From NIS2 to the EUDI Wallet

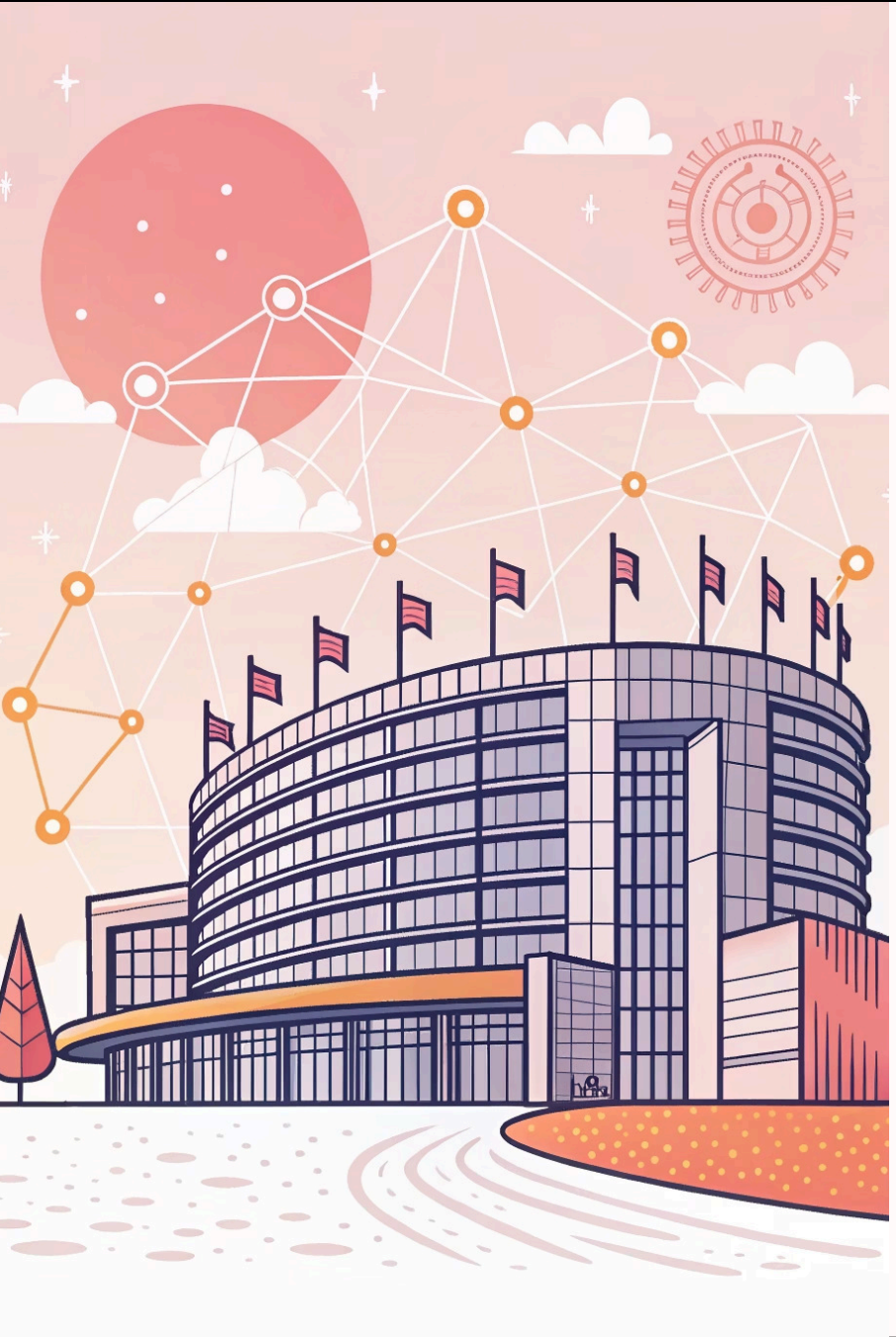
Path Dependence in EU Digital Identity Security and Assurance

GIORGIO PEDRAZZI

4th International Workshop on Trends in Digital Identity (TDI 2026)

20 April 2026 · Verona, Italy

Università di Brescia



The Broader EU Cybersecurity Framework

From framework-building to implementation

The EU acquis has expanded significantly

since the 2020 Cybersecurity Strategy.

Università di Brescia

Key Legislative Files

1. **NIS2 Directive**
   Applies since **18 Oct 2024** — main horizontal cybersecurity instrument
2. **Cyber Resilience Act (CRA)**
   In force **Dec 2024**; fully applicable **Dec 2027** — digital product requirements
3. **Cyber Solidarity Act & CSA Amendment**
   Both apply since **4 Feb 2025** — EU detection & response capacity; extends certification to managed security services
4. **EUIBA Regulation & EUCC Scheme**
   NIS2-aligned framework for EU institutions; EUCC first operational certification scheme, applies since **Feb 2025**
5. **Sector-Specific: DORA, Aviation, Electricity, EDIF, EHDS**
   DORA applies **Jan 2025**; EDIF since **May 2024**; EHDS from **Mar 2027** — phased to 2035

The Core Argument

EDIF does **not** institutionally copy NIS2.

Instead, NIS2 **conditions** the practical meaning of "security," "assurance," and "compliance evidence" inside the EUDI Wallet ecosystem.

Path dependence — not mimesis

Path Dependence vs. Mimesis

Mimesis

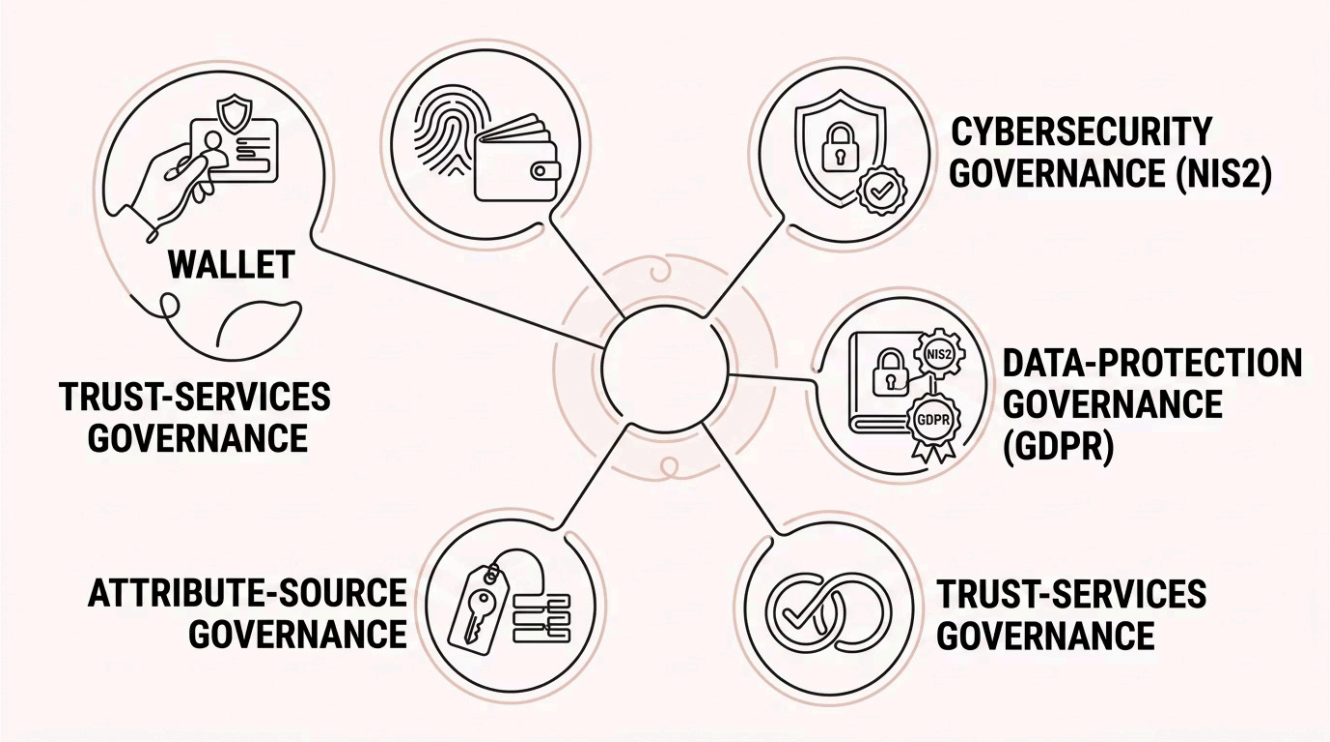
Institutional *form* — how governance is structured for legitimacy

Path Dependence

Operational *substance* — how security assurance is interpreted, supervised, and evidenced

The EDIF Governance Mesh

Nodes connected by cooperation duties – not a single hierarchy. NIS2 actors are **embedded**, not external.



Four Conditioning Mechanisms

1

Institutional Coupling

Cooperation across identity, cybersecurity & data-protection authorities

2

Baseline Importation

NIS2 "state of the art" semantics shape EDIF security posture

3

Assurance Channel

Certification & conformity assessment become de facto compliance proof

4

Vulnerability Transmission

Under-specified independence amplifies governance gaps

Mechanism 1: Institutional Coupling

Multi-regulator burden

Risk assessments & incident playbooks demanded by both identity and cybersecurity authorities

Convergence pressure

Identity assurance converges toward cybersecurity evidentiary logic

Interface governance

Cooperation protocols, MoUs, and accountable roles become compliance work

Mechanism 2: Baseline Importation

Wallet software security

Identity lifecycle

Issuance, revocation, recovery

Attribute-source integrity

Supply-chain & third-party access

⚠ Dynamic baselines — "state of the art" is a **moving target**

Evidence required: risk assessments, threat models, SDLC documentation, access-control & key-management policies.

Mechanism 3: Assurance Channel

→ Certification = de facto compliance proof

Shapes supervisory expectations and market behaviour

→ Assurance enables interoperability

Divergent assurance approaches **fragment** the ecosystem

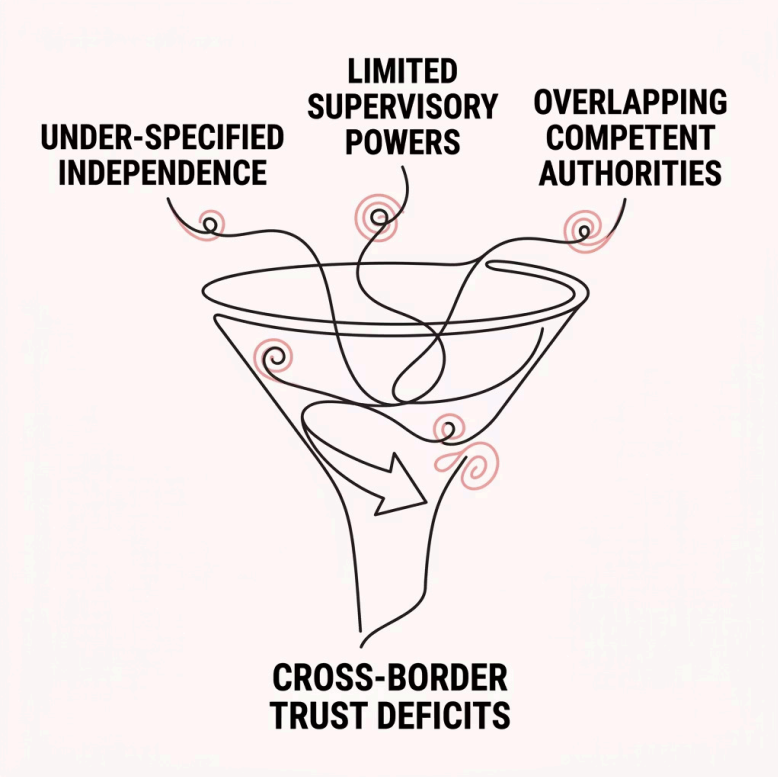
→ Liability follows assurance architecture

Who bears responsibility — wallet, issuer, attribute source, relying party?

Mechanism 4: Vulnerability Transmission

Coupling EDIF to weak or conflicted cybersecurity oversight does not merely replicate a domestic weakness – it can **compromise cross-border trust** in the EUDI Wallet ecosystem as a whole.

⊗ Layering without resolution



Stress Test: Zero-Knowledge Proofs

Privacy ≠ No Assurance

ZKPs reduce attribute disclosure — but **relocate** assurance needs to:

- Protocol trustworthiness
- Wallet certification
- Verification environment integrity

> NIS2-conditioned evidence expectations remain fully relevant

The Path-Dependence Matrix

Conditioning Feature	EDIF Touchpoint	Evidence Artifacts	Primary Risk
Institutional coupling	Wallet & trust-service supervision; SPOC; incident escalation	MoUs; RACI charts; cooperation protocols; joint exercise records	Overlap; unclear primacy
Baseline importation	Wallet security; identity lifecycle; attribute sources; supply chain	Risk assessments; threat models; SDLC evidence; key-management policies	Moving-target compliance; divergent interpretations
Assurance / certification	Wallet conformity; trust-service audits; interoperability; reliance decisions	Certification reports; audit outputs; pen-test summaries; assurance statements	Certification fragmentation; cost barriers
Incident governance	Wallet incidents; trust-service disruption; systemic failures	Incident response plans; escalation matrices; post-incident reports	Reporting confusion; compliance theatre

Three Policy Recommendations

1 Standardise evidence baselines

Harmonise artifacts for risk assessment, assurance, vulnerability management & incident readiness across the EDIF stack

2 Clarify supervisory interfaces

Define primacy and information-sharing routes for incidents across identity, NIS2, and DPA authorities

3 Align assurance for interoperability

Ensure certification outputs have comparable scope; clarify evidentiary status of privacy-preserving proofs

Key Takeaway

EDIF security is path-dependent on NIS2

Not through copying — but through inherited risk-management semantics, supervisory routines, and a compliance culture organised around **demonstrable evidence**.

Understand identity law

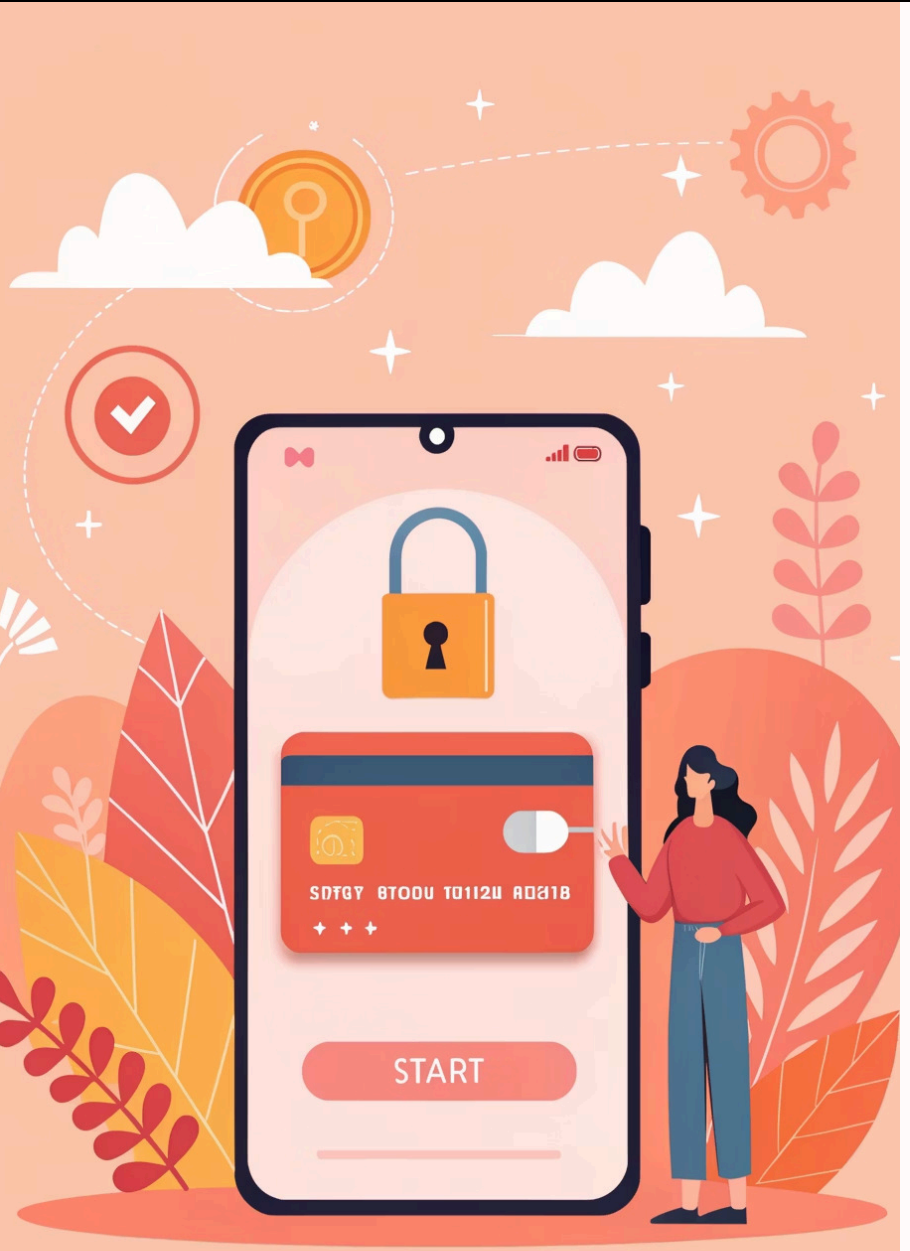
eIDAS2 / EDIF obligations

AND cybersecurity governance

NIS2 supplies operational semantics

AND evidence architecture

Auditability drives cross-border trust



Thank You!

Giorgio Pedrazzi ·

Department of Law, University of Brescia

Presented at *4th International Workshop on Trends in Digital Identity (TDI 2026)* · Verona, Italy

Università di Brescia