

Digital Trust

Authors

Helmer van Merendonk (Hogeschool Utrecht), Juul de Louw (Koning Willem 1 College), Peter Eikelboom (SURF), Marlies Rikken (SURF)

1. Trusted digital recognitions are emerging

2. More decentralisation of data ownership enabled by SSI solutions

3. Emergence of organisational wallets

4. Push for transparent supply chains with digital product passports

5. Digital Trust Frameworks: from hierarchical to distributed trust



Introduction

Trust is the foundation of all digital interactions. It is the confidence that people, systems, and technologies will act reliably, securely, and with integrity. In the digital world, trust means believing that personal data will be protected, systems will work as designed, and technologies will uphold ethical and secure practices. As digital ecosystems become more complex, maintaining and earning that trust becomes not just a technical challenge, but a strategic priority.

A shift is taking place in the way that digital identities and the verifiable credentials of individuals, organisations, and objects (physical and digital) are handled. The European Union (EU) is leading this transformation with the Digital Europe Program (DIGITAL). At the heart of this transformation is the European Union Digital

Identity (EUDI) Wallet initiative, which seeks to give citizens enhanced and secure control over their digital identities. In an age where misinformation, disinformation, and identity abuse are widespread, storing digital identities and credentials in digital wallets can help improve accountability, safeguard ownership, and reduce the misuse of personal data. By 2027, every EU citizen will have access to an initial version of a digital wallet. This wallet can be used to store and share personal details. This information will relate to both online and offline public and private services across the EU.

The EUDI Wallet will be applicable in many aspects of modern life, and it will have implications for how people use and access key identification information. For instance, it will be possible to store a digital

version of an individual's driving licence, thus eliminating the need for someone to always have a physical copy on their person. Besides identification information, the EUDI Wallet will provide a seamless recognition of qualifications and provide authorisation across the EU, simplifying education admissions, credentials management, student transfers, job applications, and talent mobility. At the same time, fraud will be reduced, while secure and cryptographically protected identities and credentials will be facilitated. This will help to reduce forgery and increase trust in qualifications.

The future of digital trust will give people more control over their own data, by embracing conceptual models such as Self-Sovereign Identity (SSI), along with the use of digital wallets to share their identities and

credentials. The success of these initiatives will have a significant impact on citizens as well as public and private organisations. Digital trust assures that the identities and data of people and organisations are handled securely, that digital interactions are reliable, and that their privacy, in terms of their identity and data, is protected. New types of trust networks will create a digital world that is more secure, fair, and trustworthy for everyone.




Contributors

Yvo Hunink (Founder of Regen Studio),
Niels van Dijk (SURF), **Peter Leijnse** (SURF), **Michiel Schok** (SURF),
Peter Nobels (HU)

TREND #1

Trusted digital recognitions are emerging

Public Values

-  **Autonomy** Personal empowerment
-  **Justice** Transparency | Equity | Inclusion | Integrity
-  **Humanity**

Maturity

- WATCH
- PLAN
- ACT

Drivers

Individualisation & Empowerment; Cybersecurity & Trust; Digital Transformation

European frameworks (eIDAS 2.0 and MiCA Regulation) are reshaping the digital landscape with two new concepts: Verifiable Credentials (VCs) and digital assets. Both will enable a shift towards trusted digital recognition of physical and digital objects by 2030.

VCs are tamper-proof digital attestations (diplomas or qualifications) issued by trusted institutions or organisations for individuals to store in their digital wallets.

Digital assets as tokens, including non-fungible tokens (NFTs), represent digital value, access, or ownership. As it is designed to be transferable: once a token leaves your wallet, its associated rights move too, making them suitable for (value) exchange, single-use recognition, or participation in initiatives.

Aspect	Verifiable Credential	Token/Digital Asset
Function	Reusable proof of achievement or skills, identity, or status	Transferable value, access, or participation
Reusability	Yes, holder can present it multiple times	No, it moves with ownership
Privacy	User-controlled, selective disclosure	Often public, depends on token design
Verification	Via digital signature and open standards (e.g. W3C, OpenID4VC)	Via blockchain consensus and smart contracts

SIGNALS

European regulation

eIDAS 2.0 Regulation (eur-lex.europa.eu) [↗](#)

Markets in Crypto-Assets (MiCA) Regulation
(eur-lex.europa.eu) [↗](#)

Nederlandse overheid - Toekomstverkenning Digitalisering 2030
(rijksoverheid.nl) [↗](#)

Education, skills & lifelong learning

SELFIE for work-based learning (education.ec.europa.eu) [↗](#)

Digital credentials & lifelong learning (unesdoc.unesco.org) [↗](#)

Union of Skills (2024) (commission.europa.eu) [↗](#)

Frameworks

Verifiable Credentials & Digital Identity (2024) - Verifiable
Credentials Data Model 2.0 (w3.org) [↗](#)

OpenID for Verifiable Presentations and Credentials
(OpenID4VC) (2024) (openid.net) [↗](#)

European Digital Identity Wallet – Architecture and Reference
Framework (2024) (eu-digital-identity-wallet.github.io) [↗](#)

Digital assets and tokens

Asset tokenization in financial markets: the next generation of
value exchange (2025) (reports.weforum.org) [↗](#)

“Trust technologies like verifiable credentials are the new invisible handshake of the digital age—empowering people and organisations to prove who they are and what they know, instantly and securely, at every interaction.”

- Adam Eunson, COO, AuvoDigital

IMPACT



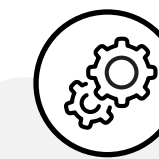
Education

- Learners gain greater control over their learning and career journeys with digital wallets, allowing them to manage and share trusted, verifiable achievements across contexts and borders. This shift enhances mobility, autonomy, and visibility.
- Educational institutions adopt new roles as issuers and validators within decentralised recognition networks, where formal credentials and purpose-driven tokens co-exist. This transformation supports modular learning pathways, personalised recognition, and broader stakeholder engagement, from employers to societal partners.



Research

- Decentralised reputation models and token-based systems enable more transparent, collaborative ecosystems and new ways of crediting contributions. At a systemic level, eIDAS 2.0 and MiCA provide the legal foundation that enables interoperable, learner-centred ecosystems to emerge and scale.
- A future-ready education and research landscape, where trust, flexibility, and recognition are embedded, positioning individuals and institutions to thrive in a digitally connected world.






Operations

Streamlined processes, reduced administrative tasks, and automated processing of credentials will be realised thanks to interoperable and trustworthy data exchange.

TREND #2

More decentra- lisation of data ownership enabled by SSI solutions

Public Values

	Autonomy	Freedom of choice Independence Privacy
	Justice	Inclusion Equity Integrity
	Humanity	Social cohesion Meaningful contact Well-being Safety Personal development Respect

Maturity

WATCH

PLAN

ACT

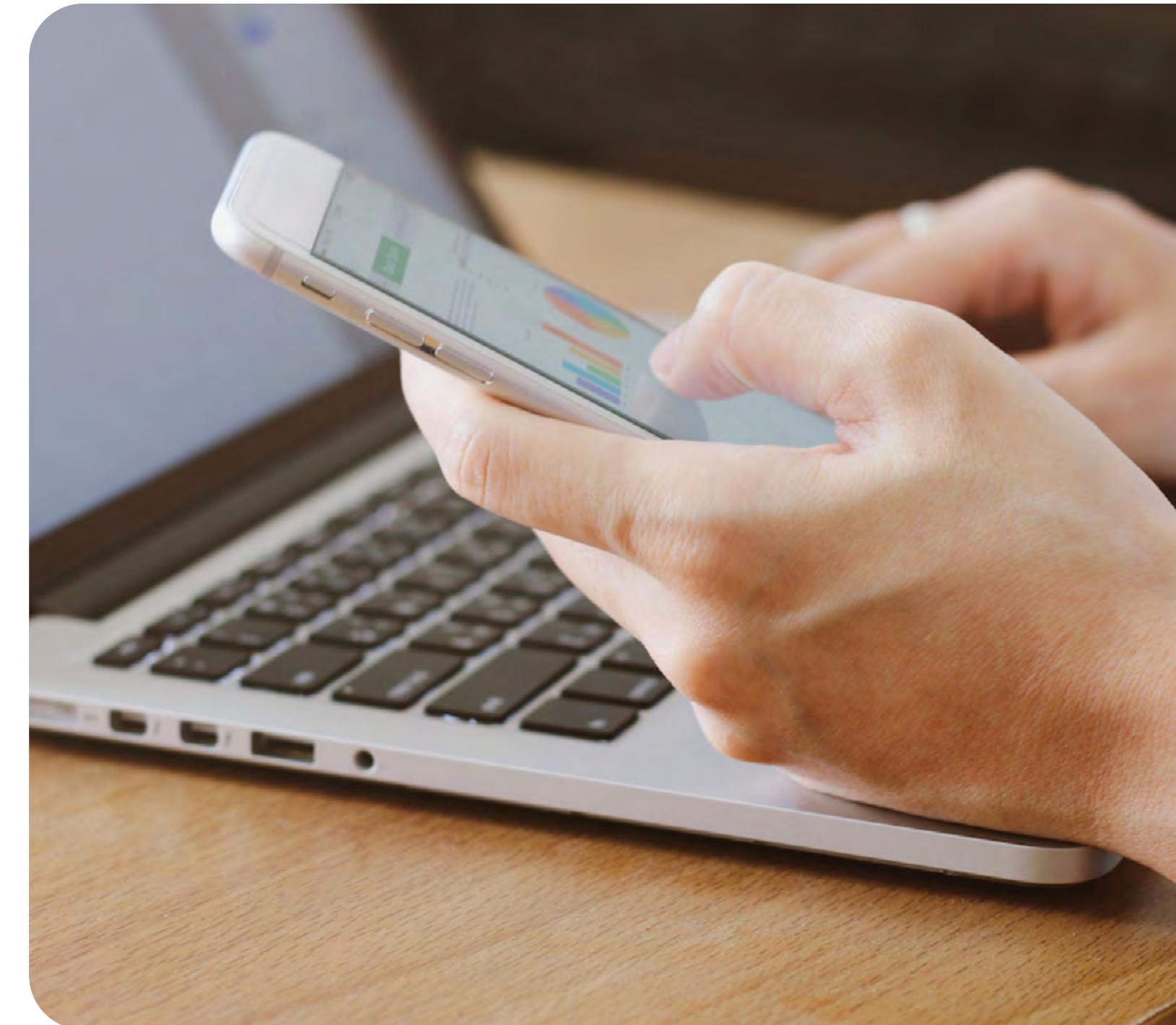
Drivers

Individualisation & Empowerment; Cybersecurity & Trust; Digital Transformation; Community Dynamics and Social Cohesion

The increasing value of personal data has led to misuse by many actors in society, ranging from big tech to data brokers and even governments.

This has prompted a counter movement focused on user empowerment and data rights protection. In the digital trust and identity domain, this movement toward data decentralisation and related individual control is commonly referred to as Self-Sovereign Identity (SSI).

The core principles of SSI include data portability, data minimisation, and access to personal data. Fundamentally, SSI seeks to empower individuals and protect data rights, with the forthcoming EUDI Wallet being a typical SSI solution.



SIGNALS

The path to Self-Sovereign Identity

(lifewithalacrity.com) [↗](#)

eIDAS 2.0 Regulation - framework for digital identity and authentication

(digital-strategy.ec.europa.eu) [↗](#)

Higher Education and Scientific Research Act (NL)

(wetten.overheid.nl) [↗](#)

A digital ID and personal digital wallet for EU citizens, residents and businesses

(ec.europa.eu) [↗](#)

Data by the Source

(digitaleoverheid.nl) [↗](#)

IMPACT



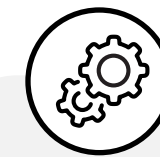
Education

Educational institutions issue credentials that require data storage for validation. Linking these credentials to individuals necessitates personal information, creating a challenge in designing processes that balance privacy and usability while promoting autonomous decision-making.



Research

The shift towards Self-Sovereign Identity (SSI) is transforming personal data management. It challenges researchers to adopt good practice and regulate systems that adhere to human rights and legal standards, are technically feasible and promote interdisciplinary research with significant social and policy impact.



Operations

- Overly simple user flows can lead to unconscious decisions and unintended data sharing, while excessive complexity can hinder usability. A balanced approach is essential. Tools based on Self-Sovereign Identity (SSI) principles can empower users to exercise their rights while meeting GDPR requirements.
- Empowering users reduces institutional control over issued credentials. Institutions must verify identities or wallets before issuing credentials, enabling users to share them across various sectors.

TREND #3

Emergence of organisational wallets

Public Values

 Autonomy Privacy

 Justice Integrity

 Humanity Safety

Maturity

WATCH

PLAN

ACT

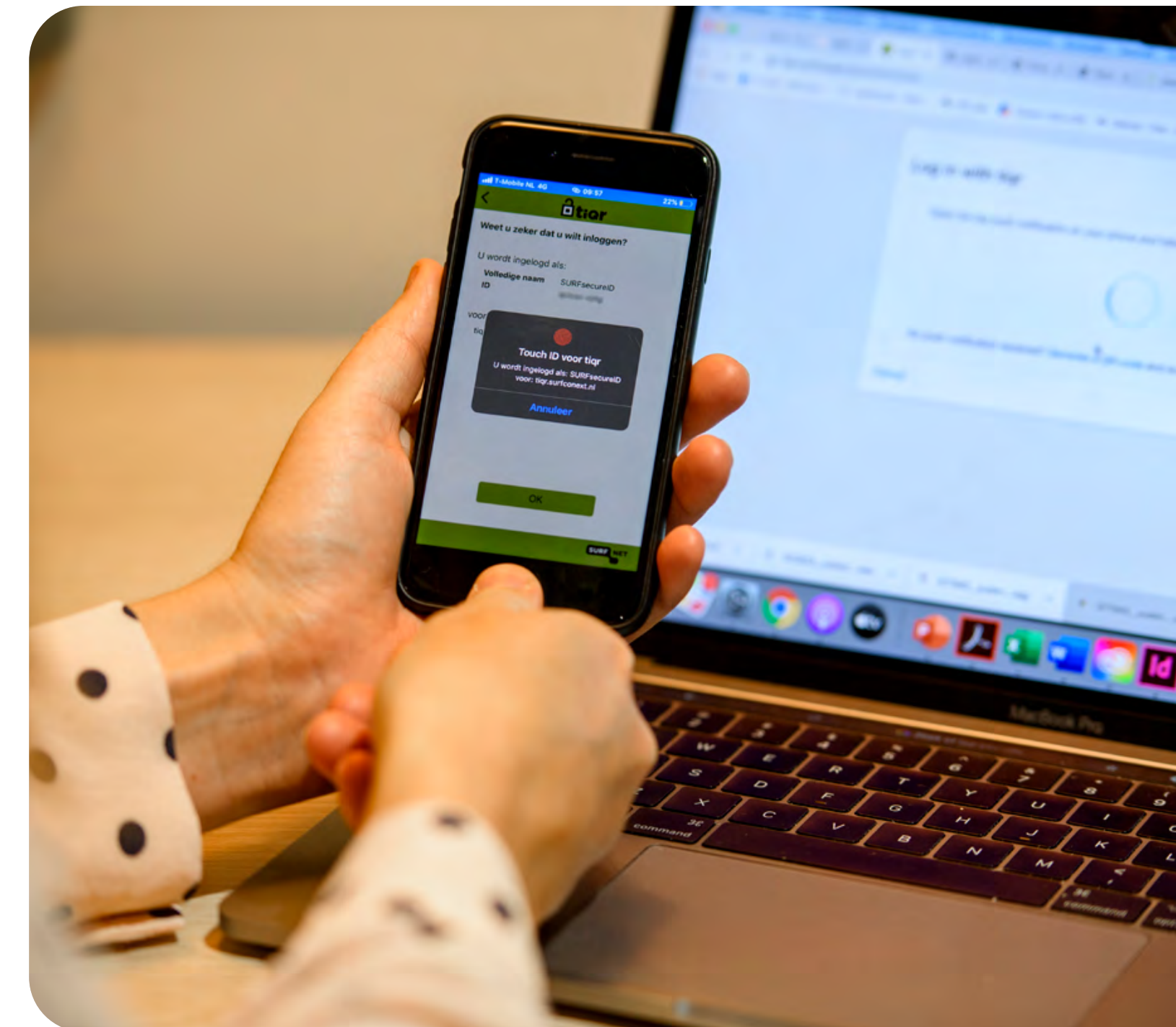
Drivers

Individualisation & Empowerment; Cybersecurity & Trust; Digital Transformation

Trust and interoperability issues have hampered business interactions across Europe. Announced in 2025, the European Business Wallet (EBW) initiative targets these inefficiencies with a unified, cross-border digital identity solution for organisations.

Organisational wallets are digital web-based wallets that provide secure digital identification, streamline data sharing, and facilitate legally valid notifications for companies and other legal entities. Unlike personal wallets, organisational wallets support multi-user access and role-based permissions (such as power of attorney).

One-click recognition of organisational identity, status, and attributes can prevent fraud (like fake websites or phishing) and compliance costs, as well as accelerate cross-border collaboration. Organisational wallets must address the complexities of legal entity identity, such as credential lifecycle management, international standards, and integration with business registers.



SIGNALS

Policy

EU Architecture and Reference Framework (ARF) ([github.com](#)) [↗](#)

European Business Wallet: digital identity, secure data exchange and legal notifications for simple, digital business ([ec.europa.eu](#)) [↗](#)

Use cases and experiments

Exploration of EU Digital Identity Wallets for legal entities with Company Passport and iSHARE ([coe-dsc.nl](#)) [↗](#)

EU large scale pilots with wallets for businesses ([digital-strategy.ec.europa.eu](#)) [↗](#)

“As the European Union moves toward full implementation of the EU Digital Identity Wallet (EUDI), businesses must prepare for a digital transformation in how identities are verified, customers are onboarded, and e-signatures are done.”

- Signicat ([signicat.com](#))

IMPACT



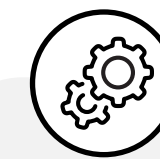
Education

- Educators and students should benefit from a significant reduction in administrative delays with international exchanges/mobility programs such as Erasmus+, and cross-border teaching or study opportunities.
- Secure, verified institutional credentials enable quick and trusted confirmation of enrolment, qualifications, and affiliations for internships, further studies, or collaborations.
- Reduced exposure to phishing and fraudulent communications enhances trust and digital safety in academic correspondence and protects personal and institutional information.



Research

- Reduced risk of impersonation or fraudulent collaboration requests safeguards intellectual property and project research credibility.
- Verified institutional identities should accelerate the establishment of cross-border collaborations, joint funding applications, and consortium agreements.






Operations

- Instant verification of institutional identity will enable faster execution of information exchange in European public-private partnerships and research collaborations, reducing administrative workload.
- Role-based digital access and trusted official communications strengthen security by reducing phishing risks, ensuring legal validity, and it also lowers compliance costs through secure, verified information exchange.
- Integration with internal systems streamlines credential checks and approvals, improving efficiency and optimising processes, although initial investment in staff training and technological infrastructure will be required.

TREND #4

Push for transparent supply chains with digital product passports

Public Values

	Autonomy	Freedom of choice Independence Privacy
	Justice	Inclusion Equity
	Humanity	Social cohesion Meaningful contact Well-being Safety Personal development Respect

Maturity

WATCH

PLAN

ACT

Drivers

Compliance and Regulation; Cybersecurity & Trust; Digital Transformation

The EU Ecodesign for Sustainable Products Regulation (ESPR) came into effect in mid-2024. This regulation mandates companies to disclose information regarding the origin of their products and their environmental impact. This mandatory implementation of digital product passports (DPPs) ensures that product data is authentic, reliable, and compliant.

Implementing DPPs will be challenging, and production and product data must be verified and accessible via a data carrier. Legislative developments will impact standardisation and DPP service providers.

While acts are being finalised, European standardisation bodies are developing the standards for DPPs for adoption by the beginning of 2026.



SIGNALS

Ecodesign for Sustainable Products Regulation

(commission.europa.eu) [↗](#)

Centre of Excellence for Digital Product Passports

(coe-dpp.nl) [↗](#)

Data Sharing – Digital Product Passport (tno.nl) [↗](#)

Position paper of Fides (formerly Dutch Blockchain Coalition)
about trusted DPPs (fides.community) [↗](#)

“Digital Product Passports will become the main reporting vehicle for all product related compliance information in the European Union. Companies that go beyond compliance and adopt the DPP at the center of their supply chain information ecosystems will see significant additional benefits.”

- Yvo Hunink, Founder of Regen Studio and co-writer of the position paper on trusted Digital Product Passports

Use cases & pilots

Demonstration of functioning DPPs in different sectors

(cirpass2.eu) [↗](#)

Digital product passports: Lessons from an early adopter
(British womenswear brand Nobody’s Child)

(voguebusiness.com) [↗](#)

IMPACT



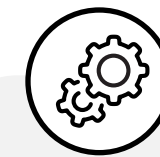
Education

- Different schools and universities are already discussing the possibilities of using DPPs, the associated challenges with using DPPs, and are working on prototypes.
- Students are and can research sustainability effects, suitable business models, and the technical (in)capabilities involved with the deployment of DPPs.



Research

DPPs can also be relevant for research and datasets, especially in areas related to sustainability, IT, product lifecycle analysis, and supply chain transparency.



Operations




- Educational institutions can minimise their environmental impact and enhance procurement and campus management.
- Although not required to comply with the Corporate Sustainability Reporting Directive (CSRD), many institutions are proactively selecting sustainable products and partners.
- The DPP will improve procurement, increase transparency, and enhance real estate management, enabling campuses to make informed, sustainable choices.



TREND #5

Digital Trust Frameworks: from hierarchical to distributed trust

Public Values

	Autonomy	Freedom of choice Personal empowerment Independence Privacy
	Justice	Inclusion Equity Integrity
	Humanity	Social cohesion Meaningful contact Well-being Safety

Maturity

WATCH

PLAN

ACT

Drivers

Individualisation & Empowerment; Cybersecurity & Trust; Digital Transformation

Much of the trust we place in credentials comes from verification by authoritative sources; we cannot rely solely on a person's own claim. This is why educational institutions are considered authoritative when issuing diplomas and credentials. Institutions must verify that the individual attended courses or examinations, and the institution itself must be verifiably accredited.

Current trust frameworks that support this system are largely hierarchical. New standards, such as OpenID Federation, enable non-hierarchical trust, complementing existing identity federations and allowing for more independent collaborations.

However, this does not eliminate the need for trust. Authorities are still required for accrediting institutions and credentials. Additionally, when processes demand a high level of trust, further technical checks and organisational rules and regulations are necessary.



SIGNALS

OpenID Global Standards

OpenID Federation 1.0 specification (openid.net) [↗](#)

OpenID API specification for the issuance of verifiable credentials (openid.net) [↗](#)

Identity federations in practice

OpenID Connect Federation: How to build multilateral federations using OIDC (indico.geant.org) [↗](#)

Identity federations and inter-federation eduGAIN (wiki.geant.org) [↗](#)

EduGAIN OIDC pilot (indico.cern.ch) [↗](#)

IMPACT



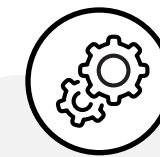
Education

The role of institutions in the education data ecosystem is evolving, and requests for data and access to tools come from both within and outside of the ecosystem. Therefore, establishing trust in credential authenticity will become more challenging.



Research

The EU Digital Identity framework's influence on the adoption of digital wallets in research and education, and its effects on trust frameworks, is subject to ongoing research.



Operations

Institutions must determine how credentials can be reliably attributed to individuals. This requires identity verification at enrolment, during assessments and perhaps even attendance.



SURF Utrecht

**Hoog Overborch Office
Building** (Hoog Catharijne)
Moreelsepark 48
3511 EP Utrecht
+31 88 787 30 00

SURF Amsterdam

Science Park 140
1098 XG Amsterdam
+31 88 787 30 00

futuring@surf.nl
www.surf.nl/en