation protocol, ensuring that the entity presenting the proof is the legitimate and intended recipient of the underlying assertions.

- **Actors and Power Dynamics:** Actors represent the collective and individual participants within the SAF, including rule-makers, infrastructure providers, organizational adopters, and knowledge producers. They interact within specific arenas (e.g., the EUDI Wallet arena) to negotiate a concrete sociotechnical outcome (e.g., the EUDI Wallet Framework). Within these arenas, actors occupy distinct *relational positions* such as *solution proponents* or *solution adopters*. These positions are dynamic and allow actors to deploy different forms of power to shape outcomes; including *legitimacy power* (the authority to define compliance and normative acceptability), *platform power* (the capacity to shape arrangements through control over widely deployed application or hardware substrates), and *epistemic power* (the capacity to produce, standardize, and circulate knowledge objects, such as protocols and reference architectures).
- The **Installed Base** constitutes the material and logical foundation of the Digital Identity ecosystem, organized into three tightly coupled strata:
  - *Architecture:* The structural design logic of Digital Identity solutions, encompassing cryptographic primitives, network interaction patterns, data models, and protocol profiles.
  - *Application:* The operational layer through which architectures are implemented and reproduced, including SDKs, middleware, and integration APIs.
  - *Hardware:* The physical computing layer that conditions application deployment. This includes the processing and memory capacity of edge user devices, communication interfaces (e.g., NFC, BLE), and dedicated cryptographic chips such as device-side Secure Enclaves and server-side Hardware Security Modules (HSMs).

  These strata define the primary vectors through which historical sociotechnical choices crystallize and harden over time.
- An **Arrangement** is a stabilized bundle consisting of: (i) architectural and application artifacts (protocols, formats, and implementation patterns) constrained by hardware and platform limits, and (ii) governance and accountability frameworks (operational practices, standards, certification regimes, audit protocols, and liability allocations) that render the technical bundle legally and operationally possible. An arrangement successfully achieves *adoption* when it addresses a problem deemed highly consequential within the SAF, imposes low integration and governance friction, satisfies usability expectations for end-users, and aligns the economic and operational incentives of the actors responsible for its maintenance.
- **Sedimentation** describes the recursive process through which sociotechnical arrangements progressively harden into the Installed Base. This hardening occurs through four overlapping, recurrent institutional dynamics:
  - *Adoption and Embedding:* the initial adoption of an architecture, application, and hardware together with the progressive embedding into the Installed Base, builds path dependence [20, 21] that generates technological and economic constraints.
  - *Diffusion and Coordination:* the growing adoption and diffusion of the arrangement create dependencies that make change increasingly costly [22, 23, 24] and generate both technological and economic constraints.
  - *Codification and Legitimation:* the formal translation of the diffused arrangement into standards, regulatory regimes, and certification criteria, locking in the technical choice [25, 26] generating institutional constraints.
  - *Routinization and Maintenance:* practices, routines, skills, and maintenance work reproduce the arrangement; switching costs, exception handling, and operational inertia make change difficult even when alternatives exist [27, 28] imposing organizational and economic constraints.

  These dynamics generate an interlocking grid of technological, economic, organizational, and institutional constraints that dictate what can successfully be deployed within each Digital Identity SAF arena.

4. Constraints to AC Adoption

Specializing the framework developed in Section 3 to the EUDI Wallet arena gives us the test case to assess why and how AC proposals face such profound friction in this ecosystem. We identify four types of constraints—*technological*, *economic*, *organizational*, and *institutional*—through a dual method. First, we identify the relevant *Installed Base* dependencies *systematically* from the ARF [7] and cited technical specifications as the current arrangement within the EUDI Wallet SAF arena; we then *infer* the technological constraints at the architecture, application, and hardware strata directly from the derived Installed Base dependencies as a result of the *Adoption and Embedding* dynamic. Second, we *derive* the remaining three constraint categories via the remaining dynamics of Section 3 as the economic, organizational, and institutional constraints emerging from the identified *Installed Base* dependencies.

4.1. Technological Constraints

Technological constraints originate from adoption, embedding, and diffusion of previous arrangements in the SAF of Digital Identity. The relevant ones for the problem of AC adoption are *inferred* from the ARF [7] and related standards.

Deployment of any AC protocol is strictly bounded by the physical and computational limitations of edge devices which hosts Wallet applications. These must operate within tight CPU, memory, and latency envelopes, relying on fragmented, vendor-controlled hardware interfaces like TEEs and HSMs for secure key generation and storage, both for device keys (Section 4.3.2 [7]) and Issuer's keys (Requirements ISSU_67, ISSU_72 in ARF HLR [7]). Transport mechanisms (QR codes[29], NFC, or BLE [13]) and presentation verification requirements further align with lightweight, instantly verifiable, and deterministically resolvable presentation artifacts [11, 12, 13]. Moreover, credentials are required to be explicitly bound to device-stored keys (Section 6.6.3.10.2 [7]) and to support revocation (Section 4.6.6 [7]). The latter relies on highly available, low-latency infrastructures like status lists [30] or online status endpoints for revocation checks. Crucially, because the verification topology is predominantly stateless, the underlying data models have stable correlation markers such us the public key which binds the credential to the device (Section 5.1 [7]). These embedded identifiers fuel downstream auditing, fast identity resolution, and automated fraud-detection pipelines. Consequently, any novel privacy-enhancing architecture must not only conform to strict edge-computing and hardware constraints but must also navigate an Installed Base that inherently equates system security with linkable, static identifiers.

4.2. Economic Constraints

Economic constraints emerge from the Installed Base driven by asymmetric incentive structures, powerful network externalities, and the switching costs originated from path dependency. As the diffused arrangement grows, network externalities, sunk investments, and multi-actor coordination costs make architectural volatility prohibitively expensive. Deployed infrastructure represents massive sunk investments in software stacks, procurement contracts, and human capital, all optimized for the highly commoditized, linkable protocols of the Installed Base. Because adoption of IHV models depend on reaching a critical mass of Issuers, Holders, and Verifiers for which they become economically viable, actors face substantial coordination costs that structurally discourage architectural volatility. Furthermore, the economic returns of privacy-preserving paradigms are fundamentally misaligned: while the diffuse benefits directly favor users and society at large, the engineering, operational, auditing and certification costs are borne by ecosystem actors. This imbalance is reinforced by the conservative risk profiles of the public-sector institutions anchoring the EUDI framework, which inherently favor low-risk, incremental extensions of legacy architectures over cryptographic innovation.

Beyond upfront integration expenditures, the Digital Identity ecosystem relies on predictable mechanisms for risk externalization and liability transfer. Traditional linkable architectures provide clear administrative and evidentiary trails, allowing actors to trace fraud or non-compliance and legally

shift liability back to the offending entity. Transitioning to untraceable or anonymous alternatives could dismantle this operational net, forcing actors to absorb transaction failures directly or self-insure against fraud losses. The transition to IHV models alters backend hosting economics, relocating operational costs across the ecosystem. This shift burdens Issuers with issuance pipelines and credential management, forces Wallet Providers to manage complex multi-device lifecycle edge cases, and imposes interoperability and trust-management expenses on all ecosystem actors. In an environment defined by tight commercial sustainability thresholds for private actors and multi-actor governance coordination, any cryptographic track that exacerbates this cost relocation or compromises auditability face a high adoption penalty.

4.3. Organizational Constraints

Organizational constraints manifest from the dynamic of routinization and maintenance within the embedded technological Installed Base where routinized administrative playbooks, lifecycle workflows, and risk-mitigation habits resist architectural disruption. The operational viability of the EUDI Wallet Framework depends on the highly routinized, deterministic procedures governing the lifecycle of credentials, as well as the administrative and technical obligations imposed on participating entities (e.g., Issuers, Wallet Providers, Verifiers). Security and administrative teams rely on deeply institutionalized, repeatable processes for entities onboarding, key rotations, entity management, Holders recovery protocols, interoperability practices and credential re-issuance. Any technical arrangement that alters these consolidated compliance and maintenance routines introduces operational friction.

Furthermore, many security practices are calibrated for data-rich environments that rely on stable identifiers and persistent telemetry. Such practices serve modern workflows for fraud prevention, incident response, and threat hunting, making these dependent on such baseline data. Cryptographic paradigms that anonymize or abstract these signals threaten to dismantle the empirical foundation of existing security models. Until alternative, privacy-preserving monitoring procedures are codified into mature organizational habits, the steep transaction costs of retraining workforces and restructuring diagnostic capabilities will cause actors to reject paradigm shifts in favor of linkable, highly observable defaults.

4.4. Institutional Constraints

Institutional constraints arise from the powerful dynamics of codification and legitimation of the embedded Installed Base, where regulatory frameworks, certification regimes, and compliance baselines structurally stabilize the arrangements that get adopted. The EUDI Wallet arena is tightly bound by standardized certification shapes and discrete Level of Assurance (*LoA*) metrics that expect legible, traditional cryptographic evidence for conformity assessment bodies. This institutional landscape is further stressed by competing regulatory mandates: while data protection frameworks such as the GDPR advocate for minimization, anti-money laundering (AML) and Know Your Customer (KYC) directives strictly dictate persistent tracking, explicit identity verification, and mandatory data retention. Consequently, novel cryptographic arrangements face an additional *burden of proof* tax during procurement and regulatory reviews, as their departure from legacy designs obscures the mapping to eIDAS assurance levels and pre-existing compliance checklists.

Furthermore, institutional defensibility relies on a deeply sedimented accountability paradigm that, via organizational routines, equates systemic security with retrospective traceability and precise liability allocation. This reality presupposes a liability regime wherein the identity of a presenting Holder can be deterministically resolved post-presentation to settle disputes or conflicts between ecosystem actors. Technical paradigms that enforce unlinkability or diffuse administrative control disrupt these established accountability norms. By threatening the generation of standard audit evidence, true privacy-preserving alternatives are frequently delegitimized as legally unmanageable by auditors and regulators who default to highly observable architectures to preserve institutional legibility.

5. Adoption Tracks

The results of the constraint analysis in Section 4 make it evident that a solution's viability cannot be evaluated solely through the lens of privacy optimization. To gauge real-world deployment viability, our focus must shift to how much each track can align with surrounding technical, economic, organizational, and institutional constraints.

We therefore evaluate the three distinct deployment tracks—Legacy-Compatible Protocols & Formats, Native Multi-Message Signature Schemes, and General-Purpose SNARK-Based Proofs—against the constraints informing the EUDI Wallet arena. To distill this assessment into a comparative matrix, we define eight analytical lenses with the following criteria:

- Each lens is a refinement for at least one constraint type.
- Each constraint type gets at least one lens; where a constraint type has two distinguishable operational facets, it is split into two lenses for finer resolution (e.g., a technological constraint may relate more to the hardware fit and another to the architecture/application layer of the installed base; an economic constraint could be separated into sunk assets and ongoing costs).
- One lens (Privacy Guarantees) is retained as the normative baseline, deliberately outside the constraint typology, so that all tracks are scored against the reason-for-being of ACs, i.e., their privacy-preserving properties.

This set of lenses allows gauging[2] each track's adoption friction with respect to the constraints of Section 4. We propose the following lenses:

- **Privacy Guarantees:** The degree to which the track achieves the core privacy-preserving properties (selective disclosure, unlinkability, untraceability, and non-transferability) defined in Section 2.1.
- **Platform & Network Integrability:** The capacity of the track to operate within the strict boundaries of scarce edge-device resources (CPU, memory, latency) and legacy transport protocols as evidenced by the literature's currently available benchmarks.
- **Infrastructure Compatibility:** The ease with which a track interfaces with the architectural and application layers of the existing identity stack, where a higher score indicates lower implementation barriers.
- **Revocation Practicality:** The operational feasibility of executing low-latency, high-availability credential status checks without reintroducing tracking vectors.
- **Asset Preservation:** The extent to which the track protects, leverages, and builds upon already deployed infrastructures, operational routines, and existing organizational human capital, thereby mitigating the penalties of path dependency.
- **Cost Sustainability:** The long-term economic viability and manageability of the track's ongoing operational, hardware certification, and compliance expenses for all ecosystem participants.
- **Auditability:** The structural capacity of the data model to provide deterministic, transparent, and legally defensible audit trails for forensic verification and exception handling without violating baseline privacy guarantees.
- **Institutional Alignment:** The alignment of the track with regulatory frameworks, established compliance baselines, and accountability norms.

5.1. Track 1: Legacy-Compatible Protocols & Formats

This track represents the undisputed path of least resistance against the constraints of the sedimented Digital Identity infrastructure. Rather than transforming the underlying cryptographic paradigms,

[2]Each lens is assigned a qualitative score informed by the framework and, where possible, the cited literature. The scoring system adopts a five-level ordinal scale {*Low*, *Low-Medium*, *Medium*, *Medium-High*, *High*}, with intermediate *Low-Medium* and *Medium-High* levels accommodating intra-track protocol variation, based on how effectively the protocols within a track align with the specific operational facet it represents.

these protocols simply modify credential formats and add the corresponding presentation verification logic to accommodate non-transferability and selective disclosure. Despite the architectural privacy limitations—these protocols at best achieve unlinkability and thus earn a *Low-Medium* score for Privacy Guarantees—their absolute compatibility with the legacy Installed Base components and the advanced standardization process [11, 12, 13], have this track poised to be the default option in the initial rollouts of the EUDI Wallet Framework. As a result, this track achieves *High* alignment in Platform & Network Integrability, Infrastructure Compatibility, and Revocation Practicality, while securing a *Medium-High* rating for Asset Preservation, Costs Sustainability, Auditability and Institutional Alignment.

5.2. Track 2: Native Multi-Message Signature Schemes

These protocols face severe deployment friction due to their fundamental misalignment with the sedimented constraints of the Digital Identity Installed Base. This AC protocols cannot be deployed incrementally or localized to a single niche use case without mandating that all use case participants, including Issuers, Wallet Providers, and Verifiers, simultaneously implement the new primitive (*Low-Medium* Infrastructure Compatibility). Cryptographically, this track offers the highest privacy guarantees (selective disclosure, unlinkability, and untraceability) by combining their signature schemes with efficient ZK proofs (*High* level of Privacy Guarantees). Certain modern constructions, such as BBS and BBS+ signatures, exhibit highly competitive performance profiles that execute efficiently on resource-constrained edge devices[3] achieving *Medium-High* score on Platform & Network Integrability.

However, the institutional and economic barriers to adoption remain the highest within the current EUDI Wallet arena. Transitioning to the most efficient BBS [16] or BBS+ [4, 6] signature schemes requires a replacement of the credential models, HSMs components, as well as issuance and verification architectures embedded across the Installed Base layers (*Low-Medium* Asset Preservation). Economically, this track forces ecosystem actors to absorb integration costs—such as rewriting issuance and presentation validation logic—alongside the operational friction of cross-actor coordination during deployment (yielding a *Medium* score for Cost Sustainability). Track 2 achieves *Medium* Auditability depending on the specific use case and the structural configuration of the attributes disclosed to the Verifier, allowing organizations to maintain essential compliance trails without reverting to persistent identity tracking.

5.3. Track 3: General-Purpose SNARK-Based Proofs

These SNARK-based approaches occupy a middle ground. Unlike Track 2 protocols, SNARK-based protocols decouple the privacy-preserving presentation layer from the issuance protocol and infrastructure. By embedding legacy signature verification (such as ECDSA or RSA) and attribute verification logic directly into an arithmetic circuit, this track can be modularly layered on top of legacy deployments for targeted, high-privacy use cases without forcing a systemic overhaul of the central issuance infrastructure. (*Medium-High* Infrastructure Compatibility). Nevertheless, this architectural flexibility introduces significant technical complexity and operational risk. Like Track 2 protocols, SNARK-based constructions deliver robust mathematical unlinkability and untraceability (*High* level of Privacy Guarantees). The security properties of SNARKs are inherently harder to audit and certify due to the mathematical complexity of the circuit implementations earning a penalty to the Auditability score of Track 3 protocols. While governance frameworks would still require updates to accommodate proof verification pipelines, layering SNARKs over existing infrastructures lowers the operational costs for limited deployments yielding a bonus to Cost Sustainability with respect to Track 2 protocols. However, the severe computational burden of proof generation on mobile hardware remains a primary structural bottleneck, generating non-trivial latency that can compromise user experience.[4] (*Low-Medium* Platform & Network Integrability).

[3] Benchmarks for CL, PS and BBS presentations can be found at e.g., [31, 32].

[4] Presentation benchmarks for the various solutions can be found in the respective papers [33, 17, 18, 19].

For both Track 2 and Track 3, status verification can be achieved without breaking untraceability by deploying cryptographic accumulators [34, 35] or zero-knowledge proofs of membership [36] against a pre-compiled status list. To further reduce operational friction, deployment scenarios within these tracks often contemplate the use of short-lived credentials, which bypasses the overhead of managing revocation resulting in *Medium-High* Revocation Practicality. Established regulatory standards and compliance baselines lack recognized operational profiles for efficient native multi-message signature schemes or general purpose SNARKs, imposing a legislative and audit penalty on early adopters (*Low-Medium* Institutional Alignment).

Finally, within the EUDI Wallet arena, the economic sustainability of these tracks deviates significantly from the advertising-driven monetization models. Instead, the ecosystem operates on a public-utility framework funded primarily through member-state subsidies and commercial Verifier onboarding fees. Because this funding structure is not significantly affected by any track, privacy focused tracks do not get a penalty for Cost Sustainability.

To represent how effectively each deployment track navigates the constraints impacting the EUDI Wallet arena, Table 1 maps their respective scores against the eight analytical lenses introduced above.

Table 1
Comparative assessment of Tracks deployments against the eight analytical lenses of Section 5

Deployment Track	Privacy Guarantees	Platform & Network Integ.	Infr. Compatibility	Rev. Practicality	Asset Preservation	Costs Sustainability	Auditability	Inst. Alignment
Track 1								
Track 2								
Track 3								

Legend: Low Score, Low-Medium Score, Medium Score, Medium-High Score, High Score.

6. Conclusion and Recommendations

As evidenced in Section 5, the EUDI Wallet arena is heavily predisposed toward Track 1 (Legacy-Compatible Protocols & Formats 2.2). This path is dictated by the imperative to maintain alignment with existing middleware, standard cryptographic protocols, organizational and institutional requirements. The resulting trajectory appears to be one of perpetual *linkability*.

To escape this *doom*, we propose a strategic pivot: rather than pursuing an all-or-nothing replacement of the identity stack, proponents of privacy-preserving alternatives should leverage the modularity of Track 3 (General-Purpose SNARK-Based Proofs 2.2). Specifically, protocols such as Longfellow [17, 37, 38] offer the capability to *layer* advanced privacy-preserving features atop the foundational Track 1 infrastructure. This modular approach facilitates deployment in specific, high-privacy use cases (such as age verification) and limited pilots, allowing these to operate on top of Track 1 protocols serving as a robust, compliant fallback. Should these pilots prove successful, they could generate the positive network externalities and institutional legitimacy required to catalyze broader adoption.

Conversely, Track 2 (Native Multi-Message Signature Schemes 2.2) remains more difficult to deploy in fragmented environments due to the higher degree of network-wide coordination required for adoption.

Finally, the looming transition to Post-Quantum Cryptography (PQC) acts as a critical forcing function. Most classical Track 2 protocols are vulnerable to quantum adversaries; given that the timelines for PQC migration and AC adoption are increasingly convergent, the viability of these native schemes is further diminished. In contrast, many contemporary SNARK proof systems are designed to be post-quantum secure. Consequently, a SNARK-based trajectory requires only the migration of the underlying keys, signature components and arithmetic circuits embedding the verification logic offering a more resilient and future-proof path toward privacy-preserving Digital Identity.

Declaration on Generative AI

During the preparation of this work, the author used *Gemini 3.5 Flash* in order to check grammar, spelling and sentence structure for better clarity and fluency. After using these tool, the author reviewed and edited the content as needed and takes full responsibility for the publication's content.

References

[1] J. Camenisch, M. Stadler, Efficient group signature schemes for large groups, in: B. S. Kaliski (Ed.), Advances in Cryptology — CRYPTO '97, Springer Berlin Heidelberg, Berlin, Heidelberg, 1997, pp. 410–424. doi:10.1007/BFb0052252.

[2] J. Camenisch, E. Van Herreweghen, Design and implementation of the idemix anonymous credential system, in: Proceedings of the 9th ACM Conference on Computer and Communications Security, Association for Computing Machinery, Washington, DC USA, 2002, pp. 21–30. doi:10.1145/586110.586114.

[3] J. Camenisch, A. Lysyanskaya, Signature Schemes and Anonymous Credentials from Bilinear Maps, in: Annual international cryptology conference, Springer, Berlin, Heidelberg, 2004, pp. 56–72. doi:10.1007/978-3-540-28628-8_4.

[4] M. H. Au, W. Susilo, Y. Mu, Constant-Size Dynamic k-TAA, in: R. De Prisco, M. Yung (Eds.), Security and Cryptography for Networks, Springer Berlin Heidelberg, Berlin, Heidelberg, 2006, pp. 111–125. doi:10.1007/11832072_8.

[5] D. Pointcheval, O. Sanders, Short Randomizable Signatures, in: Cryptographers' Track at the RSA Conference, Springer, 2016, pp. 111–126. doi:10.1007/978-3-319-29485-8_7.

[6] J. Camenisch, M. Drijvers, A. Lehmann, Anonymous Attestation Using the Strong Diffie Hellman Assumption Revisited, in: International Conference on Trust and Trustworthy Computing, Springer Cham, Cham, Switzerland, 2016, pp. 1–20. doi:10.1007/978-3-319-45572-3_1.

[7] European Commission, Architecture and Reference Framework for the EU Digital Identity Wallet, 2026. URL: https://eudi.dev/3.0.0/.

[8] N. Fligstein, D. McAdam, Toward a General Theory of Strategic Action Fields, Sociological Theory 29 (2010) 1–26. doi:10.1111/j.1467-9558.2010.01385.x.

[9] European Commission, Specification for the implementation of Zero-Knowledge Proofs based on arithmetic circuits in the EUDI Wallet, Technical Specification TS13, European Commission, 2026. URL: https://github.com/eu-digital-identity-wallet/eudi-doc-standards-and-technical-specifications/blob/main/docs/technical-specifications/ts13-zksnarks.md.

[10] European Commission, Specification for the implementation of Zero-Knowledge Proofs based on multi-message signatures in the EUDI Wallet, Technical Specification TS14, European Commission, 2026. URL: https://github.com/eu-digital-identity-wallet/eudi-doc-standards-and-technical-specifications/blob/main/docs/technical-specifications/ts14-zkps-from-mms.md.

[11] O. Terbu, D. Fett, B. Campbell, SD-JWT-based Verifiable Credentials (SD-JWT VC), 2026. URL: https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/, work in Progress.

[12] D. Fett, K. Yasuda, B. Campbell, Selective Disclosure for JSON Web Tokens, RFC 9901, 2025. doi:10.17487/RFC9901.

[13] ISO/IEC, Personal identification – ISO-compliant driving licence – Part 5: Mobile driving licence (mDL) application, Standard ISO/IEC 18013-5:2021, International Organization for Standardization, 2021. URL: https://www.iso.org/standard/69084.html.

[14] J. Camenisch, A. Lysyanskaya, An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation, in: International conference on the theory and applications of cryptographic techniques, Springer, 2001, pp. 93–118. doi:10.1007/3-540-44987-6_7.

[15] D. Boneh, X. Boyen, H. Shacham, Short Group Signatures, in: Annual international cryp-

tology conference, Springer Berlin, Heidelberg, Heidelberg, 2004, pp. 41–55. doi:10.1007/978-3-540-28628-8_3.
[16] S. Tessaro, C. Zhu, Revisiting BBS Signatures, Cryptology ePrint Archive, Paper 2023/275, 2023. URL: https://eprint.iacr.org/2023/275.
[17] M. Frigo, A. Shelat, Anonymous credentials from ECDSA, Cryptology ePrint Archive, Paper 2024/2010, 2024. URL: https://eprint.iacr.org/2024/2010.
[18] C. Paquin, G.-V. Policharla, G. Zaverucha, Crescent: Stronger Privacy for Existing Credentials, Cryptology ePrint Archive, Paper 2024/2013, 2024. URL: https://eprint.iacr.org/2024/2013.
[19] L. Eagen, H. Ngo, V. Rushi, Y. Tong, M. Tsai, J. Xia, OpenAC: Open Design for Transparent and Lightweight Anonymous Credentials, Cryptology ePrint Archive, Paper 2026/251, 2026. URL: https://eprint.iacr.org/2026/251.
[20] W. B. Arthur, Competing Technologies, Increasing Returns, and Lock-In by Historical Events, The Economic Journal 99 (1989) 116–131. doi:10.2307/2234208.
[21] P. A. David, Clio and the Economics of QWERTY, American Economic Review 75 (1985) 332–337. URL: https://www.jstor.org/stable/1805621.
[22] M. L. Katz, C. Shapiro, Network Externalities, Competition, and Compatibility, American Economic Review 75 (1985) 424–440. URL: https://www.jstor.org/stable/1814809.
[23] E. Rogers, Diffusion of Innovations, 5th Edition, Free Press, 2003. URL: https://books.google.nl/books?id=9U1K5LjUOwEC.
[24] O. Hanseth, K. Lyytinen, Design Theory for Dynamic Complexity in Information Infrastructures: The Case of Building Internet, Journal of Information Technology 25 (2010) 1–19. doi:10.1057/jit.2009.19.
[25] P. J. DiMaggio, W. W. Powell, The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields, American Sociological Review 48 (1983) 147–160. doi:10.2307/2095101.
[26] G. C. Bowker, S. L. Star, Sorting Things Out: Classification and Its Consequences, MIT press, 2000. doi:10.7551/mitpress/6352.001.0001.
[27] S. G. W. Richard R. Nelson, An Evolutionary Theory of Economic Change, Belknap Press, Belknap Press of Harvard University Press, 1985.
[28] O. Williamson, The Economic Institutions of Capitalism: Firms, Markets, Relational Contracting, Free Press, 1985.
[29] O. Terbu, T. Lodderstedt, K. Yasuda, D. Fett, J. Heenan, OpenID for Verifiable Presentations 1.0, 2025. URL: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html.
[30] T. Looker, P. Bastian, C. Bormann, Token Status List (TSL), 2026. URL: https://datatracker.ietf.org/doc/draft-ietf-oauth-status-list/18/, work in Progress.
[31] F. Veseli, J. Serna, Evaluation of Privacy-ABC Technologies - a Study on the Computational Efficiency, in: S. M. Habib, J. Vassileva, S. Mauw, M. Mühlhäuser (Eds.), Trust Management X, Springer International Publishing, Cham, 2016, pp. 63–78. doi:10.1007/978-3-319-41354-9_5.
[32] A. Flamini, G. Sciarretta, M. Scuro, A. Sharif, A. Tomasi, S. Ranise, On cryptographic mechanisms for the selective disclosure of verifiable credentials, Journal of Information Security and Applications 83 (2024). doi:10.1016/j.jisa.2024.103789.
[33] M. Rosenberg, J. L. White, C. Garman, Ian, Miers, zk-creds: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure, 2023 IEEE Symposium on Security and Privacy (SP) (2023) 790–808. doi:10.1109/SP46215.2023.10179430.
[34] G. Vitto, A. Biryukov, Dynamic Universal Accumulator with Batch Update over Bilinear Groups, in: S. D. Galbraith (Ed.), CT-RSA, volume 13161 of *Lecture Notes in Computer Science*, Springer, 2022, pp. 395–426. doi:10.1007/978-3-030-95312-6_17.
[35] J. Camenisch, A. Lysyanskaya, Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials, in: M. Yung (Ed.), CRYPTO 2002, volume 2442 of *Lecture Notes in Computer Science*, Springer, 2002, pp. 61–76. doi:10.1007/3-540-45708-9_5.
[36] K. Emura, A. Miyaji, K. Omote, A Revocable Group Signature Scheme with the Property of Hiding the Number of Revoked Users, in: H. Kim (Ed.), Information Security and Cryptology

- ICISC 2011, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012, pp. 186–203. doi:10.1007/978-3-642-31912-9_13.
[37] Google LLC, longfellow-zk, 2025. URL: https://github.com/google/longfellow-zk.
[38] M. Frigo, A. Shelat, Longfellow ZK, 2025. URL: https://datatracker.ietf.org/doc/draft-google-cfrg-libzk/.