Com(m)itology* in the Making: Regulating Through Technical Architecture in the European Digital Identity Wallet

Evelyne Putz[1,2] and Nicholas Stifter[3]

[1] University of Graz, Austria
[2] University of Vienna, Austria
[3] SBA Research, Austria

Abstract. The European Digital Identity Framework requires Member States to provide at least one European Digital Identity Wallet by late 2026. Its privacy commitments depend not only on legislation, but also on implementing acts, standards, certification, the Architecture and Reference Framework, technical specifications, and software. Hereby, the European Commission is pursuing a more agile implementation approach in which legal and technical work, expert feedback, and iterative development inform one another. In this paper we ask what benefits and vulnerabilities arise when this approach interacts with formal EU implementation, and which safeguards are needed to keep privacy-significant choices transparent, contestable, reviewable, and accountable. We combine doctrinal legal analysis with source-critical documentary analysis, using comitology as a functional benchmark. Through two complementary focal examples, unlinkability and relying-party over-requesting, we examine how privacy requirements are translated into technical architecture and distributed controls. We argue that while the agile approach can improve expert scrutiny, preserve alternatives, and support revision, its public evidence does not automatically establish a fundamental accountability advantage over conventional implementation as public visibility alone does not secure authority. Proportionate safeguards should therefore strengthen traceability, reason-giving, decision responsibility, participation, review, and correction.

Keywords: European Digital Identity Wallet · eIDAS · privacy by design · unlinkability · comitology · regulatory accountability

1 Introduction

In June 2024, following two expert calls convened by the European Commission, sixteen cryptographers published a position paper, referred to below as the *Cryptographers' Feedback*. They attached it to a public issue in the Git-based repository used to develop the Architecture and Reference Framework (ARF), the formally informative architectural reference for the European Digital Identity Wallet (EUDIW) that every EU Member State must provide from late 2026.

* In EU law, *comitology* refers to the committee procedures through which Member States oversee the Commission's exercise of implementing powers.

The paper's authors argued that mechanisms described in the then-current ARF v1.4.0 leave presentations correlatable, and concluded that it therefore could not ensure the unlinkability legally required; they urged consideration of anonymous-credential approaches instead [5,18].

Access to public administration, financial services, education, mobility, online platforms, and age-restricted services increasingly depends on establishing an identity or proving an attribute digitally. The Union's response is the European Digital Identity Framework (EUDIF), established by Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183. The Regulation obliges each Member State to provide at least one EUDIW by late 2026. Because common formats, trust relationships, interfaces, and conformity requirements are being embedded in implementations, later change may require coordinated migration. The Cryptographers' Feedback thus addresses mechanisms used in gateway infrastructure.

The amended eIDAS Regulation makes substantive privacy commitments, including user control and selective disclosure. It places specific limits on post-issuance tracking, linking, and correlation. Furthermore, it requires wallet-relying parties to register specified information concerning intended use and requested data. These are legally binding requirements, but they do not specify a complete technical system or by themselves secure an end-to-end privacy property. Whether they are attained depends on decisions taken downstream, including credential formats, presentation protocols, identifiers, status and revocation mechanisms, relying-party authentication and registration.

The EUDIF addresses that translation task through a layered implementation ecosystem. The amended eIDAS Regulation empowers the Commission to adopt implementing regulations. Standards and certification schemes acquire force where those implementing regulations refer to them or where conformity assessment relies on them. Alongside them, the EUDIW Toolbox process initiated under Commission Recommendation (EU) 2021/946 develops the ARF, common standards and technical specifications, and guidelines and best practices. These instruments differ in legal status, authorship, procedure, and reviewability, but interact in implementing the same infrastructure - an approach the Commission presents as deliberately agile [19].

This paper asks: *what procedural benefits and risks arise when legally significant privacy requirements for digital identity infrastructure are translated through fast, iterative, expert-driven and partly software-development-oriented legal-technical processes, and what safeguards are required to keep those processes transparent, contestable, reviewable and accountable?* We ask how that operationalisation is itself governed. The comparison also permits a bounded institutional assessment of whether the claimed agility makes regulation and technical innovation mutually enabling or reproduces familiar implementation trade-offs in a new form.

Methodologically, the paper combines four bounded forms of analysis. First, doctrinal legal analysis of implementing processes and powers, and the formal status of relevant instruments. Secondly, a versioned and source-critical doc-

umentary reconstruction follows selected ARF versions, public issues and discussions, expert submissions, pull requests, tag, release, and discussion-paper records. Thirdly, an exploratory analysis informed by repository-mining research examines the public ARF Git history and GitHub issue and pull-request event record, frozen at public `main` commit `6373eee...` on 23 July 2026 [25,7,27].

Fourthly, structured functional and normative institutional comparison applies common procedural questions to the two complementary focal examples and derives safeguards from identified deficiencies. Examples examined in separate sections expose different mechanisms of legal-technical translation. The Cryptographers' Feedback on unlinkability provides a versioned public record of a contested architectural choice and proposed alternatives. Relying-party over-requesting instead shows legal responsibility, practical prevention, evidence, and review distributed across registration, certificates, wallet controls, and enforcement. They are analytically complementary rather than representative.

The general public technical corpus is frozen at 24 July 2026, with a final critical update check on 30 July 2026; ARF v3.0.0 provides the baseline for general propositions, while earlier and superseded versions are retained where a claim depends on them [16]. Unresolved public material is recorded as such, and inaccessible/non-public material falls outside the corpus, which necessarily sets limitations. Public repository traces show observable platform activity, not the full distribution of authority, influence, or institutional reasons. They do not capture Cooperation Group meetings, private correspondence, standards-body discussions, or internal Commission deliberation. A recorded merge may implement a decision reached elsewhere, and chronological succession does not establish causal influence. The paper accordingly claims neither a comprehensive reconstruction nor findings of capture, unlawfulness, technical failure, and it does not evaluate deployed Wallet systems.

Section 2 distinguishes legal privacy commitments from technical properties and sets out the procedural questions used throughout. Section 3 locates comitology within the EUDIWs' formal implementation and distils its limits as a public-law benchmark. Section 4 maps the EUDIW implementation ecosystem and its public repository layer. Sections 5 and 6 examine unlinkability and relying-party over-requesting as complementary focal examples. Section 7 synthesises the findings, derives safeguards, and concludes.

2 Regulation Through Technical Architecture

Technical architecture is not law, but it structures the actions that a system makes possible, costly, or visible. Reidenberg's *lex informatica* and Lessig's account of code as a regulatory modality explain why protocols, data structures, and interfaces can shape conduct alongside legal and organisational constraints [31,28]. In a digital identity system, architectural choices affect which party can request or learn an attribute, what evidence is produced, whether transactions can be correlated, and what a user or supervisory authority can later reconstruct.

Such choices do not displace the amended eIDAS Regulation's requirements; they are where the content of those requirements is operationalised in practice.

Law-by-design-obligations scholarship provides the closest conceptual neighbour to our analysis. It identifies a category of obligations that operate across the development lifecycle, pursue legal goals through design, and deliberately leave implementers discretion [14]. Djeffal accordingly concludes that the legitimacy of such obligations cannot be assessed in the abstract, but only within specific implementation contexts [14]. This paper examines one such context by shifting attention from the design obligation itself to the wider process in which legislation, standards, technical specifications, and other artefacts translate that obligation into practical system requirements. Recent EUDI scholarship addresses adjacent aspects. Weigl and Reysner analyse the institutional governance of the EUDIF; Podda et al. examine how zero-knowledge techniques may support data-minimisation compliance; and technical work evaluates privacy risks in particular ARF versions and the properties and constraints of anonymous-credential families [32,30,1,8]. These contributions address institutional arrangements and technical properties while we address the process that connects them.

Translation from legal commitment to technical property is neither one-to-one nor confined to a single component. In the context of the EUDIW, selective disclosure is a technical capability to disclose selected attributes or parts of a credential. Regulation (EU) 2024/1183 makes selective disclosure an operative Wallet capability and, in recitals, links that capability to data minimisation objectives. Selective disclosure may reduce the data revealed in a presentation, but it neither establishes that the relying party's request is necessary nor prevents correlation across presentations. Privacy properties are also compositional: a property holding at one layer may be undone by identifiers, status mechanisms or metadata at another; legal sufficiency therefore attaches to the composition rather than to any single artefact. Two mechanisms carry this translation, and both raise the same question. Standards and conformity processes operationalise legal requirements while concentrating technical interpretation and participation in specialist forums and making participation resource-intensive [24]. Public issues, proposed text, reviews, and version histories can improve documentary visibility, but an open contribution channel does not by itself establish representative participation, equal capacity to contribute, or public decision authority [29,27].

The analysis therefore uses a common set of procedural questions synthesised from public-law accountability, comitology, standards governance, and documentary process scholarship. They concern authority and mandate; access to information; participation and representation; reason-giving and treatment of objections; documentary traceability; responsibility and correction; review and revisability [9,10,24,29]. For this analysis, visibility supplies information; accountability additionally requires an identifiable actor to explain a choice before a forum able to assess that explanation and, where appropriate, require correction. Sections 5 and 6 apply these questions where the public record supports a conclusion and identify the remaining gaps as such.

3 Comitology as a Public-Law Benchmark

The Treaty on the Functioning of the European Union (TFEU) is one of the two Treaties on which the EU is founded. It sets out the Union's competences and how its institutions exercise them, including the division between making law and implementing it. The European Parliament and the Council adopt legislative acts such as the eIDAS Regulation. Where uniform conditions for implementing such an act are needed throughout the Union, the act confers implementing powers on the Commission, defining the Commission's mandate and selecting the procedure. The procedures through which Member States control the Commission's exercise of those powers are customarily called *comitology*. The general rules governing these procedures are laid down in Regulation (EU) No 182/2011, which specifies how committees are composed, which of two procedures (advisory or examination) applies, and the effect of committee opinions.

Comitology is the ordinary route for implementing acts, and a high-volume one. In 2024, 368 committees delivered 2,129 opinions, leading to the adoption of 1,938 implementing acts [21]. It is also a central part of the EUDIF. Article 48 of the eIDAS Regulation establishes a committee and makes the examination procedure applicable. The implementing regulations that give the EUDIF its binding technical content are adopted by this route. The Commission prepares the draft and a committee of Member State representatives, chaired by a non-voting Commission representative, examines it. The Commission then adopts the implementing regulation. A positive opinion by qualified majority obliges the Commission to adopt. A negative opinion bars adoption in that form, but does not end the procedure: the Commission may submit an amended draft to the same committee or refer the draft to an appeal committee. Where no opinion is delivered, the Commission may as a rule adopt, except in listed subject areas that do not include digital identity, where the basic act itself excludes such adoption, or where a majority of the committee's members opposes the draft. The procedure also identifies participants and structures deliberation. Each committee must adopt its own rules of procedure, on the basis of standard rules drawn up by the Commission; the eIDAS Committee's rules follow that model [20,17].

Draft acts and agendas are circulated in advance, any member may propose amendments, and before the vote the chair must try to find solutions commanding the widest possible support and tell the committee how largely supported suggestions were treated. That explanation is owed to the committee, not to the public. Where no member objects, the chair may establish a positive opinion by consensus without proceeding to a formal vote. Opinions may also be obtained by written procedure, which is the a frequent route: in 2024 committees carried out 1,211 written procedures [21]. There, under Regulation (EU) No 182/2011 a member who neither opposes the draft nor explicitly abstains before the deadline is treated as having tacitly agreed. Delegations may bring experts with the chair's permission, but each Member State counts as one member and a delegation's composition does not affect the vote. Other experts and third parties may be invited to speak at the chair's discretion, subject to opposition by a simple majority of members, and are excluded from the vote [20,17].

Comitology further supplies a documentary structure. Pursuant to Regulation (EU) No 182/2011, the Commission must keep a register of committee proceedings covering agendas, summary records, draft and final draft implementing acts, voting results and information on adoption, and must publish an annual report. The Regulation requires only that the references be made public, together with statistical data on the committees' work. The Parliament and the Council receive agendas and draft acts at the same time as committee members, and either institution may indicate to the Commission that a draft implementing act exceeds the implementing powers conferred by the basic act. The Commission must then review the draft and inform both institutions whether it intends to maintain, amend or withdraw it. The right carries no power of veto: the Commission may state that it intends to maintain the draft, and adopt it.

The record itself is layered rather than open. Members have the right to have their position recorded in the minutes, whereas the public summary record describes each agenda item and the voting result and must not mention individual members' positions in the discussion. Committee discussions are confidential, and documents submitted to members, experts and third parties remain confidential unless released; access requests are handled under Regulation (EC) No 1049/2001, subject to its exceptions, including the one protecting an institution's decision-making process. The register therefore establishes that a decision was taken, by which body and on which text, more reliably than why it was taken, or whether it was voted on at all.

Public visibility does not depend on the register alone. Under a *Better Regulation* commitment, the Commission undertook that important implementing acts should be made public for four weeks, allowing stakeholders to comment before any vote in the committee, but nothing obliges the Commission to record what it received or how it was treated.[4] Across comitology the practice is selective: 108 drafts were published for feedback in the same year in which 1,938 implementing acts were adopted [21]. In the EUDIF it has been applied consistently.

Comitology is an imperfect benchmark. Scholarship has criticised its limited public visibility, the Parliament's restricted position compared with legislation, official and specialist dominance, and the risk that technical framing obscures distributive or rights-relevant choices [9,10,6,11,13]. Others have read comitology as a setting for deliberative problem-solving rather than only intergovernmental bargaining [26,13,6]. A study of 2005 practice found summary records missing for roughly a third of meetings and of poor quality for most committees that published them [10]; because it predates later changes to the register, it cannot establish the quality of the present record.

What we take from comitology is its formal structure, and that structure holds on either account: an identified adopting institution, a defined membership, and a mandate traceable to a basic act. The resulting act must state the reasons on which it is based and is published in the *Official Journal*.

We use comitology functionally, as a realistic reference point rather than an idealised alternative, and not as a proposal to run every technical revision

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015DC0215

through a committee. Binding implementing regulations in the European Digital Identity Framework coexist with the ARF and related versioned technical materials. Section 4 examines how those materials can exercise practical influence while lacking the formal mandate, adopting institution, or reviewability of an implementing act.

4 The European Digital Identity Framework as a Legal-Technical Implementation Ecosystem

The formal route described in Section 3 is one component of a wider implementation ecosystem. That ecosystem governs a distributed system: a wallet user holds a wallet unit from a wallet provider; providers of person identification data and of electronic attestations of attributes issue data; wallet-relying parties request presentations; and registration, trust, certification and supervisory functions support those transactions. The amended eIDAS Regulation confers implementing powers on the Commission, and the principal wallet implementing regulations adopted under them cover issuance, wallet integrity and core functionality, protocols and interfaces, certification, relying-party registration and attestations of attributes. Their technical content, however, is largely developed outside the committee procedure.

This is by design, and the vehicle is the common Union Toolbox. Commission Recommendation (EU) 2021/946 recommended that Member States cooperate to produce three deliverables: a technical architecture and reference framework, common standards and technical specifications, and common guidelines and best practices; it assigned implementation to the eIDAS expert group. That role is now performed by the European Digital Identity Cooperation Group, which Article 46e of the amended eIDAS Regulation establishes as a Commission-chaired body of representatives appointed by the Member States, with relevant stakeholders invitable as observers on an ad hoc basis. Its tasks include advising the Commission in the early preparation of draft implementing and delegated acts. The Cooperation Group is not the eIDAS Committee. Both bodies are composed of Member State representatives and chaired by the Commission, but the Group advises and coordinates, whereas the Committee delivers the formal opinion preceding adoption, and only the latter is recorded in the comitology register. Toolbox work is not a source of binding law and becomes binding only so far as it is incorporated into an act adopted under the Regulation's powers. Standards, certification, and supervisory processes form part of the wider implementation ecosystem but are not independently reconstructed here; they enter the analysis only where the focal materials or binding acts expressly rely on them.

Within the Toolbox, the ARF occupies a distinctive position, and the binding acts establish this themselves. In their recitals, implementing regulations state that their technical specifications rely on the work carried out under the Recommendation and in particular the ARF, and that the Commission should review and update them to stay in line with it. In their operative provisions, the subject-matter article of the principal EUDIW implementing regulations, e.g.,

Commission Implementing Regulation (EU) 2024/2979, states that the rules it lays down are "to be updated on a regular basis to keep in line with technology and standards developments and with the work carried out on the basis of Recommendation (EU) 2021/946, and in particular the Architecture and Reference Framework". Alignment with a document maintained outside the legislative process is therefore part of these acts' own enacting terms. In practice, that commitment has been acted upon: Commission Implementing Regulations (EU) 2026/1730, 2026/1731 and 2026/1735, adopted on 15 July 2026, give as their reason that "the architecture and reference framework has evolved significantly". Binding law has been revised because, on the amending acts' own stated reasons, a document maintained in a public repository changed.

The ARF is nevertheless published and maintained not in the *Official Journal* but in a public specification repository, through versioned releases, issues, discussions and pull requests. Hereby, it has moved quickly: between the Cryptographers' Feedback of June 2024 and the corpus freeze, the ARF advanced by 24 releases from version v1.4.0 to v3.0.0. Propositions about the ARF therefore require that the version is named, and the binding acts name none: the alignment obligation in their subject-matter articles attaches to the ARF as such. The ARF v3.0.0 release was published on GitHub on 23 July.[5] Its changelog states that it aligns the ARF with the amending acts, incorporates the Topic X relying-party-registration refinement, and introduces a Functional Conformance Assessment Framework [16]. This documents alignment across artefacts, not the direction of influence or incorporation of every ARF requirement into binding law. Version 3.0.0 contains the architecture's narrative and high-level requirements, links to technical specifications and to discussion topics identified by letter (e.g., Topic A, Topic X). It guides the reference implementation, and describes itself as informative, not replacing the eIDAS Regulation or its binding implementing and delegated acts [16]. The release workflow published on 21 June 2026, examined at public `main` commit `6373eee1` of 23 July 2026, describes the ARF as informative guidance supporting binding implementing regulations and provides that content changes require a Cooperation Group opinion and Commission approval. That approval concerns production of the informative ARF; it is not adoption of an implementing act. The release flow distinguishes public issues and pull requests from Member-State feedback channelled through the Cooperation Group. Both streams are consolidated across two synchronised repositories before the completed release is published to the public repository. However, the public repository does not expose the underlying Member-State feedback or the separate record of its integration and the workflow description contains references to `*-private` repositories and a public mirror, indicating non-public workflows [15].

Formal status and practical influence do not track each other: the ARF and related specifications can constrain what is implementable or make particular options easier to adopt. The public repository records proposals and changes, which is a form of visibility but does not confer decision authority.

[5] The Git tag is however actually dated 21 July.

A bounded analysis of the frozen (public-facing) repository sharpens that last point by distinguishing contribution from integration. The corpus contains 406 accepted non-merge content commits by 28 direct authors, of whom the four most active account for 75.9%. It records 334 pull requests with 42 authors, 30 formal reviewers and 33 accounts exercising triage-associated events. Seven recorded `User` accounts merged 289 pull requests into `main`; one accounts for 77.9% and three for 94.5%. The visible contribution route was therefore broader than the public integration layer, while integration activity was concentrated. These counts do not identify a complete maintainer roster, effective representation, intellectual influence, or institutional decision authority [25,7,27].

For the issues examined here the repository preserves a public record of technical proposals, reviews and version changes, but it does not reproduce Cooperation Group deliberation, Member State feedback, standards-body discussion, internal Commission reasoning, or approval reasons. A recorded merge may implement a decision taken collectively or elsewhere. The ecosystem thus exercises practical influence across artefacts that share no single legal status, decision-maker or review channel. Sections 5 and 6 test how far the combined legal and public records make that influence contestable.

5 Unlinkability and the Cryptographers' Feedback

Article 5a(16)(a) of the amended eIDAS Regulation requires the Wallet's technical framework not to enable providers of electronic attestations of attributes or other parties, after issuance, to obtain data permitting transactions or user behaviour to be tracked, linked, or correlated, unless explicitly authorised by the user. Article 5a(16)(b) separately requires the technical framework to enable privacy-preserving techniques ensuring unlinkability where an attestation does not require identification. Unlinkability, from a technical perspective, is not a context-free property. Instead, one must take assumptions about observer(s) and observations into consideration. Repeated presentations to one wallet-relying party, presentations to colluding relying parties, correlation of issuance and presentation by an attestation provider and relying party, and observation of system metadata are all distinct threat models [5,8]. A protocol property that can be guaranteed under one model does not automatically extend to the entire implementation or end-to-end system.

The episode surrounding the Cryptographers' Feedback began as an internally initiated expert consultation. The European Commission's EUDIW Team invited cryptographers to calls on 5 and 6 June 2024, presented ARF v1.4.0, and requested feedback on attestations and zero-knowledge proofs. As a response, participants from the call and other experts published a position paper [5] on 19 June in the public ARF repository under GitHub Issue #200, subsequently converted into Discussion #211. The paper argues that under same- and colluding-relying-party models and issuer–relying-party collusion the considered salted-hash design can not be repaired through minor modifications. It instead recommends a larger redesign that leverages the properties of anonymous credentials,

which would require the adoption of compatible digital signature schemes such as BBS/BBS+. A BBS-derived proof can disclose selected signed messages through a fresh proof that is unlinkable at the proof layer to the issuer's base signature and to other derived proofs [33,8]. The paper further calls for the EUDIW to be designed to follow principles of crypto-agility, i.e., facilitating that its underlying technologies can be changed or upgraded quickly if the need arises. This was an expert assessment of the analysed design, not an institutional finding of unlawfulness or insecurity under every threat model.

Paolo De Rosa, the issue assignee and a Commission policy officer publicly identified as the EUDIW technical lead, provided the clearest implementation-side response in the public thread [12]. He acknowledged the privacy potential but argued that an EUDI solution also had to satisfy requirements associated with Assurance Level High, including robust holder and device binding and tamper and duplication resistance, while also addressing revocation and deployment on market-available secure elements or hardware security modules. He questioned support for the necessary cryptographic primitives in existing secure hardware and stated that revocation, although possible, did not appear fully resolved in the proposed approach. These concerns connected the cryptographic choice to interoperability, maturity, cost, and the statutory timetable. He nevertheless proposed collaboration on a zero-knowledge solution supporting holder binding and revocation on available hardware [12].

The response therefore qualifies the Cryptographers' Feedback's claim that a BBS-based standard and reference implementation could be developed with modest effort and does not establish that anonymous credentials are unsuitable. His project role makes the comment institutionally informative, but not a formal Commission or Cooperation Group disposition. Replies in the discussion disputed whether the constraints were decisive and proposed technical variants; the public thread records no institutional outcome of the proposed follow-up meeting. Subsequent research offers device-bound constructions compatible with BBS while confirming that trusted-hardware integration is non-trivial [22] and the W3C BBS cryptosuite was still a Candidate Recommendation Draft in April 2026 [33].

Later materials show continued treatment of related concerns without establishing causal influence. Topic A distinguishes relying-party from attestation-provider linkability, discusses batch issuance, and states that a salted-hash approach cannot technically prevent a provider retaining issuance data from recognising a returned credential. Topic G distinguishes selective disclosure, relying-party unlinkability, and fuller unlinkability, and addresses non-revocation, device binding, issuer trust, pseudonyms, performance, and standardisation [2,3]. Commission Implementing Regulations 2026/1731 and 2026/1735 address particular status, attestation, and revocation channels, including requirements intended to hinder linkability or traceability. They do not adopt anonymous credentials or demonstrate end-to-end unlinkability. A peer-reviewed evaluation identifying linkability, identifiability, and excessive-disclosure concerns analysed ARF v1.5.0, not the later v3.0.0 [1].

Procedurally, the episode establishes visibility and contestability more clearly than accountable correction. The Commission-side invitation enabled early specialist scrutiny; publication of the response and ensuing exchange exposed both a technically specific objection and countervailing assurance and deployment concerns. The repository preserved contributors' competing technical arguments and later versioned treatment in unusual detail. Effective participation nevertheless required specialised expertise and, initially, access to an invited consultation. More importantly, the thread records contributors' positions, including an implementation-side counterargument, but no institutional disposition identifying who accepted, rejected, or deferred each material proposition, why, and in which effective version. The workflow published in 2026 identifies Cooperation Group opinion and Commission approval for current ARF content, but does not retrospectively reconstruct the 2024 episode [15]. The sequence is consistent with revisability; it does not show that the feedback caused later requirements or that the objections were fully resolved. The evidential gap concerns the chain from legal mandate through expert objection and counterargument to an identifiable institutional decision and review, not proof that the feedback was ignored or that the architecture is unlawful or technically defective.

6 Over-Requesting: Beyond the Registered Scope

Relying-party over-requesting concerns whether a wallet-relying party requests attributes that are unnecessary for its specified purpose. Article 5(1)(b) and (c) GDPR requires purpose limitation and data minimisation, while Article 5b of the amended eIDAS Regulation requires relying parties to register their intended use and requested data and prohibits requests outside that declaration.

The July 2026 implementing measures establish a three-level control structure. Implementing Regulation (EU) 2025/848 initially left registration certificates optional. Regulation 2026/1730, entering into force on 11 August, amends that regime to require each Member State to authorise at least one registration-certificate authority. The parallel Regulation 2026/1731, also entering into force on 11 August, adds WRP-VALIDATION-01 to -03 in clause 4.4 of the amended annex. They require the EUDIW to validate the relying party's registration certificate before presenting the request and specify warnings and provider policy where validation fails. WRP-OVERASKING-01 to -03 then require comparison of the live request with the registered attributes, a warning and explicit approval where the request exceeds that scope, and a provider decision whether to continue, disclose only the registered subset, or reject the request. These controls answer different questions: whether the certificate is valid; whether the request is consistent with the registration; and whether the requested data are substantively necessary. The first two can be technically checked. The third remains a legal and contextual assessment. Explicit user approval is neither proof of necessity nor necessarily consent in accordance with the requirements of the GDPR or another legal basis.

The same sequence illustrates movement between informative and binding artefacts. ARF v3.0.0 requirement RPRC_21 describes comparison, warning, and provider response, while the implementing regulation states related functions as binding, named technical requirements [16]. While this does not make the ARF binding or establish direct provenance for every adopted requirement, it shows that technical structures developed in the wider process can reappear in a binding annex, while the public record may not preserve a complete chain linking technical authorship, institutional treatment, stated reasons, and responsibility.

Topic X makes part of that process visible. The 2026 refinement round exposed alternatives and invited submissions on relying-party registration [23,4]. The *Agencia Española de Protección de Datos* (AEPD) argued that machine-readable registration certificates should be mandatory so that Wallets could check requests locally and by default, rather than depend on user-initiated checks or queries to a central registrar that could reveal which services a user accesses.[6] The subsequent legal requirement for certificate issuance is consistent with revision of the earlier optional model, but chronology does not establish that the AEPD intervention caused that change. Nor does certificate-based verification establish the necessity of everything a relying party registered.

Recent user research reinforces why the approval step cannot carry the compliance burden. In a survey of 1,035 users and 27 experts and a simulated study with 1,002 users, Zingg et al. found that approximately 20% of surveyed users indicated that they would disclose an official identity credential to a news website; in the simulated study, their Credential Assistant reduced average disclosure mistakes from about 15% to 7%, but did not eliminate them [34]. The study concerns user disclosure decisions, not the legality of relying-party requests, and used a simulated, context-limited setting without selective disclosure. Its bounded implication is nevertheless important: warnings and decision support can improve user choices, but leaving protection to the user permits residual oversharing and cannot substitute for relying-party compliance or preventive system controls.

The governance problem is thus not the disappearance of legal responsibility, but the distribution of prevention, evidence, and correction. Certificates and Wallet checks can expose and, depending on provider policy, prevent deviations from a registered declaration; the user can refuse disclosure. Later administrative or supervisory correction may be available, but those routes are not reconstructed here. No single control establishes necessity before disclosure. The public Topic X record also documents proposals and objections without revealing the complete focus-group deliberation or a reasoned institutional disposition of the AEPD submission. This section therefore shows legal responsibility remaining identifiable while operational accountability is fragmented across legal, technical, organisational, and supervisory layers.

[6] https://github.com/user-attachments/files/26022498/topicXrefinement.AEPD.response.pdf

7 Synthesis and Safeguards

The analysis supports a hybrid but legally differentiated account of implementation. Binding legislation and implementing acts establish duties, powers, and uniform conditions, while the formally informative ARF and versioned technical materials shape interoperable implementation. Requirements developed in the informative layer can reappear as named obligations in a binding annex, as the over-requesting control sequence shows, without thereby establishing direct provenance [16]. This is selective formalisation, not transformation of the ARF into law: adoption clarifies authority for the binding requirement, while upstream authorship, alternatives considered, and institutional treatment may remain only partly traceable. Practical influence does not confer legal authority.

Table 1: Benchmarked findings from the formal route and focal examples. Propositions are established in Sections 3–6.

Authority and mandate: formal authority and current ARF roles are distinct	
Formal route. Conferred powers; Commission adoption; regulated Member-State committee opinion	*ARF record.* Informative guidance; the current workflow requires Cooperation Group opinion and Commission approval implementing act
Access to information: different public records, neither complete	
Formal route. Register, final act, and document-access rules; confidential discussions and unattributed public summaries	*Repository record.* Granular proposals, reviews, and versions; no public Member-State feedback, deliberation, or approval reasons
Participation and representation: different entry routes, common specialist barriers	
Formal route. Member-State representatives; invited experts and third parties may speak but do not vote	*Repository record.* Public contribution, specialist-intensive effective participation, and concentrated recorded integration; no proof of representation or authority
Reason-giving, treatment of objections: contributor arguments are not institutional reasons	
Formal route. Internal explanation of substantially supported suggestions and reasons, but no required public answer to technical objections	*Repository record.* Detailed contributor objections and alternatives, but no public institutional disposition of focal objection or approval reasons
Documentary traceability and versioning: complementary records, incomplete provenance	
Formal route. Fixed act, adopter, and text; examined references to "the ARF" are not release-specific	*Repository record.* Stable issues, pull requests, commits, and releases; no complete chain from mandate and objection to institutional outcome, requirement, and version
Responsibility and correction: legal responsibility is clearer than operational correction	
Formal route. Commission adoption; a reasoned and amendable act, reviewable through applicable routes	*Focal examples.* Legal responsibility remains identifiable; prevention, evidence, escalation, and correction are distributed, with no public objection-specific correction route
Revisability and path dependency: available revision, bounded inference	
Formal route. The July 2026 acts show amendment, not objection-specific correction or causation	*Technical record.* Versioned revision is available; interdependent choices may raise migration costs, but irreversible entrenchment is not shown

Related weaknesses recur through different mechanisms. In comitology, the chair must tell the committee how substantially supported suggestions were treated, while the final act states its essential considerations; the public record need not answer each technical objection. Repository threads record contribu-

tor's objections, alternatives, and counterarguments, but the examined workflow does not establish an equivalent institutional duty of disposition. In both settings, public input is not consistently connected to a public account of uptake, and effective participation demands specialist capacity. The records are connected at several points, but they do not provide a complete public chain linking the legal mandate, technical objection and alternatives, and responsible institutional disposition. Furthermore, the combination creates an asymmetric versioning problem. The subject-matter articles of the principal implementing regulations refer to alignment with the ARF without identifying a release, whereas ARF v3.0.0 states in turn that it aligns the July 2026 amending acts [16]. The resulting gap is not absence of versioning on both sides, but absence of a provision-specific public map linking the legal baseline, technical source, institutional disposition, and effective version.

The Commission presents this combination of parallel legal and technical work as more agile, and the record bears that out in part [19]. On access to information, for the examined issues, the repository preserves a more granular public record of technical proposals and objections; technical options and objections were exposed before adoption of the relevant later measures, and there is versioned revisability before and after formal adoption. A strong defence treats the arrangement as functional specialisation [26]. Formal delegation, committee control, Cooperation Group coordination, and public technical scrutiny perform different tasks, and the July 2026 measures show an operative route for amendment and revision. Furthermore, the four-week publication of draft implementing acts is selective across comitology generally but appears to have been used consistently in this framework.

Our conclusion is nevertheless narrower than the agility claim implies. The demonstrated gains concern access, tempo, technical granularity, and revisability. On the criteria that bear on accountability, namely authority, treatment of objections, public reason-giving, and effective participation, the demonstrated gains in public technical visibility are not accompanied by a demonstrated improvement on institutional answerability or corrective capacity. Comitology makes the formal mandate and adopter clearer but may reveal little objection-specific technical reasoning; repositories may preserve detailed reasoning without identifying who authorised the outcome [20,15]. Formal adoption in the EUDIF still proceeds through implementing acts and comitology, while incomplete public reasons and partly non-public deliberative paths remain visible across both routes. The focal examples expose complementary problems. In the unlinkability episode, technically specific objections, alternatives, and feasibility constraints became publicly visible, but the record does not supply a complete institutional disposition. In over-requesting, legal responsibility remains identifiable while evidence, escalation, and correction are distributed across several controls and institutions.

Three measures follow from the comparison rather than from individual layers. Against *version drift*, binding alignments should identify the relevant ARF release or dated technical baseline on which it relies. Against the recurring *failure of reason-giving*, a duty to record what was received and how it was treated

should attach at both sites, covering the four-week feedback as well as material repository objections; the resulting disposition should name responsible actor, outcome, principal reasons, effective version, and conditions for reconsideration. Furthermore, stable identifiers should *connect* the legal basis, public issue, institutional disposition, and version, so that institutional authorisation and reasons and contributors' arguments can be distinguished and linked. Five further measures strengthen existing mechanisms rather than creating a parallel procedure. On *authority*, governance rules should distinguish public contribution, recorded integration, institutional opinion, and approval. On *access to information*, the public corpus should be indexed at privacy-significant milestones, and the Cooperation Group opinion and Commission approval published alongside the release they authorise. On *participation*, review at those milestones should be multidisciplinary , with an escalation forum able to initiate correction. On *responsibility*, the responsible body should publish a concise disposition naming the decision-maker, outcome, principal reasons, and conditions for reconsideration. On *revisability*, conformity requirements should be version-specific, with defined review triggers and migration planning. Applied proportionately, these measures preserve iteration while supplying answerability and correction.

8 Conclusion

Binding privacy commitments direct technical development in the EUDIF while iterative architecture and specification work tests feasibility and exposes conflicts that formal rules alone cannot resolve. On the bounded public record, however, the arrangement the Commission describes as agile produces informational and temporal gains without a demonstrated corresponding improvement in institutional answerability or corrective capacity. It improves the timing, specificity and documentary visibility of scrutiny and can support revision, but does not demonstrably overcome familiar weaknesses. Decision authority, institutional reasons, and correction remain distributed, and the additional technical layer can create provenance and responsibility gaps. The evidence therefore supports a proportionate package of legal-to-technical traceability, reasoned disposition of substantive objections, named decision responsibility, and version-specific correction.

The comparison has limits beyond those already stated. It sets two public records side by side, and the committee record is assessed only as published. Both focal issues were high-salience and expert-attended, and may not represent ordinary practice in either layer. Later versions, certification practice, national implementation, supervision, and deployment may alter the assessment. The broader implication is narrow but consequential. Digital regulation may depend not only on rules governing technical systems, but also on versioned technical processes that help make those rules operational.

References

1. Abellán Álvarez, I., Hölzmer, P., Sedlmeir, J.: Privacy evaluation of the European Digital Identity Wallet's Architecture and Reference Framework. Computers &

Security **160**, 104707 (2026)
2. European Digital Identity Wallet Architecture and Reference Framework: Topic a—privacy risks and mitigation. https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/v3.0.0/docs/discussion-topics/a-privacy-risks-and-mitigations.md (2025)
3. European Digital Identity Wallet Architecture and Reference Framework: Topic g—zero knowledge proof. https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/v3.0.0/docs/discussion-topics/g-zero-knowledge-proof.md (2025)
4. Topic x—relying party registration (revision round). https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/v3.0.0/docs/discussion-topics/x-rr-relying-party-registration.md (2026)
5. Baum, C., Blazy, O., Camenisch, J., Hoepman, J.H., Lee, E., Lehmann, A., Lysyanskaya, A., Mayrhofer, R., Montgomery, H., Nguyen, N.K., Preneel, B., shelat, a., Slamanig, D., Tessaro, S., Thomsen, S.E., Troncoso, C.: Cryptographers' feedback on the EU Digital Identity's ARF. https://github.com/user-attachments/files/15904122/cryptographers-feedback.pdf (Jun 2024)
6. Blom-Hansen, J., Brandsma, G.J.: The EU comitology system: intergovernmental bargaining and deliberative supranationalism? JCMS: Journal of Common Market Studies **47**(4), 719–739 (2009)
7. Bock, T., Alznauer, N., Joblin, M., Apel, S.: Automatic core-developer identification on GitHub: A validation study. ACM Transactions on Software Engineering and Methodology **32**(6), 1–29 (2023)
8. Bormann, C., Lehmann, A.: SoK: Anonymous credentials for digital identity wallets. In: Pöhls, H.C., Mitchell, C.J. (eds.) Security Standardisation Research. Lecture Notes in Computer Science, vol. 16466, pp. 3–25. Springer, Cham (2026)
9. Brandsma, G.J.: Delegated and implementing acts: rule-making by the Commission. In: Handbook on European Union Public Administration, chap. 17, pp. 253–265. Edward Elgar, Cheltenham (2024)
10. Brandsma, G.J., Curtin, D., Meijer, A.: How transparent are EU 'comitology' committees in practice? European Law Journal **14**(6), 819–838 (2008)
11. Christiansen, T., Dobbels, M.: Comitology and delegated acts after Lisbon: how the European Parliament lost the implementation game. European Integration online Papers **16**(13) (2012)
12. De Rosa, P.: Response to 'cryptographers' feedback on the EU Digital Identity's ARF'. https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/discussions/211#discussioncomment-9882388 (Jun 2024)
13. Dehousse, R.: Comitology: who watches the watchmen? Journal of European Public Policy **10**(5), 798–813 (2003)
14. Djeffal, C.: Law by design obligations: The future of regulating digital technologies in europe? Computer Law & Security Review **59**, 106232 (2025)
15. EDICG: CI gates and release workflow (2026), https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/v3.0.0/CI_AND_RELEASE_WORKFLOW.md
16. EDICG: The European Digital Identity Wallet Architecture and Reference Framework, version 3.0.0. https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/releases/tag/v3.0.0 (Jul 2026)
17. eIDAS Committee: Rules of Procedure for the eIDAS Committee. Adopted under Article 9(1) of Regulation (EU) No 182/2011; Comitology Register, committee code C47300. Ref. Ares(2020)5494835

18. eIDAS Expert Group: The European Digital Identity Wallet Architecture and Reference Framework, version 1.4.0. GitHub release, https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/releases/tag/v1.4.0 (May 2024)
19. European Commission: The european digital identity regulation was created in a more agile way, https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/915931909/The+European+Digital+Identity+Regulation+was+created+in+a+more+agile+way
20. European Commission: Standard rules of procedure for committees. OJ C 206, 12.7.2011, p. 11 (2011)
21. European Commission: Report from the Commission on the working of committees in 2024. COM (2025) 642 final, European Commission, Brussels (Oct 2025), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0642
22. Friedrichs, K., Harding, F., Lehmann, A., Lysyanskaya, A.: Device-bound anonymous credentials with (out) trusted hardware. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 345–375. Springer (2026)
23. Topic x—relying party registration (refinement round). https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/discussions/645 (Feb 2026)
24. Gornet, M., Maxwell, W.: The European approach to regulating AI through technical standards. Internet Policy Review **13**(3) (2024)
25. Joblin, M., Apel, S., Hunsen, C., Mauerer, W.: Classifying developers into core and peripheral: An empirical study on count and network metrics. In: 2017 IEEE/ACM 39th International Conference on Software Engineering. pp. 164–174. IEEE (2017)
26. Joerges, C., Neyer, J.: From intergovernmental bargaining to deliberative political processes: the constitutionalisation of comitology. European Law Journal **3**(3), 273–299 (1997)
27. Kalliamvakou, E., Gousios, G., Blincoe, K., Singer, L., German, D.M., Damian, D.: An in-depth study of the promises and perils of mining GitHub. Empirical Software Engineering **21**(5), 2035–2071 (2016)
28. Lessig, L.: Code and Other Laws of Cyberspace. Basic Books, 2 edn. (2006), published as Code: Version 2.0;
29. O'Mahony, S., Ferraro, F.: The emergence of governance in an open source community. Academy of Management Journal **50**(5), 1079–1106 (2007)
30. Podda, E., Hölzmer, P., Amard, A., Sedlmeir, J., Fridgen, G.: The impact of zero-knowledge proofs on data minimisation compliance of digital identity wallets. Internet Policy Review **14**(3) (2025)
31. Reidenberg, J.R.: Lex informatica: The formulation of information policy rules through technology. Texas Law Review **76**, 553–584 (1998)
32. Weigl, L., Reysner, M.: The governance of the European Digital Identity Framework through the lens of institutional mimesis. Regulation & Governance (2025), advance online publication, 22 May 2025
33. World Wide Web Consortium: Data integrity BBS cryptosuites v1.0. W3C candidate recommendation draft, W3C Verifiable Credentials Working Group (Apr 2026), https://www.w3.org/TR/2026/CRD-vc-di-bbs-20260407/, editors: Greg Bernstein and Manu Sporny; published 7 April 2026
34. Zingg, S., Lain, D., Nakatsuka, Y., Kostiainen, K., Bechtold, S., Čapkun, S.: Credential disclosure in (EU) digital identity wallets: Privacy risks and practical mitigations. arXiv preprint arXiv:2606.06354 (2026)