From NIS2 to the EUDI Wallet: Path Dependence in EU Digital Identity Security and Assurance

Giorgio Pedrazzi[1]

[1]Department of Law, University of Brescia, via Battaglie 58, 25121 Brescia, Italy

Abstract

Digital identity regulation in the European Union is increasingly embedded in a wider cybersecurity governance framework. This paper develops a bounded account of regulatory path dependence in the European Digital Identity Framework (EDIF) established by the revised eIDAS Regulation. It argues that EDIF does not replicate NIS2 institutionally; rather, NIS2 conditions its implementation through formal supervisory interfaces and indirect compliance spillovers, whose intensity varies across actors. The paper identifies four channels: institutional coupling between identity and cybersecurity authorities; the importation of risk-management and state-of-the-art security baselines; interaction between NIS2 compliance practices and the certification pathways established by eIDAS and the Cybersecurity Act; and incident-governance and reporting routines. Vulnerability transmission is treated as a cross-cutting risk where supervisory mandates, institutional capacity, or evidentiary expectations remain uneven. An illustrative analysis of zero-knowledge proofs shows that privacy-preserving design relocates rather than removes assurance requirements, shifting them from direct data disclosure to the trustworthiness of protocols, wallets, and verification environments. The paper contributes a matrix linking these conditioning channels to EDIF actors, legal interfaces, and likely compliance evidence, and concludes by recommending harmonised evidentiary baselines, clearer supervisory primacy in cross-border incidents, and interoperable assurance pathways.

Keywords

European Digital Identity Framework (EDIF), revised eIDAS Regulation, NIS2, Digital identity governance, Compliance evidence, Cybersecurity, Conformity assessment and certification, Zero-knowledge proofs (ZKPs), Interoperability, Regulatory path dependence

1. Introduction

The European Digital Identity Framework (EDIF), established by Regulation (EU) 2024/1183 amending the eIDAS Regulation (the revised eIDAS Regulation, often referred to as "eIDAS 2.0"), is usually framed as an identity project: a framework for deploying the European Digital Identity Wallet (EUDI Wallet), enabling cross-border identification, and supporting trustworthy digital interactions across the Single Market [1, 2]. Yet EDIF is also a project about infrastructure assurance. Wallet ecosystems, attribute sources, and relying parties will only be viable at scale if they operate under a credible baseline of cybersecurity and operational resilience. Policy and practitioner literature already treats cybersecurity as a precondition for trust in wallet-based identity systems [3, 4].

This paper develops that intuition as a bounded path dependence argument. The claim is not that EDIF institutionally copies NIS2. It is that the practical meaning of "security," "assurance," and "compliance evidence" inside the EUDI Wallet ecosystem is conditioned by the pre-existing cybersecurity governance architecture of NIS2. The contribution is doctrinal and governance-analytical rather than empirical: it identifies the channels through which NIS2 shapes EDIF implementation and distils them into a path dependence matrix linking conditioning features, governance touchpoints, and likely evidentiary artefacts.

TDI 2026: 4th International Workshop on Trends in Digital Identity, April 20–21, 2026, Verona, Italy
giorgio.pedrazzi@unibs.it (G. Pedrazzi)
https://expertise.unibs.it/resource/person/1842 (G. Pedrazzi)
0000-0002-1634-9966 (G. Pedrazzi)

1.1. Research question and scope

This paper asks how Directive (EU) 2022/2555 (NIS2) structures the operational security meaning of the European Digital Identity Framework and what implications this conditioning has for assurance and cross-border interoperability. The paper examines the EU legal architecture and its cross-border coordination mechanisms. It does not undertake comparative case studies of national implementation, although national supervisory bodies necessarily appear as components of that EU governance structure.

1.2. Contribution

The paper makes three contributions.

1) It clarifies regulatory path dependence in a layered EU regulatory stack and distinguishes it from simple institutional borrowing.
2) It develops a mechanism-based account of how NIS2 conditions EDIF implementation through institutional coupling, baseline importation, assurance and certification pathways, and incident governance and reporting readiness [1, 5].
3) It provides a path dependence matrix translating those mechanisms into concrete governance touchpoints and likely compliance evidence artefacts, while treating vulnerability transmission as a cross-cutting governance risk.

1.3. Roadmap

Section 2 defines the paper's path dependence framework. Section 3 maps the EDIF governance mesh and its key interfaces with cybersecurity regulation. Section 4 identifies the four conditioning mechanisms and the cross-cutting risk of vulnerability transmission. Section 5 applies the framework to zero-knowledge proofs as an illustrative assurance case. Section 6 presents the path dependence matrix. Sections 7 and 8 derive implications and conclude.

2. Conceptual framework: path dependence in the EU regulatory stack

This paper uses *path dependence* to explain how cybersecurity governance shapes the European Digital Identity Framework (EDIF). The point is not that EDIF institutionally replicates the NIS2 Directive [5]. Rather, the claim is that EDIF's operational security semantics, what it means in practice to be "secure," "assured," or "compliant", are conditioned by a pre-existing regulatory substrate comprising NIS2 duties, supervisory routines, incident-governance practices, and expectations about state-of-the-art cybersecurity.

2.1. Defining "path dependence" for regulatory stacks

In the classic institutional literature, path dependence describes how early choices constrain later options through increasing returns, sunk investments, and coordination effects. Transposed into a regulatory setting, especially an EU setting characterised by overlapping instruments, the concept is used here in a narrower sense. Regulatory path dependence exists where a later instrument's practical implementation is structured by an earlier instrument's obligation set, institutional routines, or compliance-evidence expectations, such that actors interpret or operationalise the later instrument through governance practices already established under the earlier regime.

This definition identifies three observable channels:

1 *Obligational conditioning*: later obligations are implemented using pre-existing compliance architectures.
2 *Institutional conditioning*: later governance is mediated through institutions or coordination structures already active under the earlier regime.

3 *Evidentiary conditioning*: what counts as persuasive proof of compliance is influenced by existing audit, supervision, and incident-response paradigms.

The result is not legal identity between regimes. Nor does the argument claim irreversible lock-in in the strong historical-institutionalist sense. Rather, it concerns path-shaped implementation trajectories within a layered Union regulatory order. This usage overlaps with regulatory layering and institutional spillover [6], but retains the language of path dependence to capture the structured way in which an earlier cybersecurity regime can supply operational reference points for a later identity-governance framework.

The intensity of NIS2 conditioning is not uniform across the EDIF ecosystem. It may be *direct* where an EDIF actor independently falls within NIS2's scope—qualified trust service providers, for example, are essential entities irrespective of size under Article 3(1)(b) NIS2 [5]. It may be *formally mediated* where the revised eIDAS Regulation requires cooperation or information exchange with NIS2 authorities. It may also be *indirect* where NIS2 risk-management and evidentiary practices influence certification, supervision, contractual assurance, or market expectations without creating an additional NIS2 obligation for the EDIF actor concerned. This threefold distinction prevents regulatory conditioning from being conflated with direct legal applicability.

Methodologically, the paper proceeds through a doctrinal reading of the revised eIDAS framework, NIS2, the Cybersecurity Act, and implementing measures and governance instruments adopted for the EUDI Wallet ecosystem. The analysis identifies legal and institutional interfaces through which conditioning or spillover may occur, while remaining cautious about the current limits of comparative implementation evidence at Member State level.

2.2. Path dependence vs. "mimesis"

A risk in EDIF scholarship is to treat similarities in governance architecture as proof of direct copying. Weigl and Reysner [7] identify institutional mimesis (mimetic isomorphism) in which the Commission seeks legitimacy by emulating features of the GDPR governance model in an area where subsidiarity sensitivity is high. On that account, EDIF governance may be "GDPR-like" because the GDPR supplies a familiar institutional model that can stabilise expectations and support central coordination.

Those scholars make a different claim about cybersecurity regulation: the relationship between NIS2 and EDIF is not an instance of "NIS2 mimesis." Instead, security obligations and practices associated with NIS2 affect how EDIF is implemented and protected. The distinction is important because *mimesis* concerns institutional form and legitimacy, whereas *path dependence* in the sense used here concerns operational substance: how security and assurance are interpreted, supervised, and evidenced. A regulatory system can therefore be mimetic at the level of governance architecture while being path-dependent at the level of compliance practice.

2.3. Analytical approach: mechanism tracing and compliance-evidence mapping

a) *Focus on interfaces, not full doctrinal restatement.* NIS2 and the revised eIDAS Regulation are extensive instruments. Rather than restating either regime exhaustively, the analysis targets interfaces where EDIF governance requires cooperation, information exchange, assurance, or enforcement routines that are connected to cybersecurity governance.

b) *Treat assurance as a compliance problem.* EDIF depends on demonstrable assurance: a credible way to show that wallets, trust services, and connected actors satisfy applicable security expectations. Path dependence becomes visible where assurance relies on established certification practices, conformity assessment pathways, audit routines, and risk-management evidence.

c) *Make compliance evidence explicit.* The path dependence matrix links NIS2 conditioning features to EDIF touchpoints and associated technical or procedural artefacts, including risk assessments, policies, audit reports, certification outputs, and incident-response documentation.

Making evidence explicit serves two purposes. First, it provides an operational account of how EDIF compliance is likely to be evaluated. Second, it allows a disciplined discussion of fragmentation: where evidence expectations remain under-specified or are implemented differently, discretion and divergence may increase.

2.4. Analytical propositions derived from the framework

The framework yields four doctrinal expectations at EU level:

- H1 *Institutional coupling*: EDIF governance will depend on cooperation between identity and cybersecurity authorities, causing cybersecurity institutions and coordination routines to mediate EDIF outcomes.
- H2 *Baseline importation*: EDIF security requirements will be interpreted through risk-management and state-of-the-art baselines familiar from NIS2 supervision.
- H3 *Assurance channel*: certification and conformity assessment will become practical pathways through which EDIF technical choices are rendered governable and comparable.
- H4 *Incident-governance conditioning*: EDIF incident handling and cross-border escalation will be structured by reporting practices, coordination channels, and evidentiary routines developed within EU cybersecurity governance.

Across all four propositions, uneven supervisory capacity, independence safeguards, or evidence expectations may transmit national governance weaknesses into the cross-border EDIF ecosystem. The next section maps the governance interfaces at which these propositions become relevant.

3. EDIF governance at EU level: actors, interfaces, and discretion

To understand how NIS2 conditions the European Digital Identity Framework, the relevant unit of analysis is not a single authority but a governance mesh spanning wallet supervision, trust services, cybersecurity, data protection, and certification. Weigl and Reysner emphasise that EDIF governance builds on a mix of pre-existing national institutions and newly introduced coordination structures, while the revised eIDAS Regulation itself creates formal interfaces with NIS2 authorities and ENISA [7, 1].

3.1. The EDIF governance mesh (high-level map)

At EU level, EDIF governance can be described through five functional nodes: wallet governance, trust-services governance, attribute-source governance, cybersecurity governance under NIS2, and data-protection governance under the GDPR [8]. Certification adds a further assurance layer grounded in the revised eIDAS Regulation and the Cybersecurity Act [9, 10]. These nodes are connected by coordination and cooperation duties rather than arranged in a single hierarchy. Questions of wallet security, assurance, and incident handling are therefore distributed across institutions with different legal mandates.

3.2. Interface points with NIS2: cooperation and institutional coupling

The strongest interface point is institutional. Article 46a of the revised eIDAS Regulation requires wallet supervisory bodies to inform the competent authorities designated under Article 8(1) NIS2 of significant security breaches or losses of integrity; Article 46b contains a parallel rule for trust-service supervision. Article 46e further connects the European Digital Identity Cooperation Group with ENISA and the NIS Cooperation Group [1]. These are formal legal interfaces, not merely functional similarities. They make cybersecurity authorities and coordination routines part of EDIF incident governance even where a particular wallet provider or relying party is not itself directly subject to NIS2.

3.3. Discretion and fragmentation risks in a multi-authority system

A multi-authority governance mesh creates predictable coordination burdens and fragmentation risks [11]. The revised eIDAS Regulation gives wallet supervisory bodies concrete information-gathering, inspection, remedial, and suspension powers [1]; the structural concern is therefore not the formal absence of supervisory powers. Rather, the risk lies in variation in institutional capacity, functional separation, allocation of competences, and the practical exercise of authority across Member States. Those variations can affect the standards applied in supervision and the evidence demanded from regulated entities, with potential consequences for cross-border recognition.

3.4. Independence and institutional conflicts as governance vulnerabilities

A related concern is institutional independence. Weigl and Reysner note that the GDPR contains detailed independence guarantees for data protection authorities, whereas the revised eIDAS framework specifies independence less elaborately; they also recall eIDAS1-era risks of supervisory bodies simultaneously providing qualified trust services [7]. The point here is not to assess any specific Member State, but to identify a vulnerability channel: coupling identity and cybersecurity governance does not itself resolve conflicts of role, uneven supervisory capacity, or unclear functional separation.

3.5. Complementary regimes and analytical delimitation

EDIF security governance does not arise in a regulatory vacuum, and NIS2 is not the sole regime shaping the EUDI Wallet ecosystem. The revised eIDAS framework establishes wallet-specific rules on certification, security-breach reactions, relying-party registration, and the list of certified wallets through dedicated implementing regulations [10, 12, 13, 14]. The broader environment also includes data-protection law, the European cybersecurity certification framework under the Cybersecurity Act [9], technical specifications on wallet functionality and protocols [15, 16], and the Architecture and Reference Framework developed through the EUDI toolbox process [17]. The paper's narrower claim is therefore one of relative structuring force: within this broader ecology, NIS2 supplies a central horizontal baseline for risk-management and incident-governance practices and creates important supervisory interfaces with EDIF.

4. Mechanisms of NIS2 path dependence in the EDIF

This section develops the paper's core analytical claim through four mechanisms. The intensity of conditioning differs by actor: it is direct where an actor independently falls within NIS2, formally mediated where the revised eIDAS Regulation creates an interface with NIS2 institutions, and indirect where cybersecurity practices shape assurance or evidentiary expectations without extending NIS2's personal scope.

4.1. Mechanism 1: Institutional coupling through cooperation and information-sharing

The revised eIDAS Regulation expressly links wallet and trust-service supervision to NIS2 authorities. Wallet supervisory bodies must inform the relevant NIS2 competent authorities of significant security breaches or losses of integrity, and cross-border incidents may engage the NIS2 single point of contact; the European Digital Identity Cooperation Group also exchanges cybersecurity information with ENISA and may hold joint meetings with the NIS Cooperation Group [1]. Institutional coupling is therefore a formal feature of the legal architecture.

EDIF touchpoints. Institutional coupling is most visible in:

1. oversight of wallet providers and their security posture;
2. coordination around incidents affecting wallet ecosystems or trust services;

3. supervisory expectations for assurance processes; and
4. cross-authority escalation through single points of contact and cooperation groups.

Compliance consequences. The evidentiary implications differ according to legal status. For actors independently falling within NIS2, relevant security evidence may be requested by cybersecurity authorities as part of NIS2 supervision. For other EDIF actors, NIS2-based evidentiary practices may operate indirectly through identity supervision, certification, procurement, or contractual assurance. In both cases, interface governance becomes part of compliance work: organisations may need to maintain clear role allocation, escalation procedures, information-sharing protocols, and records capable of supporting coordinated supervision. The mechanism thus concerns institutional mediation, not an assumption that every EDIF participant is directly subject to NIS2.

4.2. Mechanism 2: Importation of cybersecurity baselines ("state of the art" semantics)

Weigl and Reysner emphasise that the relationship between NIS2 and EDIF is not "NIS2 mimesis" but a path-dependent relation in which NIS2 security obligations and best practices affect how EDIF is implemented and protected [7]. Baseline importation matters wherever EDIF requires secure implementation or adequate protection, including wallet software security, identity lifecycle governance, integrity of attribute sources, third-party access, and incident detection and response.
Compliance consequences.

1. *Risk management as an organising principle.* Even where EDIF rules are technology-neutral or high-level, implementation is likely to be organised around recurring risk assessment, controls, monitoring, testing, and incident response.
2. *Evidence of appropriate and proportionate measures.* Organisations will be expected to produce documentation demonstrating that controls are suitable, maintained, and tested, although the precise legal source of that duty varies by actor.
3. *Dynamic baselines.* Because the cybersecurity state of the art evolves, acceptable assurance is not static. The path-dependent effect lies in the use of familiar cybersecurity methods to give operational content to EDIF security requirements.

The claim is therefore interpretive rather than jurisdictional: NIS2 helps supply the practical vocabulary through which adequate security posture is assessed, but it does not automatically extend its duties to every EDIF actor.

4.3. Mechanism 3: Assurance and certification as a governance channel

In complex technical ecosystems, legal requirements become governable through conformity assessment, certification, audit schemes, and related assurance practices. For EUDI Wallets, certification is established by the revised eIDAS framework and Commission Implementing Regulation (EU) 2024/2981, within the wider certification architecture of the Cybersecurity Act [1, 10, 9]. NIS2 contributes more indirectly by reinforcing risk-management, vulnerability-handling, and evidence-based compliance practices that can shape how certification outputs are produced and used. ENISA's 2026 EUDIW scheme remains a draft candidate European cybersecurity certification scheme rather than an operative final scheme [18].
EDIF touchpoints. Assurance channels are relevant for wallet conformity, trust-service audits, interoperability profiles, procurement, and reliance decisions. Policy and practitioner literature has likewise treated certification and conformity assessment as potential trust-building mechanisms for wallet ecosystems [3].
Compliance consequences.

1) *Certification as strong, but scoped, evidence.* Certification may become an important shortcut for demonstrating that defined wallet components or requirements have been assessed, but it does not by itself establish compliance with every EDIF, GDPR, or NIS2 obligation.

2) *Assurance as an interoperability condition.* Interoperability is not solely technical: divergent certification scopes, assessment practices, or acceptance of evidence can fragment cross-border reliance.
3) *Allocation of assurance responsibilities.* The assurance architecture influences which actor must generate, retain, or rely upon particular evidence, without displacing the liability rules applicable under the underlying legal regimes.

4.4. Mechanism 4: Incident governance and reporting readiness

Incident governance provides the clearest operational bridge between EDIF and NIS2. The revised eIDAS Regulation requires wallet and trust-service supervisory bodies to notify relevant NIS2 competent authorities of significant security breaches or losses of integrity, while Commission Implementing Regulation (EU) 2025/847 specifies reactions to security breaches of EUDI Wallets [1, 12]. Article 46e of the revised eIDAS Regulation also provides for cooperation with ENISA and joint meetings with the NIS Cooperation Group on cyber threats, incidents, vulnerabilities, exercises, and standards [1].
EDIF touchpoints. The mechanism is most visible in wallet ecosystem incidents, trust-service disruption, credential compromise, systemic dependency failures, and cross-border escalation.
Compliance consequences. Incident readiness makes procedural evidence particularly salient: incident-response plans, escalation matrices, detection and logging policies, tested communication routes, exercise records, incident timelines, and post-incident remediation. Differences in thresholds, channels, or supervisory expectations can generate duplicative reporting or inconsistent demands. Here path dependence is visible in the transplantation of cybersecurity incident-governance routines into the operation of identity infrastructure.

4.5. Cross-cutting governance risk: vulnerability transmission

Vulnerability transmission is better treated as a cross-cutting risk than as a fourth mechanism. Weigl and Reysner argue that supervisory independence is specified less elaborately in the revised eIDAS framework than under the GDPR and identify historical risks of conflicts of institutional role [7]. The revised eIDAS Regulation nevertheless grants concrete supervisory powers; the relevant vulnerability therefore concerns uneven capacity, functional separation, coordination, or exercise of those powers rather than their formal absence [1].

Where these weaknesses persist, coupling can have ambiguous effects. It may add layers of oversight without resolving role conflicts, contribute to divergent supervisory intensity, or generate inconsistent evidentiary demands. These are prospective governance risks rather than demonstrated empirical outcomes. In path dependence terms, EDIF can inherit mature cybersecurity assurance and incident routines while remaining exposed to uneven institutional implementation across Member States.

4.6. Output: the path dependence matrix as an operational bridge

These mechanisms motivate the paper's main operational output: a path dependence matrix linking conditioning features to EDIF touchpoints, likely compliance evidence, and governance risks. The matrix distinguishes technical artefacts (such as logs, test outputs, and certification reports) from procedural artefacts (such as policies, escalation protocols, and inter-authority procedures). Vulnerability transmission is represented as a cross-cutting governance effect rather than as a separate conditioning feature.

5. Illustrative application: zero-knowledge proofs as an assurance and interoperability case

This section uses zero-knowledge proofs (ZKPs) as an illustrative application rather than as independent empirical evidence. The question is whether the governance account still explains implementation

choices when privacy-preserving architectures reduce direct data disclosure. The example is anchored in a live implementation environment: the toolbox process has produced an Architecture and Reference Framework, while the revised eIDAS framework and its implementing measures now regulate wallet certification, the list of certified wallets, relying-party registration, and reactions to security breaches [17, 10, 14, 13, 12].

ZKPs sharpen a core governance tension in wallet ecosystems: privacy-enhancing design may reduce attribute disclosure, but it does not eliminate assurance needs. If a relying party receives a derived proof rather than the underlying attributes, confidence must be rebuilt through other evidence, such as assessment of wallet components, validated trust chains, protocol conformance, and assurance statements [19, 20]. NIS2-conditioned expectations concerning secure implementation, testing, vulnerability handling, and incident readiness may therefore remain relevant even where the transaction itself becomes more privacy-preserving.

The example supports two narrower points. First, the revised eIDAS framework requires wallets to support selective disclosure, while the implementing rules specify technical support for selective disclosure without prescribing a single privacy-preserving proof architecture [1, 15, 16]. That leaves room for implementation choices whose interoperability depends on comparable assurance practices. Second, the legal question is not only whether a privacy-preserving proof is technically valid, but also what evidentiary weight its outputs and surrounding assurance artefacts should carry in supervisory review, incident analysis, and reliance decisions. Privacy-preserving design therefore relocates rather than removes the problem of assurance.

6. The path dependence matrix: conditioning features, touchpoints, and compliance evidence

Sections 2–5 develop an EU-level argument that EDIF's operational security meaning is conditioned by NIS2 through mechanisms of varying legal intensity. The matrix translates that regulatory-stack claim into identifiable conditioning features, EDIF touchpoints, likely compliance evidence, and governance risks. It also makes visible where under-specification or divergent implementation may shift the burden onto national authorities, assurance schemes, or market practice.

A key premise is that compliance in complex infrastructures is increasingly evidence-mediated: actors do not merely claim that systems are secure; they must be able to demonstrate relevant controls, procedures, and assurance in auditable form. The matrix therefore treats evidentiary conditioning as an attribute of each mechanism, while vulnerability transmission appears as a cross-cutting risk rather than a separate operational feature.

6.1. Matrix (core version)

Table 1 operationalises the four conditioning mechanisms by identifying the EDIF interfaces at which they become relevant, the forms of evidence likely to become salient, and the principal governance risks. The entries are prospective analytical expectations, not a claim that every listed artefact is legally mandatory for every EDIF actor.

Table 1: Path-dependence matrix: conditioning features, EDIF touchpoints, compliance evidence, and governance risks.

Operational conditioning feature	**EDIF touchpoint**	**Likely compliance evidence**	**Primary governance risk / effect**
Institutional coupling (cooperation and information-sharing)	Wallet and trust-service supervision; single points of contact; incident escalation	Authority-interface procedures; role allocations; cooperation and information-sharing procedures; exercise records; incident-communication templates; audit trails of coordination decisions	Overlap or duplication; inconsistent guidance; unclear primacy during incidents; fragmented cross-border escalation

Table 1 continued

Operational conditioning feature	EDIF touchpoint	Likely compliance evidence	Primary governance risk / effect
Baseline importation (state-of-the-art security semantics; risk-management routines)	Wallet security posture; identity lifecycle; attribute-source integrity; third-party and supply-chain access	Risk assessments; threat models; security requirements; secure-development lifecycle evidence; access-control and key-management policies; recovery and change-management records; risk-proportionate logging policies	Moving-target compliance; divergent interpretations of adequate or proportionate security; privacy–accountability tension in logging
Assurance and certification pathways (conformity assessment as compliance substrate)	Wallet conformity; trust-service audits; interoperability profiles; procurement and reliance decisions	Certification and conformity-assessment reports; audit reports; penetration-testing summaries; vulnerability-remediation evidence; scoped assurance statements; reliance and verification records	Fragmented certification practice; cost barriers; uneven acceptance or interpretation of evidence across Member States
Incident governance and reporting readiness (operational resilience logic)	Wallet incidents; trust-service disruption; credential compromise; systemic dependency failures; cross-border crises	Incident-response plans; escalation matrices; detection and logging policies; exercise evidence; post-incident reports; lessons learned and control updates; incident timelines and disclosure records	Duplicative or inconsistent reporting; unclear thresholds; paper compliance without demonstrated operational readiness; vulnerability transmission through uneven implementation

Reading the matrix. The matrix distinguishes the governance features through which NIS2 conditions implementation from the forms of evidence through which security and assurance may be assessed. Baseline importation explains why wallet security is evaluated through familiar cybersecurity semantics; assurance and certification pathways explain why conformity-assessment outputs can become important for trust and interoperability; and incident governance explains why procedural readiness and cross-authority evidence become central during security events. The ZKP example fits the same logic: privacy-preserving architectures remain governable only if their outputs and surrounding controls can be translated into recognised assurance and evidence forms.

7. Implications and recommendations

The analysis implies that EDIF compliance will be shaped not only by abstract statements of secure implementation but also by supervisory routines and evidence expectations embedded in the wider cybersecurity governance environment. Even before extensive comparative Member State practice has accumulated, the legal framework contains potential sources of divergence: inter-authority cooperation, incident reporting, risk-management duties, and wallet-specific certification and registration layers. In a multi-authority setting, non-comparable interpretations of adequate security and assurance can increase compliance costs and weaken cross-border interoperability.

Two implications follow. First, EDIF harmonisation should be evaluated not only at the level of substantive obligations but also at the level of comparable auditability: which artefacts are expected, for what purpose, and with what evidentiary weight. Second, institutional coupling makes clear supervisory interfaces especially important during incidents, when overlapping mandates can otherwise generate duplicative reporting or inconsistent directions.

Accordingly, the paper advances three EU-level recommendations addressing recurring issues across the four conditioning features in Table 1.

1) *Standardise minimum security-evidence expectations* across relevant EDIF touchpoints, specifying baseline artefacts for risk assessment, assurance outputs, vulnerability management, and incident readiness. Commission Implementing Regulation (EU) 2024/2981 already embeds risk assessment

and certification documentation in the wallet-certification framework [10]. A practical next step would be to use such risk and threat documentation to promote greater comparability in the technical and procedural evidence accepted across Member States.

2) *Clarify supervisory interfaces and primacy for incident scenarios*, including information-sharing routes and coordination between wallet and trust-service supervisors, NIS2 competent authorities and CSIRTs, and data protection authorities. The revised eIDAS Regulation already establishes formal information-sharing links with NIS2 authorities; clearer operational procedures could reduce duplicative reporting and contradictory directions [1, 12].
3) *Align assurance pathways to support interoperability*, ensuring that certification and conformity-assessment outputs have comparable scope and meaning across the ecosystem. This should include clearer guidance on the evidentiary treatment of privacy-preserving proofs and their surrounding assurance artefacts, so that data minimisation does not create avoidable uncertainty in audits or reliance decisions.

These steps would not eliminate Member State discretion, but they could reduce the space for non-comparable evidence demands that fragment the EDIF ecosystem or weaken trust in cross-border reliance.

8. Conclusion

This paper argues that EDIF security is path-dependent on NIS2 in a bounded regulatory sense. The relationship is not one of institutional copying, nor does it imply that all EDIF actors are directly subject to NIS2. Rather, NIS2 conditions EDIF implementation through a combination of direct applicability to some actors, formal supervisory interfaces, and indirect spillovers in risk-management and evidentiary practice.

The analysis develops this claim in three steps. First, it distinguishes regulatory path dependence from institutional mimesis and from strong historical accounts of lock-in. Second, it shows that EDIF operates as a multi-authority governance mesh in which identity supervision, trust services, cybersecurity, data protection, and certification are structurally connected. Third, it identifies four mechanisms through which NIS2 conditions EDIF outcomes: institutional coupling, baseline importation, assurance and certification pathways, and incident governance and reporting readiness. Vulnerability transmission is treated separately as a cross-cutting risk arising where supervisory capacity, functional separation, coordination, or evidence expectations remain uneven.

The path dependence matrix translates that diagnosis into an operational account linking conditioning features to EDIF touchpoints and likely compliance evidence artefacts. The legal architecture examined in the paper is consistent with the four analytical propositions set out in Section 2.4, while the brief ZKP example illustrates how privacy-preserving innovation remains dependent on recognised assurance and auditability pathways.

The policy implications follow directly from this diagnosis: establish more harmonised evidentiary baselines across relevant EDIF touchpoints, clarify supervisory interfaces and primacy in incidents, and align certification and conformity-assessment outputs to support interoperability. More broadly, the paper suggests that understanding the EDIF requires attention not only to identity law, but also to the cybersecurity governance regimes that help supply its operational security semantics.

Declaration on Generative AI

During the preparation of this work, the author used ChatGPT 5.2 to assist with grammar and spelling checks. The author subsequently reviewed and edited the text and assumes full responsibility for its content.

References

[1] European Parliament and Council of the European Union, Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 april 2024 amending regulation (EU) no 910/2014 as regards establishing the European Digital Identity Framework, Official Journal of the European Union, 2024. URL: https://eur-lex.europa.eu/eli/reg/2024/1183/oj, oJ L, 2024/1183, 30.4.2024.

[2] B. Podgorelec, L. Alber, T. Zefferer, What is a (digital) identity wallet? A Systematic Literature Review, in: Proceedings of the 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC 2022), 2022, pp. 809–818. doi:10.1109/COMPSAC54236.2022.00131.

[3] A. F. Radu, I. Petcu, D.-C. Barbu, EU digital identity: Privacy and security-related challenges of the future, Romanian Cyber Security Journal 4 (2022) 39–52. doi:10.54851/v4i2y202205.

[4] Z. Ebadi Ansaroudi, R. Carbone, G. Sciarretta, S. Ranise, Control is nothing without trust: A first look into digital identity wallet trends, in: V. Atluri, A. L. Ferrara (Eds.), Data and Applications Security and Privacy XXXVII: 37th Annual IFIP WG 11.3 Conference, DBSec 2023, Sophia-Antipolis, France, July 19–21, 2023, Proceedings, volume 13942 of *Lecture Notes in Computer Science*, Springer, Cham, 2023, pp. 113–132. doi:10.1007/978-3-031-37586-6_7.

[5] European Parliament and Council of the European Union, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 december 2022 on measures for a high common level of cybersecurity across the Union, amending regulation (EU) no 910/2014 and directive (EU) 2018/1972, and repealing directive (EU) 2016/1148 (NIS 2 Directive), Official Journal of the European Union, 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj, oJ L 333, 27.12.2022, p. 80.

[6] M. Bassini, M. Maggiolino, A. de Streel, Better Law-Making and Evaluation for the EU Digital Rulebook, Technical Report, CERRE, 2025. URL: https://cerre.eu/publications/better-law-making-and-evaluation-for-the-eu-digital-rulebook/, published 22 January 2025.

[7] L. Weigl, M. Reysner, The governance of the European Digital Identity Framework through the lens of institutional mimesis, Regulation & Governance (2025). doi:10.1111/rego.70032, advance online publication.

[8] European Parliament and Council of the European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj, oJ L 119, 4.5.2016.

[9] European Parliament and Council of the European Union, Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 april 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing regulation (EU) no 526/2013 (Cybersecurity Act), Official Journal of the European Union, 2019. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj, oJ L 151, 7.6.2019, p. 15.

[10] European Commission, Commission implementing regulation (EU) 2024/2981 of 28 november 2024 laying down rules for the application of regulation (EU) no 910/2014 of the European Parliament and the Council as regards the certification of European Digital Identity Wallets, Official Journal of the European Union, 2024. URL: https://eur-lex.europa.eu/eli/reg_impl/2024/2981/oj, oJ L, 2024/2981, 4.12.2024.

[11] G. De Gregorio, A. Vicinanza, The enforcement of european digital regulation: Overlaps and pathways, Yearbook of European Law (2026). doi:10.1093/yel/yeag002, advance online publication, 8 April 2026.

[12] European Commission, Commission implementing regulation (EU) 2025/847 of 6 may 2025 laying down rules for the application of regulation (EU) no 910/2014 of the European Parliament and of the Council as regards reactions to security breaches of European Digital Identity Wallets, Official Journal of the European Union, 2025. URL: https://eur-lex.europa.eu/eli/reg_impl/2025/847/oj, oJ L, 2025/847, 7.5.2025.

[13] European Commission, Commission implementing regulation (EU) 2025/848 of 6 may 2025 laying down rules for the application of regulation (EU) no 910/2014 of the European Parliament and of

the Council as regards the registration of wallet-relying parties, Official Journal of the European Union, 2025. URL: https://eur-lex.europa.eu/eli/reg_impl/2025/848/oj, oJ L, 2025/848, 7.5.2025.

[14] European Commission, Commission implementing regulation (EU) 2025/849 of 6 may 2025 laying down rules for the application of regulation (EU) no 910/2014 of the European Parliament and of the Council as regards the submission of information to the Commission and to the Cooperation Group for the list of certified European Digital Identity Wallets, Official Journal of the European Union, 2025. URL: https://eur-lex.europa.eu/eli/reg_impl/2025/849/oj, oJ L, 2025/849, 7.5.2025.

[15] European Commission, Commission implementing regulation (EU) 2024/2979 of 28 november 2024 laying down rules for the application of regulation (EU) no 910/2014 as regards the integrity and core functionalities of European Digital Identity Wallets, Official Journal of the European Union, 2024. URL: https://eur-lex.europa.eu/eli/reg_impl/2024/2979/oj, oJ L, 2024/2979, 4.12.2024.

[16] European Commission, Commission implementing regulation (EU) 2024/2982 of 28 november 2024 laying down rules for the application of regulation (EU) no 910/2014 as regards protocols and interfaces to be supported by the European Digital Identity Framework, Official Journal of the European Union, 2024. URL: https://eur-lex.europa.eu/eli/reg_impl/2024/2982/oj, oJ L, 2024/2982, 4.12.2024.

[17] European Commission, Version 2.0 of the Architecture and Reference Framework now available, EU Digital Identity Wallet portal, 2025. URL: https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/900014854/Version%2B2.0%2Bof%2Bthe%2BArchitecture%2Band%2BReference%2BFramework%2Bnow%2Bavailable, published 29 May 2025.

[18] ENISA, Draft candidate EUDIW scheme v0.4.614 for public review, European Union Cybersecurity Certification portal, 2026. URL: https://certification.enisa.europa.eu/publications/draft-candidate-eudiw-scheme-v04614-public-review_en, draft Candidate Scheme; published 31 March 2026, updated 7 April 2026.

[19] R. Ramos Fernández, Evaluation of trust service and software product regimes for zero-knowledge proof development under eIDAS 2.0, Computer Law & Security Review 53 (2024) 105968. doi:10.1016/j.clsr.2024.105968.

[20] E. Podda, P. Hölzmer, A. Amard, J. Sedlmeir, G. Fridgen, The impact of zero-knowledge proofs on data minimisation compliance of digital identity wallets, Internet Policy Review 14 (2025). doi:10.14763/2025.3.2019.