FIDES.

Accelerating
Digital Trust

2024

Position Paper

Trusted Digital Product Passports

WITH CONTRIBUTIONS FROM

TNO

quintessence research

Warren Brandeis

sphereon

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

wipro

GS1 Nederland

UNIVERSITY OF APPLIED SCIENCES UTRECHT

Dutch Blockchain Coalition
connect and create

CREDENCO

REGEN STUDIO
Pioneering Innovations
for Ecosystem Regeneration

CMS
law·tax·future

Do you support the conclusions in this report?

Consider giving your support to:

FIDES.COMMUNITY

CONTENTS

CLICK THE ARROW
TO GO TO THE CHAPTER

Summary

The transition to sustainability and circularity presents organisations and governments with new challenges, such as complex supply chains, fraud, and disruptions. This position paper highlights the essential role of Digital Product Passports (DPPs) as tools to address these challenges. The European Ecodesign for Sustainable Products Regulation (ESPR) serves as a significant legal foundation for the implementation of DPPs.

In this document, we outline a vision and strategy for the development of Trusted Digital Product Passports (tDPPs). These tDPPs are digital systems designed to share reliable and verifiable information about a product throughout its lifecycle. They are designed according to open, decentralised, and permissionless architectures, where self-sovereign digital identities for individuals, organisations, and objects form the core. The goal is to keep data as transparent, secure, and accessible as possible for all stakeholders, with protections in place where necessary. This strengthens digital trust, supports the circular and sustainable value chain, and contributes to a fair environment where concentrations of power are prevented. tDPPs can also enable the development of new business models that go beyond regulatory requirements.

Three strategic horizons have been established to achieve tDPPs. Until 2027, the focus is on interoperability, standardisation, and compliance. Until 2030, the emphasis shifts to fully integrating decentralised digital identities for (legal) entities. From 2030 onwards, the focus will be on creating added value that exceeds legal requirements, introducing autonomy by considering the tDPP as the digital identity of an object and allowing self-organising ecosystems to form around it.

This paper also presents criteria for the relevance of tDPPs to clarify that extensive tDPPs are particularly beneficial in specific contexts, such as long lifespans, strong sustainability claims, or fraud prevention. These criteria assist in identifying product groups for which tDPPs can add significant value, especially in highly regulated sectors or where complex stakeholder involvement is essential.

A set of use cases has also been outlined, with scores based on the need for trust according to the criteria, connectedness, and ecosystem readiness to act. This analysis identifies the vehicle passport as the most urgent case. Other product groups, such as batteries, buildings, textiles, computers, aluminium, hydrogen, and bioethanol, offer significant potential to expand the adoption of tDPPs, particularly in sectors with strong regulatory requirements and increasing sustainability goals.

In designing tDPP architectures, a balance must be struck between decentralised components for resilience, transparency, and security, and centralised components for simplicity and cost-effectiveness. The degree of decentralisation should align with complexity, user requirements, and regulatory needs. The success of tDPPs, especially in complex ecosystems, depends on a workable, open, and permissionless architecture that supports inclusion and verifiable data. The greatest challenge for a scalable, trusted DPP ecosystem is interoperability.

Collaboration is crucial for the development of tDPPs. Promoting interoperability through open standards and shared experimental spaces accelerates adoption. Bringing together the ecosystems of digital identities and DPPs is essential, but this is only possible with broad-based collaboration. Initiatives like FIDES facilitate this collaboration by creating a neutral environment where knowledge sharing, interoperability, and innovation are central.

Introduction

The necessity for sustainability and circularity is undeniable, and this has also heightened the demand for transparency and trust in information. Europe has recognised this trend by introducing the concept of Digital Product Passports (DPPs) via the Ecodesign for Sustainable Products Regulation (ESPR). A standardisation process for DPP systems has also been initiated, involving European and national standardisation organisations, aiming for completion by the end of 2025. Within this framework, however, system providers still have significant design choices.

In this position paper, we argue that DPPs should be designed with a foundation in digital trust, and we outline design possibilities with a focus on interoperability. We present a vision around which we hope to form an ecosystem of DPP stakeholders who, based on this vision, can establish a trust architecture leading to Trusted Digital Product Passports (tDPPs). Standards from the domain of decentralised digital identities, applicable to individuals, organisations, and objects, provide a powerful basis in this context.

Our starting point is the intrinsic drivers and a forward-looking vision on trust networks, where distributed power and control play a significant role. We explore various architectural scenarios within the DPP ecosystem that aim to prevent the centralisation of power and ensure interoperability between DPP systems. Additionally, we propose several applications that we consider promising as starting points for development. This shared position demonstrates consensus among the signatories and provides a foundation for standardisation discussions and future interoperability agreements.

"In this Position Paper we argue that DPPs should be designed with the value of Digital Trust in mind and will we discuss what this means for architecture choices."

CHAPTER 1

Drivers for DPPs

WRITTEN BY
Arno Laeven | CEO at Warren Brandeis
Jorn Fokkens | Change Lead & Business Development at Wipro
Yvo Hunink | Lead Digital Product Passports at Dutch Blockchain Coalition and Founder of Regen Studio

The landscape of supply chains is moving towards DPPs because of intrinsic drivers in the market. In this chapter, we look at some of the most important drivers.

Complexity of Supply Chains

In the 21st century, the creation of a final product involves a complex journey through a long chain of suppliers. This chain, commonly known as the supply chain, includes carriers, warehouses, and other service providers operating worldwide. What further complicates this chain is that each participant increasingly stores digital data in their own databases, leading to a widespread and decentralized setup. This decentralization implies that product and service suppliers operate independently, often resulting in limited visibility across the entire chain.

Increase of Digital Data

The volume of digital data stored continues to increase, especially to comply with new EU regulations. When accessed correctly and trusted, this data can be used not only to optimize the supply chain but also to reveal key information such as CO2 emissions for ESG (Environmental, Social, and Governance) purposes. Digitization can play a crucial role here, reducing paperwork and creating reliable digital passports for products are essential to make this feasible.

Disruptions and Resilience

Supply chains are not immune to disruptions. The COVID-19 pandemic demonstrated how vulnerable and costly disruptions can be. But it is not only pandemics that disrupt supply chains. Climate change, geopolitical tensions, wars, and blockades also have a massive impact on the availability of raw materials and goods. A ship unable to unload due to missing paperwork, or the recall of products with manufacturing defects, are just a few examples of issues that may arise. These challenges highlight the need for better insight and resilience in the supply chain, where DPPs can be of help.

Preventing and Detecting Fraud

Many businesses and consumers face fraud, be it with counterfeit products, sustainability claims by suppliers, or warranty fraud. DPPs could become a vehicle to counter or at least reduce such forms of fraud. The ESPR (Ecodesign for Sustainable Products Regulation) also requires that a DPP includes information on ways to verify the authenticity of a product. Additionally, digital safeguards can record critical points in the product life-cycle, such as the date of sale to the customer. The DPP system thus provides a foundation to prevent misuse.

Responsibility and Sustainability

Alongside supply chain managers, the sustainability department also plays a critical role. The demand for reliable, real-time data is growing, driven by organizations' ambitions to become climate-neutral and increasingly strict laws and regulations. Organizations struggle with how to comply with these requirements, achieve their sustainability goals, and protect their reputations. For example, the energy sector has a high demand for traceability throughout a product's life cycle. "Verifiable Responsible Sourcing" is becoming increasingly important for both producers and legislators, as society increasingly demands that materials be responsibly sourced, free of child labour, and sustainably produced. A digital passport for products, linked to a reliable verification system, can help here. These passports allow for availability and approval by multiple authorities without creating new power structures.

Business Case

There is a strong business case for DPPs. Every major company wants to plan efficiently, which works best with reliable, verifiable digital data that is accessible at any time. Legislators, society, and regulatory bodies want environmental and quality standards to be validated efficiently and digitally. Thus, a DPP can become the "one-stop-shop" for a product, serving consumers, suppliers, logistics, storage, and legislators. Once this foundation is established, scalability is just a small step away, and a DPP can lead to significant simplification of processes. An analysis by Wipro, regarding their DPP solution, estimated that organizing work around DPPs could save about 20% of man-hours. Not only is there a business case in terms of efficiency, but also in prevention, such as preventing more products than necessary from being returned during a recall.

Standardisation

Standardization is another key driver for DPPs. Manufacturers often request the same information from their suppliers but in slightly different ways. Harmonization and standardization make the industry more efficient. On top of that, European standardization requires further specifications to ensure extensive interoperability. This standardization should also work across sectors with as many systems as possible in a flexible way. Thus, DPPs act as a vehicle to achieve extensive standardization across global supply chains, creating a uniform picture that allows consumers to compare products.

Conclusion on drivers for DPPs

The intrinsic drivers for DPPs in supply chains are complexity, the rise of digital data, the need for resilience during disruptions, combating fraud, standardization, the business case, and increasing demands around sustainability and responsibility. Transparency and trust are now more important than ever to achieve circularity, and this can be realized with a trusted DPP by embracing complexity and ensuring interoperability.

While the implementation of DPPs is driven by clear advantages for businesses, such as cost savings and process optimisation, legislation currently plays the most significant role in DPP adoption. European regulations, such as the ESPR, are pressuring companies to swiftly transition to digital product passports. The combination of intrinsic drivers and regulation makes the use of DPPs inevitable for businesses that want to be prepared for a future where transparency, accountability, and resilience are central. Only in this way can companies equip themselves to face the challenges of today and tomorrow and successfully navigate the uncertainties of an ever-changing world.

The biggest driver is not intrinsic of nature, but are the laws and regulations being formed in Europe.

"Transparency and trust are more important than ever for circularity and with a 'Trusted' DPP this can be reached, by embracing complexity and ensuring interoperability.."

CHAPTER 2

Laws & Regulations

WRITTEN BY:
Akin Aslan of CMS

"The Commission plans to establish around 30 delegated acts between 2024 and 2030."

Legal Basis of DPPs

DPPs find their legal foundation in the information requirements set forth by the Ecodesign for Sustainable Products Regulation (ESPR). This legislation defines the concept of a DPP and establishes several fundamental system components. Based on this regulation, the European Commission (the "Commission") has the authority to set specific minimum requirements for products introduced to the European market through delegated acts. These requirements may pertain to sustainability and circularity, as well as social aspects.

Delegated acts establish what information must be included in DPPs and how it should be presented. Both information obligations and performance obligations may be set. The DPP is a mandatory component of a delegated act and can include further rules regarding technical or governance aspects, such as processes, structures, and guidelines for validating and verifying the information. This may include guidelines for data sharing, the roles of various stakeholders in the DPP ecosystem, and the responsibilities each holds.

The Battery Act is one of the first pieces of EU legislation to introduce the DPP, serving as a model for how such delegated acts may look. The regulation establishes DPP requirements for certain types of batteries, mandating detailed information on the producer, battery composition, carbon footprint, expected lifespan, and performance. The Global Battery Alliance, comprising representatives from the battery sector, has published a 'Battery Passport Content Guidance,' providing detailed content specifications for the battery passport.

In addition to batteries, risks have been identified in several other product categories, prompting the Commission to likely issue delegated acts for these as well. Textiles, building materials, electronic products, and chemical materials are among those expected to fall under such regulations. The Commission plans to establish a total of 30 delegated acts between 2024 and 2030. A project group has already been established for textiles to begin designing the necessary regulations.

DPP Deployment for Compliance with Other Legislation

Besides being mandatory under delegated acts based on the ESPR, DPPs can also help companies comply with obligations from other reporting-focused legislation. One example is the Corporate Sustainability Reporting Directive (CSRD), which mandates certain companies to report on the negative impact of their activities on people and the environment. Beyond the CSRD, there are the Deforestation-free Product Regulation, the Forced Labour Regulation, and the Critical Raw Material Act, which impose obligations on certain companies to monitor their supply chains and report the origin of their products. DPPs may also assist in implementing the Carbon Border Adjustment Mechanism (CBAM), for instance, to automate import tariffs based on reliable emissions data.

Influence of Conditional Legislation

Various laws and regulations impact the design requirements for DPPs, thus establishing prerequisites. The electronic Identification, Authentication and Trust Services regulation (eIDAS2) provides a trusted framework for electronic identification and authentication of persons and organizations. DPPs can utilize eIDAS-based services for identity verification and authorization to ensure authenticity. Additionally, eIDAS requires security standards for electronic transactions and services, enhancing the protection of DPP information from misuse, which is critical for building trust in DPPs.

The General Data Protection Regulation (GDPR) contains rules on personal data processing. As DPPs and related information may contain personal data, such as that of the manufacturer, technician, or certifying authority, DPPs must comply with GDPR. Practically, this necessitates a consent system and selective access based on attributes. The EU Data Strategy focuses on creating a European “Data Space” to promote data sharing, stimulate innovation, and boost competitiveness. The Data Governance Act sets rules for data sharing and management within the EU, ensuring trust, interoperability, and control over personal data. Both initiatives aim to enable a digital single market where data can flow freely while protecting individual and organizational rights

> “The electronic Identification, Authentication and trust Services regulation (eIDAS2) gives a framework that guides the design of trust networks around DPPs.”

European Standardisation Request

Under standardization law, the Commission has the authority to request standardization from European standards organizations. It has exercised this authority, requesting standardization within the ESPR and DPP context. As a result, the Joint Technical Committee 24 (JTC24) has been organized by CEN/CENELEC, led by Germany. This committee aims to produce a standard of a technical system for DPPs by the end of 2025. This standard will subsequently be referenced in future delegated acts. According to the ESPR, deviation from the standard framework after its introduction in a delegated act is only allowed if there are valid reasons to do so.

The standardization request is divided into different modules: 'identification numbers, data carriers, access rights, interoperability, data formats, data storage, data reliability, and APIs.' Some contributors to this position paper, being TNO, Quintessence, and Regen Studio, are active in the JTC24 working groups. These working groups use a list of pre-supplied standards by the European Commission, which includes many decentralized foundational building blocks from the FIDES ecosystem. Much uncertainty remains about the extent to which the standard can reconcile the many interests and variations of DPPs already on the market and whether interoperability can be achieved without significant trade-offs in other areas like privacy and security.

Conclusion on Laws & Regulations

Together, these elements form a legal framework for DPPs, with the delegated acts under the ESPR as the basis for DPP implementation. Reporting legislation, including the CSRD, further gives incentive for DPP use, and other EU data and privacy regulations, like eIDAS2, provide additional guidance.

The EU standardization of DPPs allows for the integration of existing building blocks within the FIDES ecosystem, fostering a robust trust architecture. The standard will likely still contain gaps that need addressing for full interoperability, and further specification will be required.

"Deviating from the in 2025 published European standard for delegated acts will only be possible if valid reasons exist for that."

CHAPTER 3

Vision on Trusted DPPs

WRITTEN BY
Yvo Hunink | Founder of Regen Studio and lead DPP bij DBC
Peter Nobels | Senior Business Consultant at Utrecht University of Applied Sciences
Helmer van Merendonk | Projectleider Web3 Hub at Utrecht University of Applied Sciences
Arno Laeven | CEO at Warren Brandeis
Eelco Klaver | CTO at Credenco
Jorn Fokkens | Change Lead & Business Development at Wipro
Maarten Vergouwen | CIO at GS1 Nederland
Niels Klomp | CTO at Sphereon
Sjoerd Rongen | Consultant Smart Industry at TNO

Now that we have a clear view of the intrinsic drivers for DPP adoption and how European legislation acts as an extrinsic driver, we can outline a vision for the future role of DPPs in our world.

The transition to a sustainable and circular economy presents challenges that traditional systems can no longer solve. The increasing complexity of supply chains, the growing demand for transparency, and the need to ensure trust in an increasingly digital world require a new approach. Digital Product Passports offer a promising solution, but their full potential is only realised when they are designed as decentralised, permissionless systems with a certain degree of digital autonomy built into the object. In other words, the object must have an independent digital right to exist so that it continues to function even if the surrounding organisations cease to operate. In this chapter, we explain why this approach is crucial for establishing 'Trusted DPPs' (tDPPs) and how they can contribute to a future where power in the supply chain is more evenly distributed, and interoperability remains safeguarded.

Beyond the Boundaries of Traditional Systems

Traditional, centralized systems struggle with fundamental limitations in flexibility, resilience, and security. They are often ill-equipped to handle the complexity and unpredictability of product life cycles, especially when products are recycled or reintroduced into the circular economy. Furthermore, power tends to concentrate in the hands of a limited number of entities, which can lead to monopolies and undermine the system, eroding trust within the network. In establishing tDPPs, these systems must be integrated, but actors who were previously unable to participate in the information chain should be able to contribute independently to the reliability of the information. This requires a certain level of openness and transparency regarding data and process control. This approach not only increases the resilience and security of the system but also strengthens the sovereignty of all parties involved. As a result, parallel trust networks can form around the DPP, which essentially acts as an autonomous digital representation of the object—a digital identity for the product that sits at the centre of the trust network.

Decentralized, Permissionless Architectures as a Basis for Digital Trust

When designing tDPPs, we view open, decentralized and permissionless architectures as the most desirable solution, especially when reliance on a single party is undesirable or when there is a lack of trust among supply chain partners. But what exactly does "decentralized" mean? This concept extends beyond decentralized storage alone. Decentralization can be considered from various aspects, such as management, decision-

making, financial model, verification methods, or authorization and identification. Given the complex and intertwined nature of supply chains, there are few cases where all elements can be managed by a single organization. Therefore, we adopt the design principle: decentralized, unless. Permissionless means having unrestricted access to view and perform transactions around the DPP. While this may not be possible for every data point, it is important in DPP governance to prevent monopolies and cartels, which can only be achieved if influence is open to all. Since decentralized, permissionless systems are more challenging to establish, in some cases, a centralized setup might be chosen. In Chapter 6, we outline some product characteristics where this approach becomes more necessary.

Digital Identities as a Foundation

A cornerstone of tDPPs is the use of self-sovereign digital identities. This decentralized and permissionless form of digital identities can be applied to individuals, organizations, and products, enabling them to participate securely and in a verifiable way in digital ecosystems and build their own trust networks. For individuals, this means having full control over their data while still being able to share it in global networks. For organisations, it offers the ability to collaborate with other parties in a trusted manner without being entirely dependent on a central authority or an excess of paperwork. The concept of digital identities for products allows for the creation of a digital identity for objects, even for digital entities like algorithms. This enables the complete history of a product to be transparently and reliably recorded by hundreds of actors, even if they are not part of the same chain. This combination of identity forms enables a broadly interoperable trust network and allows product designers to make DPPs programmable, facilitating advanced automation such as releasing funds upon proven recycling, linking independent audits, or implementing attribute-based access to information. For example, a mechanic replacing a part in a car could register this action in the DPP. There are also practical reasons to link these identity standards to DPPs, as they play a role in the European movement around eIDAS2, such as in the development of the European Digital Identity Wallet and the Large Scale Pilots associated with it.

More than a Passport

Current legislation approaches the DPP mainly as a passport—a minimal set of information that must be available to the consumer to meet established requirements. While this is a good starting point, it also carries risks and results in missed opportunities. Think about yourself: you are much more than just a passport and the data it contains. Although that data is sufficient for travel, it does not fully represent you. Imagine if we could only share the information from our passport on the internet. The internet would look very different. The same comparison applies to products. By designing a centrally organized DPP, where only a few parties determine what a product passport should contain, we not only create incentives to keep supply chains opaque but also limit the autonomy and creativity of the product's digital representation. Looking beyond compliance allows for the potential to add, adapt, or innovate additional societal value.

Trusted Digital Product Passports

Various types of DPPs are emerging, such as 'Decentralized DPPs,' 'Tokenized DPPs,' and 'Verifiable DPPs.' However, we believe these terms do not fully capture what a DPP should provide to ensure digital trust. Therefore, we introduce the term 'Trusted DPPs' (tDPPs). We do not see this as a standalone concept; rather, we view it as encompassing the other DPP types. tDPPs are typically decentralized and verifiable, allowing us to look beyond just the technical foundations.

Trustworthiness and trust are distinct concepts often confused. In the vocabulary of ISO/IEC standards, 'trustworthiness' is defined as "the ability to meet stakeholder expectations in a verifiable and demonstrable way." This means that trustworthiness revolves around measurable performance and consistently meeting agreements, forming the basis for building stakeholder trust objectively. Key characteristics for trustworthy systems include availability, reliability, controllability, resilience, security, privacy, transparency, integrity, authenticity, quality, usability, and accuracy. With attention to all these characteristics, the likelihood of a system being trusted increases.

In contrast, the concept of 'trust' also includes subjective feelings such as satisfaction, comfort, and comprehensibility. While trustworthiness is mainly measurable and verifiable, trust relies on perception, experience, and acceptance by users. Both aspects are essential to the success of DPPs but need to be approached and integrated differently into tDPP design principles. For example, if trust in the company were compromised, it could directly impact trust in the DPPs, even if the DPP adheres to all rules. This extends beyond technology, data, services, and products, encompassing ecosystem governance, so that actors can be held accountable. Open, decentralized, and permissionless systems can foster this trust, but are not sufficient. Moreover, the tDPP must have extensive interoperability, allowing it to fit within and between supply chains in various contexts. Therefore, an ecosystem approach is crucial to the success of tDPPs.

While the ESPR emphasizes measurable trustworthiness, subjective trust is less addressed. The assumption is that compliance with all rules will automatically lead to consumer trust, which is not always the case. A tDPP must go beyond mere legal compliance and focus on added value for users. Integrating open decentralized, permissionless economic structures on top of DPPs could also help foster this type of trust by rewarding users for desired behaviour. This requires viewing the DPP as the digital identity of an object, with a degree of digital autonomy, allowing various entities to interact with it independently and enabling a self-organizing ecosystem capable of adapting to real-world complexity.

In summary, a tDPP can be described as:

- Built from open, decentralised, and permissionless structures for identity, verifiability, and governance.
- The result of interactions between digital identities for individuals, organisations, and objects.
- Integrating interoperable building blocks that enable use within and across supply chains.
- An evolution of DPPs towards autonomous digital objects that facilitate self-organising complex ecosystems.
- Moving beyond compliance, adding extra value for users.

Conclusion of the Vision

Where trust at scale is essential, where there is no complete overview of the supply chain, where stakeholders involved in the future are hard to predict, where these parties have both shared and conflicting interests, and where no clear centre of trust justifies centralization, Trusted DPPs (tDPPs) provide a solid foundation for DPP design. This is generally the case for the complex network of supply chains.

A tDPP is typically an open ecosystem with decentralized and permissionless structures for technology, data, and processes. It is essential to integrate building blocks of self-sovereign digital identities for individuals, organizations, and objects to facilitate trust networks around the DPP. Additionally, the tDPP focuses on extensive interoperability within and beyond its own chain. The DPP must also have a certain degree of digital autonomy built in, to allow the self-organisation of complex trust networks. Finally, the tDPP looks beyond compliance, addressing the subjective aspects of trust by focusing on added value for end-users. This makes the system more resilient to abuse of power, more democratic, reliable, and easier to adopt in complex ecosystems. Designing with this vision in mind today can bring that future closer to reality.

However, the question remains: How do we get to Trusted DPPs?

Next chapter describes the steps we want to take to reach the implementation of tDPPs.

CHAPTER 4

Strategic Horizons

WRITTEN BY

Yvo Hunink	| Lead DPP at Dutch Blockchain Coalition and Founder of Regen Studio
Peter Nobels	| Senior Business Consultant at Utrecht University of Applied Sciences
Helmer van Merendonk	| Projectleider Web3 Hub at Utrecht University of Applied Sciences
Arno Laeven	| CEO at Warren Brandeis
Eelco Klaver	| CTO at Credenco
Jorn Fokkens	| Change Lead & Business Development at Wipro
Maarten Vergouwen	| CEO at GS1 Nederland
Niels Klomp	| CTO at Sphereon
Sjoerd Rongen	| Consultant Smart Industry at TNO

With a clear vision of the future, we can set milestones to guide our journey forward.

This chapter introduces three horizons that serve as milestones in the evolution of tDPPs.

We start where the urgency of regulation is felt, with ecosystems ready to take action together to work on standards and interoperability agreements. Next, we integrate the broader trust network of digital identities for individuals, organizations, and objects. Finally, we bring identity to the object to capture value creation through autonomous tDPPs, helping society build trust in DPPs.

HORIZON 1 | until 2027

Interoperability, Standardisation & Compliance

The first horizon focuses on the period from 2025 until 2027, with an emphasis on meeting EU and international regulations. It is crucial in this phase to develop DPPs that meet the goals set by the Ecodesign for Sustainable Products Regulation (ESPR) and the resulting standardization that started in 2024. This includes designing and implementing architectures aimed at interoperability between DPP systems and contributing input to EU standardization committees to ensure compliance with these architectures.

THE CORE ACTIVITIES IN THIS HORIZON ARE

- Forming and guiding DPP ecosystems around relevant use cases that feel the urgency to engage with the topic due to regulation.
- Promoting (applied) research on tDPP ecosystems within these use cases.
- Developing a specification profile for tDPP interoperability to prevent the formation of silos.
- Participating in European standardization and ensuring that desired interoperability agreements are achievable within the standard.
- Establishing an international hub of knowledge around DPPs, bringing together like-minded parties to tackle shared challenges through events and working groups.

HORIZON 2 | until 2030

Trustworthiness by integrating with Digital Identities

The second horizon, aimed at the period starting from 2027, further expands the DPP concept by fully integrating digital identities for individuals, organizations, and objects. These identities form the basis for a broader ecosystem of digital trust. The goal is to enable distributed identification, authentication, and authorization, allowing different actors to work together securely and in a verifiable way and to contribute to the DPP without a central authority managing access. This will require techniques such as attribute-based access control, zero-knowledge proofs, and other privacy-enhancing technologies.

THE CORE ACTIVITIES IN THIS HORIZON ARE

- Connecting DPPs with ecosystems that design wallets, identifiers, and credentials for individuals and organizations and integrating these systems.
- Taking a comprehensive approach to use cases where digital identities for individuals, organizations, and objects play a critical role in forming a trust network.
- Conducting experiments within and between use case ecosystems to test the interaction between tDPPs and digital identities in practice.

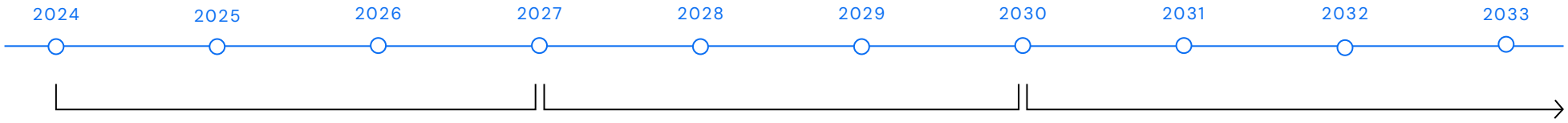
HORIZON 3 | from 2030

Trust through New Value Creation and Autonomy

The third horizon looks further into the future, beyond 2030, where digital objects can gain full autonomy, allowing society to organize around them. This means that products and materials, as well as digital entities such as data, content, or algorithms, will eventually have a DPP that enables them to perform automated actions independently. This phase opens up new possibilities for value creation, where DPPs play a role not only in compliance and transparency but also in supporting self-organizing ecosystems. This can serve as a foundation for autonomous vehicles or automated drone delivery, while also embedding incentive models for recyclable materials that can be activated independently at the end of the chain without the producer's involvement.

THE CORE ACTIVITIES IN THIS HORIZON ARE

- Building architectures for digital identities of objects that allow autonomous operations around the DPP without intervention.
- Developing governance systems that support self-management and peer-to-peer interactions, facilitating ownership and value creation in a distributed way.
- Testing new business models and value creation for end users that help foster adoption and trust in tDPPs, thus making circularity a reality.



HORIZON 1

Interoperability, Standardisation & Compliance

HORIZON 2

Trustworthiness by integrating with Digital Identities

HORIZON 3

Trust through New Value Creation and Autonomy

Conclusion on the Strategic Horizons

Following these horizons is not merely a technological necessity but a strategic choice that is fundamental to realizing the full potential of DPPs. Each horizon represents an essential step in the evolution of trusted digital product passports, where the focus shifts from compliance and standardization to the integration of digital identities, and ultimately, to value creation through autonomous digital objects. This horizon-based approach offers a framework for the strategic development of DPPs and forms the foundation for the scenarios and criteria discussed in the following chapters.

CHAPTER 5

Criteria for the relevance of Trusted DPPs

WRITTEN BY

Helmer van Merendonk | Projectleider Web3 Hub at Utrecht University of Applied Sciences
Arno Laeven | CEO at Warren Brandeis
Yvo Hunink | Lead DPP at Dutch Blockchain Coalition and Founder of Regen Studio

Not all product groups are the same. And designing an open, decentralised, and permissionless system for tDPPs is not an easy path to take. Therefore, one might question whether it is necessary to set up such a permissionless system for every product. Does, for example, a pair of socks need its own digital identity?

In this chapter, we define the criteria that, in our view, make a product suitable for a tDPP, and how the relevance of these criteria increases the desirability of an open, decentralised, and permissionless approach.

Integrity of Data

Products intended for circular economic models benefit from a tDPP that tracks their life cycle along the commonly used 'R-ladder', making accurate and accessible data available to all future contributors, even those who cannot yet be predicted.

High Value Retention

Products with significant economic or societal value are ideal candidates for tDPPs, particularly when ownership needs to be demonstrated and purchase value needs to be linked for resale as proof of value retention.

Intensive Maintenance

Products that require frequent or complex maintenance benefit from a tDPP where technicians can independently document and update maintenance records, potentially even autonomously. This reduces the administrative burden on stakeholders and provides insight into what changes have been made and who was responsible.

Modular Design

For products composed of interchangeable components, a tDPP can support dynamic configuration management, allowing seamless updates by part suppliers. For example, when replacing a battery in an electric vehicle, it becomes easy to link the DPP of the new battery to the vehicle.

Exclusivity and Uniqueness

Unique products, whether due to rarity or exclusive customization, require a tDPP that can verify and preserve their distinctive characteristics in all interactions and transactions, as well as ensure the secure transfer of ownership. The tDPP may also contain concealed information for a buyer, or providing specific instructions to verify authenticity.

Long Lifetime

Products designed for long-term use need a tDPP that can track their history, even as owners, companies, and technologies evolve, ensuring continuity and data trustworthiness while enabling ongoing economic interaction.

High Risk of Fraud

In contexts where there are incentives for misuse or where fraud is a concern, a tDPP provides decentralized assurance that all product-related data remains authentic, untampered, and traceable.

Susceptible to Theft

Products prone to theft benefit from a tDPP that can (autonomously) document usage history, discouraging misuse and aiding in the recovery of stolen items.

Strong claims

Products with strong claims on, for example, sustainability or responsibility require a tDPP that transparently documents their environmental and social impact, enabling verifiable and reliable reporting. These records should also be (automatically) adjusted based on new insights into emission values.

Highly Regulated

Products subject to strict regulation benefit from a tDPP that ensures compliance with diverse and evolving legal requirements and facilitates the integration of new circumstances.

Service Products

For products tied to services, a tDPP facilitates data management, improving efficiency and consistency among service providers.

Complex Multi Stakeholder Involvement

Products that involve many stakeholders throughout their life cycle are suited for a tDPP that transparently supports collaborative data management, reducing friction and enhancing trust among stakeholders.

Self Organising Ecosystems

Products designed to operate autonomously or within decentralized networks require a tDPP that enables independent decision-making and self-management of data exchange, aligned with their operational model. An example of this could be open-source code for an AI model, where contributions can be tracked and training datasets can be transparently verified

Conclusion on the criteria for relevance of tDPPs

This non-exhaustive list of criteria guides the selection of products for which tDPPs are used. Each criterion highlights specific product characteristics that enhance the value proposition of a tDPP, justifying the transition to an open, decentralized, and permissionless system, where digital autonomy of the product passport is safeguarded. When a product group meets even one of these criteria, it is suitable for tDPPs, with suitability increasing as it meets multiple criteria. Understanding and evaluating these criteria can help stakeholders better assess the relevance of tDPPs for their products.

CHAPTER 7

Defining Use Cases

WRITTEN BY
Baris Ozkan | Assistant Prof. Industrial Engineering & Innovation Sciences at Eindhoven University of Technology
Arno Laeven | CEO at Warren Brandeis
Jorn Fokkens | Change Lead & Business Development at Wipro
Yvo Hunink | Lead DPP at Dutch Blockchain Coalition and Founder of Regen Studio

RISING DPP ECOSYSTEMS

Differences in ecosystems mean that some product groups have a greater need for an extensive trust infrastructure.

Europe has recognized this as well. Batteries, for example, are under active development, and textiles are moving towards DPP implementation through delegated acts due to the significant impact in these product groups. This chapter presents our analysis of the socio-technical systems around various product groups, aiming to identify where the greatest urgency lies to build extensive open, decentralized, and permissionless systems.

The analyzed product groups were selected from the list of groups preparing for delegated acts for ecodesign requirements and mandatory DPPs, or those mentioned in the ESPR as highly relevant for circularity. The working group made a selection based on the participants' expertise in evaluating the product groups, including **vehicles, aluminum, recycled plastics, batteries, bio-ethanol, buildings, textiles, hydrogen, tires, semiconductors, computers, lubricants,** and **food packaging**.

The analysis is not exhaustive and subject to the interpretation of the contributors named at the beginning of this chapter. In our future activities, we aim to improve and expand the methodology for analysing use cases, applying approaches like 'Ecosystem Value Mapping' to focus on high-priority cases. In our analysis, **we ranked product groups based on three scores.** We took into account the earlier criteria from Chapter 6 and evaluated two additional parameters relevant to adoption: connectedness and ecosystem readiness.

TRUST SPECTRUM

This score is based on the relevance criteria for tDPPs from Chapter 6. The more points, the greater the need to establish an extensive trust infrastructure. It indicates varying degrees of openness and power distribution—from more restricted and controlled to fully transparent and permissionless ecosystems.

CONNECTEDNESS

The number of connections between product groups shows how many touch points the DPP has with other groups, indicating the need for interoperability. Each product group that can be part of another product group's DPP represents a connection, serving as an indicator of how quickly broader market adoption can be achieved through network effects.

ECOSYSTEM AVAILABILITY

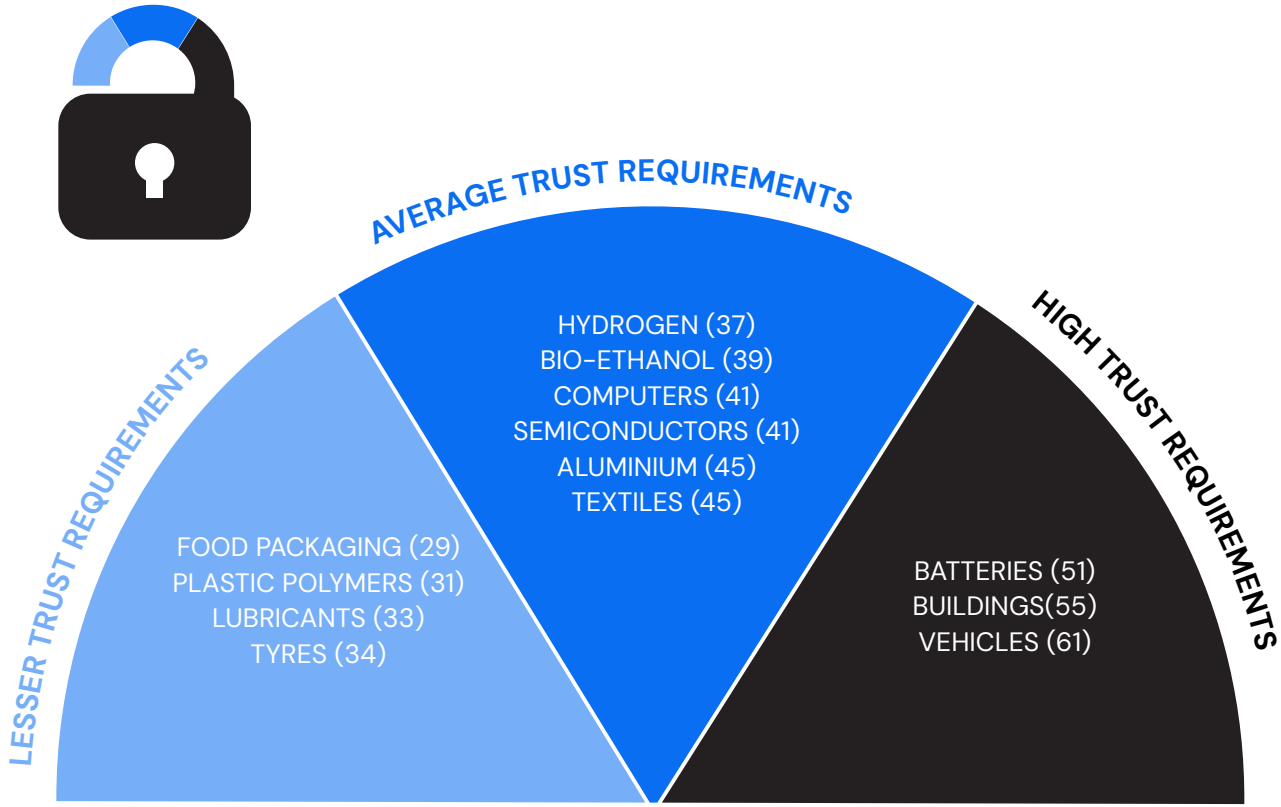
The readiness of surrounding ecosystems and stakeholders who already show interest in DPP projects and are likely to adopt these systems. Our method is a non-structured qualitative approach based on existing knowledge and limited desk research. This exercise reflect mainly the writers' perspective on the DPP landscape, and we aim to conduct it more robustly in the future.

7.1 Trust Spectrum

This figure shows where different product groups fall on a trust spectrum, helping to determine which groups require a higher level of trust, leading to more open, decentralized, and permissionless self-organizing networks. Lower-scoring groups may be able to operate with less openness and autonomy, where power is more concentrated among a few predefined trusted actors.

METHOD

A score matrix (criteria x product group), with a score from 1 to 5 given for each combination. All criteria are equally weighted and assessed individually for each use case in an online workshop with contributors. The total is the final score, with a clustering of scores into low, medium, and high trust.

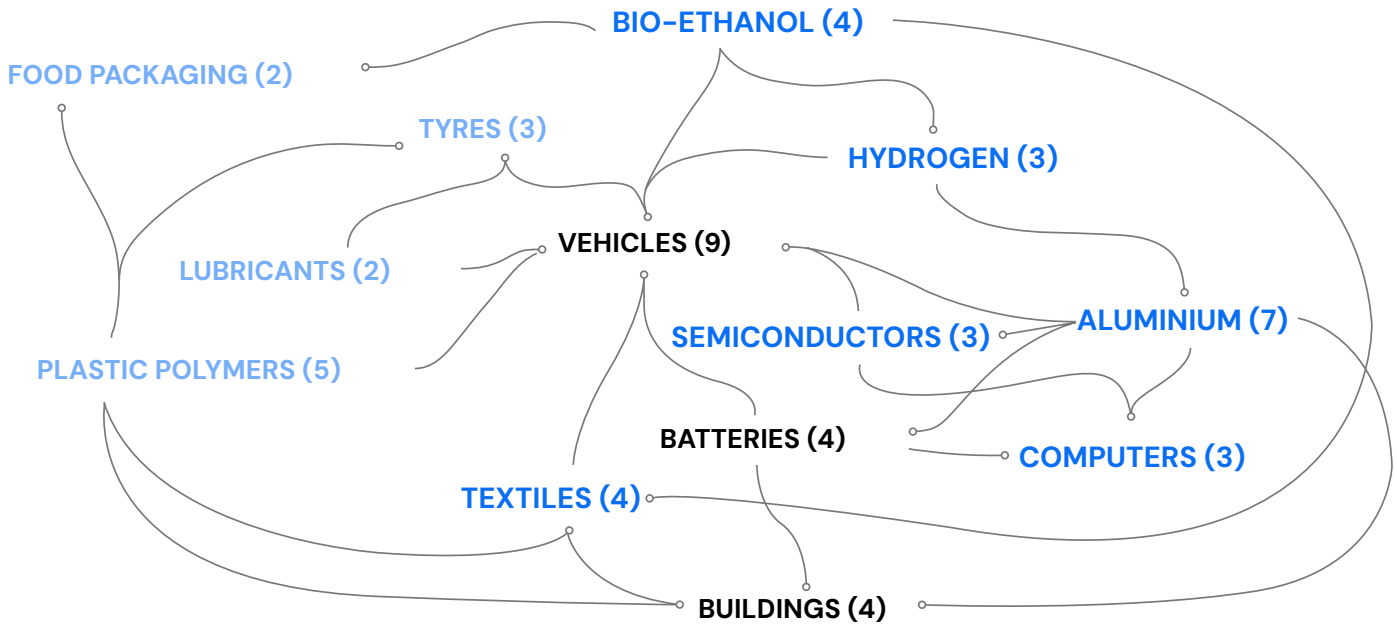


7.2 Connectedness

As shown, product groups like vehicles, batteries, bio-ethanol, textiles, computers, and buildings are highly interconnected within the broader ecosystem. These sectors need seamless data exchange with each other. Each connection in this ecosystem represents a critical point where data must be shared to maintain a smooth, transparent, and reliable supply chain. Starting in the centre of this connected ecosystem increases the likelihood of achieving broad tDPP adoption. The number of connections also strongly indicates which product groups would benefit most from a tDPP.

METHOD

When a product group can be part of another product group, a connection is shown with a line. Since vehicles use lubricants, there is therefore a line between these two. The circle at the end of the line indicates the product that encompasses the other product. The total number of connections is the score, which is clustered into highly, moderately, and minimally connected.



HIGH CONNECTEDNESS
Vehicles (9)
Aluminium (7)

AVERAGE CONNECTEDNESS
Plastic polymers (5)
Batteries (4)
Bio-ethanol (4)
Buildings (4)
Textiles (4)
Hydrogen (3)
Tyres (3)
Semiconductors (3)
Computers (3)

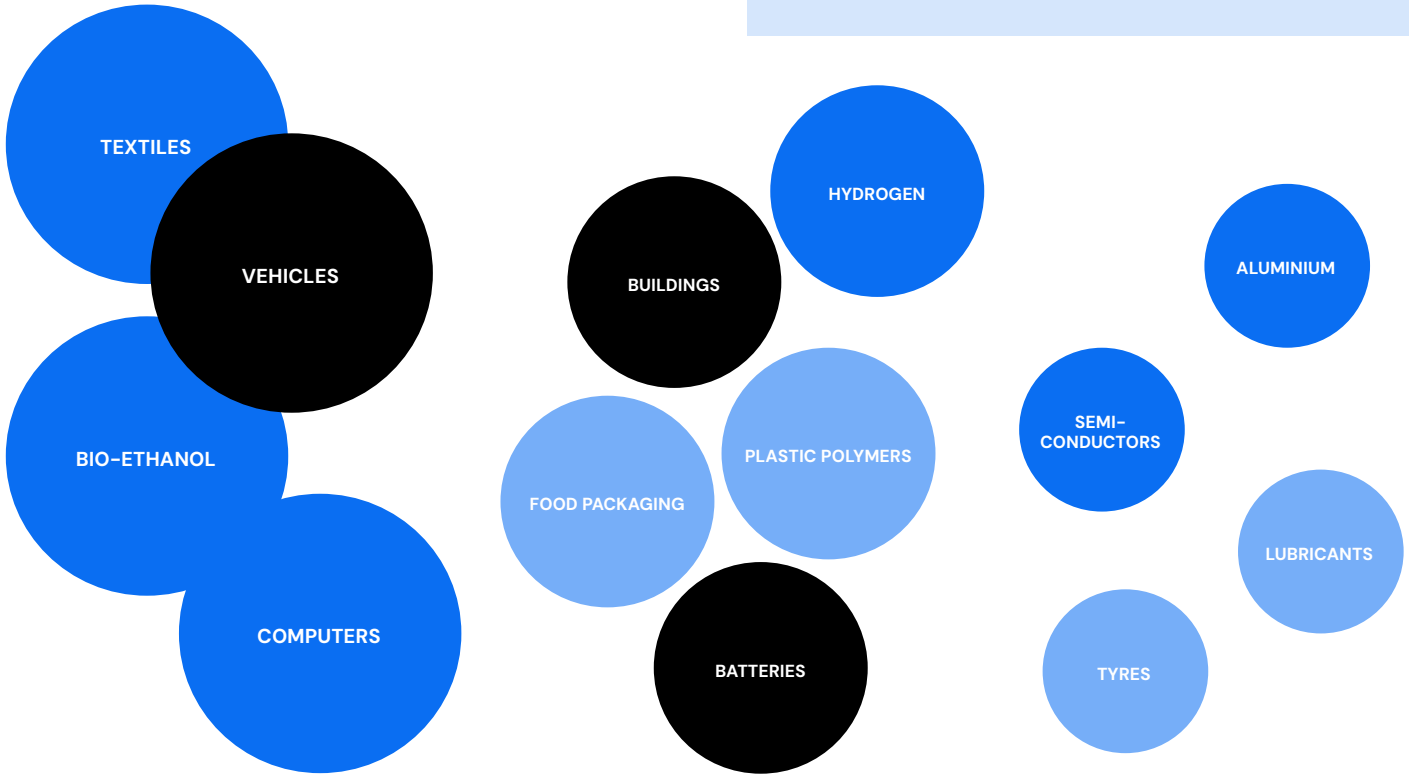
LOW CONNECTEDNESS
Lubricants (2)
Food Packaging (2)

7.3 Ecosystem Availability

In addition to our assessment of trust levels and connectedness, we must consider the readiness of ecosystems within these product categories. The willingness of these ecosystems to work on a DPP system with a broader group of stakeholders directly impacts the practical prioritization of product groups.

METHOD

This parameter is assessed in an unstructured qualitative manner. It is therefore only from the perspective of the authors and does not imply that no DPP communities exist within these product groups. However, the authors have had varying degrees of contact with parties from these product groups, and through discussion, it has been determined which nearby ecosystems offer opportunities for creating tDPPs.



Vehicle Passports as the Highest Priority Use Case

Vehicle passports top the list as a potential use case for our tDPP activities, given their high scores in all three areas.

We use the term 'vehicle' broadly, but this specifically includes road vehicles. With nine connections to industries such as batteries, tyres, lubricants, bio-ethanol, and aluminium, vehicles are central to many other sectors. Additionally, vehicles score high on the trust spectrum, indicating a significant need for more open and autonomously accessible DPP systems to manage the complex network of stakeholders involved in all stages of the vehicle and component life cycle.

In Chapter 8, we delve further into this case by outlining a scenario to illustrate certain architectural choices we would recommend for a high-trust use case like this.

WHAT DOES THE ESPR SAY ABOUT VEHICLES?

In Recital 13 and Article 1.2.h, vehicles are specifically mentioned as being out of scope for the creation of delegated acts, which is the means to mandate the DPP. So why propose a vehicle passport? The reason, as also stated in the ESPR, is that existing rules already describe the ecodesign requirements for certain vehicle types, such as those specified in Article 2(1) of Regulation (EU) No. 167/2013, Article 2(1) of Regulation (EU) No. 168/2013, and Article 2(1) of Regulation (EU) 2018/858. These vehicles are subject to various specific requirements and type approvals, such as Directives 2000/53/EC and 2005/64/EC.

In Recital 76 of the ESPR, road vehicles are specifically mentioned in a proposal for a future amendment to the regulation, which would require vehicles to record energy consumption and present it to consumers, while market parties would be obligated to make such data and climate information available to the European Commission in a privacy-friendly manner for product compliance with ecodesign requirements, with consumer consent. During the ESPR evaluation, the Commission must also assess the impact on vehicle circularity, as stated in Article 75.2. Furthermore, the ESPR addresses key vehicle components such as batteries and tyres, which are within scope because they are not sufficiently addressed in other regulations.

Although the vehicle passport is not officially mandatory or required through a delegated act, it appears highly feasible to apply DPPs to vehicles in practice to comply with existing legislation.

Important Considerations for Designing Vehicle Passports

THE PRODUCT THAT CONNECTS ALL OTHER PRODUCTS

Almost every product eventually comes into contact with a vehicle during transport movements. When considering interconnected sectors and interoperable DPP networks, the vehicle acts as the glue binding everything together. Moreover, a vehicle passport is essential for calculating transport emissions, which vary by vehicle type and its specific characteristics. A standardised approach to identifying vehicles and determining their impact on the carbon footprint of products is therefore necessary, which would also accelerate DPP adoption across the economy.

INTEGRATION OF OTHER DPPS

To fulfil the promise of interoperability, the integration of DPPs from other product groups is essential. Relevant connections include batteries, tyres, (renewable) fuels, aluminium, and textiles. Vehicle DPPs must be able to accommodate these integrations and dynamically update as other DPPs evolve.

APPLICATION IN CROSS-BORDER IMPORTS

Vehicles are produced and assembled in multiple countries, with parts and entire vehicles, including used ones, sourced worldwide. DPP systems must support cross-border interoperability, enabling seamless data sharing between manufacturers, importers, suppliers, and regulators in different jurisdictions. For this reason, the Dutch Tax and Customs Administration has shown interest in vehicle passports.

EXISTING ECOSYSTEMS

In addition to projects from the organisations involved in this position paper, vehicle passports are also seen as a viable option by others. One example is Catena-X, the first open and collaborative data space for the automotive industry, which itself is a spin-off of the Gaia-X ecosystem—a federated digital governance system and cloud/edge technology stack. Another example is the Mobility Open Blockchain Initiative (MOBI), which works on digital identities for vehicles, with an emphasis on interoperability and decentralised data management. These ecosystems highlight the growing momentum towards DPPs in the automotive industry.

PATH DEPENDENCIES

Because the initial investment for open, decentralised, and permissionless systems is considered high and risky, ecosystems with short-term business cases often choose to start with a closed approach, promising a transition to a permissionless model in the future. However, these promises rarely materialise, and projects are more likely to fail than to undergo a transition. Research on path dependencies in transitions shows that fundamental choices made in the early stages are often the only way to achieve the desired state of the system, even if they are challenging.

Conclusion on Defining Use Cases

Vehicle passports are the most urgent use case due to high scores across all components. Other product groups, such as batteries, buildings, textiles, computers, aluminium, hydrogen, and bio-ethanol, offer significant potential to expand the adoption of tDPPs, especially in sectors with strong regulatory requirements and increasing sustainability goals. Adopting tDPPs for these sectors will not only improve regulatory compliance but also stimulate innovation and interoperability.

CHAPTER 8

Towards Architectures for DPPs

WRITTEN BY
Baris Ozkan | Assistant Prof. Industrial Engineering & Innovation Sciences At Eindhoven University of Technology
Theodor Chirvasuta | Semantic Interoperability Expert at TNO
Abhishek Mahadevan Raju | Founder and CEO at Quintessence Research B.V.
Yvo Hunink | Lead DPP at Dutch Blockchain Coalition and Founder of Regen Studio

8.1 Building Trust

Organisations, governments, IT systems, and economic structures can be viewed as networks of nodes (people, organisations, or objects) and connections (relationships or interactions).

In the context of the vision outlined in Chapter 4, a tDPP functions as an interface for the digital identity of the product within a network of various actors—responsible economic operators, supply chain partners, government agencies, consumers, and many others—who play a role in the DPP ecosystem. All these parties together will form a trustworthy system and network around the DPP that can reassure not only consumers but all stakeholders that the information they receive about a product is accurate, valid, and complete. In this section, we explain how ecosystems of trust come into being.

DESIGNING TRUSTED ECOSYSTEMS

A certain degree of openness and permissionlessness is essential for trusted ecosystems, and this can be achieved through more decentralised or distributed architectures across various network and system components. Even within this approach, there are numerous options and variations of architectural choices to consider.

In more centralised networks and systems, which are indeed more efficient and easier to set up, power tends to concentrate at a few nodes, leading to an unequal distribution of benefits and increased vulnerabilities, such as "Single Points of Failure." Sometimes, this also results in perverse incentives, which can eventually lead to abuse of power, ultimately undermining trust. On the other hand, well-designed decentralised networks and systems are more resilient, promote a fair distribution of value and power, aim for digital sovereignty over one's own data, and are governed by democratic decision-making. Within the context of digital identities, the parties forming the FIDES ecosystem have found that these characteristics of decentralised systems are essential for building trustworthy ecosystems and can also be applied to DPPs. However, they are also more complex to design, have higher initial costs, and are, to some extent, unpredictable. Now to instil trust in an ecosystem is extremely difficult thing to design for up front, and is more reflected in the design choices resulting from interacting with the stakeholders to see what captures their trust.

Especially in sectors where there is no clearly trusted party that all stakeholders mandate to hold power, an open, decentralised and permissionless trust ecosystem is a desirable way forward. In a tDPP, any participant can contribute data, verify information, or interact with the DPP, albeit with attribute-based access control, as long as they adhere to the standards and open protocols developed by the ecosystem in consensus.

WHEN ARE SYSTEMS AND NETWORKS DECENTRALISED?

We considered terms like 'federated' and 'distributed' and, for simplicity of semantics, concluded that these all represent 'degrees of decentralisation.' This allows DPP networks and systems to be better described as systems with a 'degree of decentralisation,' depending on how each component is implemented. A system or network is considered more decentralised when underlying processes are openly accessible, reusable, and adaptable by a wide range of participants. In decentralised networks, decision-making is more democratic, enabling more inclusive participation and a fairer distribution of power. This leads to open and transparent verification of transactions and interactions, minimising technical information asymmetry between participants. However, this does not mean that the DPP system must avoid all centralisation, nor that all DPP system components should always be permissionless and decentralised. There are additional criteria in system design that must be weighed, which we will do in 8.2. Nevertheless, especially in identity and access systems that support DPPs, we strongly recommend a decentralised approach.

HOW TO DESIGN A DECENTRALISED SYSTEM OR NETWORK?

Our envisioned tDPPs are not merely decentralised collections of data that record and store product and product life cycle data but may also use decentralised identity and access controls, verification models and governance. This means a broad range of potential design options, with more radical decentralisation applied to one component and a more federated or centralised option chosen for others. In Section 8.3, we list all DPP components to which decentralisation can be applied to varying degrees, and in Section 8.4, we present several design scenarios.

THE PARADOX OF (DE)CENTRALISATION

Designing for decentralisation is no easy task. It often results in creating a complex adaptive system that operates in fundamentally unexpected ways. Sometimes, measures intended to decentralise a network ultimately lead to centralised ecosystems. It is important to note that even in a maximally technically decentralised system, the resulting operations within the network can still become highly centralised. This is because centralisation often arises from non-technical aspects, such as governance or the incentive model. For instance, the 'mining' community around the Bitcoin network today is extremely centralised, with only a few 'Mining Pools' handling transaction validation, due to an aspect of the mechanism design that encourages this behaviour.

The introduction of a shared aspect, such as a (centralised) standard, can support decentralisation within the network, provided the governance over the standard remains decentralised. However, a standard can also lead to centralisation, particularly if it benefits the organisations managing or heavily involved in its development. Therefore, we suggest that a DPP system should strive to offer various options, resulting in a DPP standard that is an umbrella of standards—some more decentralised, others less so.

In practice, complex **DPP ecosystems are expected to be inclined to follow hybrid approaches, with more decentralised and more centralised architectures across different elements**, guided by stakeholder preferences and criteria. The next section defines some of these criteria.

8.2 Criteria for Architectural Choices

While many choices are possible, an ecosystem implementing a DPP solution must make trade-offs between architectural choices based on certain criteria. Here, we present a non-exhaustive list of criteria that are important and relevant for parties to consider.

Resilience

The ESPR specifies explicit requirements for resilience against system failures. In data storage solutions, greater independence among the involved parties generally means higher resilience. This is why P2P networks with illegal content are so difficult for authorities to shut down. However, this does not mean that decentralised systems and networks are immune to disruptions. Every implementation of a technical system or governance model by a DPP ecosystem comes with its own considerations for resilience. The more resilient they are, the more these DPPs can be trusted to meet our needs.

Cost of Ecosystem Adoption

The costs of adoption include not only the initial setup and implementation but also the expenses related to securely connecting and adapting internal systems to comply with DPP models and maintaining these qualities throughout their life cycle. This includes IT reporting, data management, change management, and integration efforts at the end of product life cycles. Organisations must consider the financial impact of adapting existing systems to meet DPP requirements, as well as the ongoing costs of maintaining secure and compliant data flows. Although organisations typically define these costs themselves, we propose that trust ecosystems surrounding DPPs should consider the costs for the entire ecosystem to understand where expenses are most unevenly distributed and where bottlenecks remain for full ecosystem participation.

Manageability

Modern business systems are designed around modularity, enabling interconnectivity via interfaces. The manageability of a DPP system that must connect with these business systems can vary depending on the complexity, diversity, and volume of these connections. Key differences arise when considering the type of modules that would be connected to the DPP system and the frequency of maintenance. An analysis is needed of the required complexity of the DPP system, the connections, and the business logic necessary. Additionally, governance systems must remain manageable, which largely depends on how information is processed and distributed throughout the ecosystem, and how decision-making is organised.

Data Sovereignty

Companies are concerned about too much competitive information potentially becoming public and generally prefer extensive control over their data in the supply chain. This involves the freedom to store data on their own servers and to organise selective access. A more decentralised storage and identity system implies that each DPP provider has the capability to shield sensitive data and organise access. However, it must be ensured that individuals cannot compromise data integrity or that compliance with DPP requirements is not obstructed by restrictions. Here, the dilemma between transparency and privacy comes into play. A system that provides digital sovereignty to businesses and consumers typically requires higher costs but can help resolve this dilemma. The trade-off between allocating resources for the system and operational freedom must be evaluated when deciding between these solutions.

Risk of Security/Data Breaches

The risk of data breaches and security incidents is considerable, given that DPP data often requires collaborative processing by multiple parties over the life cycle of a product. While trusted components deployed locally can mitigate some risks, the potential for misconfiguration and vulnerabilities remains a concern. Smaller organisations with limited resources may benefit from using a certified and audited service provider offering cloud infrastructure. This approach, however, should be coupled with a strong access control framework and the implementation of robust yet flexible digital identities to ensure the security of the system.

Adaptability and Versatility

The ability to customise the DPP to the specific needs and requirements of an organisation within its business context is crucial. Solutions with a higher degree of adaptability may incur additional development and implementation costs but provide better alignment with unique business processes. More standardised solutions, on the other hand, may offer lower initial costs but less flexibility. The flexibility to integrate more information about products can provide new insights to business partners.

Involvement in the Decision-Making Process

Organisations and individuals value an ecosystem more when they have influence within it. However, the more actors are given influence, the less influence each actor has. Therefore, organisations have an interest in participating in decision-making while excluding others. In forming a DPP and the trust ecosystem surrounding it, such perverse incentives around concentration of power in decision-making should be avoided, while ensuring that participation remains appealing to a broader group of stakeholders.

The criteria will require further definition and specification but point us towards a path for how DPP ecosystems can evaluate the design choices of their required trust architecture. In the next section, we broaden our perspective to the system components of the DPP ecosystem to which these criteria apply.

8.3 Components of the DPP System

DPP systems require various components, each with its own existing standards and a wide range of different architectural designs.

Several European research projects and initiatives, such as CIRPASS(2), BatteryPass, and StandICT, have proposed initial versions of horizontal DPP systems, still allowing for multiple implementations. At a global level, there are many similar initiatives, such as the United Nations Transparency Protocol (UNTP). **In the context of this chapter, we focus on a few key system components and discuss their architectural options**, with specific attention to their potential to enable trust ecosystems around DPPs.

Identifiers for Products, People, Organisations, and Locations

Identifiers are crucial for uniquely identifying digital product passports at the model, batch, and item level, but they are also necessary for natural persons, legal entities, and locations, such as the manufacturer, representative, and the facility used. Key considerations include the life cycle of and access to these identifiers. Methods for physically binding products, such as data carriers or cryptographic modules, can play a critical role for certain product categories. A general way to determine whether an identity system is centralised or decentralised is by examining how these identifiers are created, communicated, stored, and where the keys are kept that prove control over an identifier.

Identity and Access Control Systems

Identity and access control systems are essential building blocks for managing who can add, view, edit, and modify data within DPP ecosystems and under what conditions. Building on identifiers, these systems bring the trust ecosystem to life. They are responsible for user authentication, ensuring that only authorised persons or entities can access sensitive information. Decentralised concepts like Self-Sovereign Identity (SSI) enable individuals and organisations to manage their own identities while using attributes through selective disclosure to determine who can access what and when, or using cryptographic techniques to prove information without revealing data. Decentralised solutions enable more privacy-friendly, dynamic, and scalable permissions for multiple stakeholders, protecting actors active within many DPP ecosystems from centralised identity systems, where participants would need to create an account for each DPP, with associated security risks. With SSI,

they can instead simply present an attribute proving they are an employee of the company granted access through the governance process. An important aspect is the ability to revoke attribute validity when needed, which is crucial for ensuring DPP data remains protected while retaining the flexibility needed for broad stakeholder participation across diverse ecosystems.

Data Storage

Through DPPs, we expect a substantial increase in data. Hosting and managing this internally can be costly, and many companies may find it infeasible to maintain such infrastructure. The ESPR mandates decentralised data storage, making the DPP not a central database but rather a 'knowledge graph' of interconnected datasets hosted by various stakeholders. Because self-hosting data can be cumbersome, it is often easier to use a service provider where data can be stored, though this carries the risk of dependency on cloud systems. Decentralised storage or P2P solutions solve some issues around resilience, transparency, and fairness but may introduce risks concerning complexity and competitiveness if not considered in the design. It is expected that multiple centralised and decentralised storage methods will converge within the same DPP.

DPP Interfaces and Services

These protocols include IT services and APIs that serve as interfaces for accessing and managing DPP data across various platforms. They also encompass data exchange standards, specifying the message models, formats, and procedures used to exchange information among stakeholders to ensure interoperability. Industry-driven semantic standards for domain-specific data should be accompanied by sufficient additional horizontal DPP context meta data to enable interoperability in complex ecosystems or be harmonised. Accepted services managed by one or a small group of actors run the risk of dependencies and single points of failure. A more decentralised approach to services and interfaces ensures a wide range of service providers can interact with and add value to the DPP, but may also increase the risk of malicious actors and make interfaces harder to manage.

DPP Governance

Responsibilities around decision-making are part of DPP governance. This not only involves managing technical components of the DPP system, such as semantics, ontologies, and interoperability profiles, but also considers political, economic, organisational, and sometimes even social aspects for governing the ecosystem. How an ecosystem governs itself can range from bottom-up self-organisation to top-down hierarchical management, consensus-based or legally mandated. While decision-making can proceed faster in centralised models, decentralised models offer greater transparency and democratic principles. The ESPR accounts for self-regulation, where product groups not covered by a delegated act have the option to design and establish self-regulating measures with approval from the European Commission. This means that DPP ecosystems can define their own ecodesign requirements and integrate themselves into the European DPP landscape.

Verifiability

Verifiability in DPP systems is crucial for trust. This is achieved through protocols that allow independent auditors to validate data, which users can then verify, such as the CO2 footprint of a product. Through ecosystem management and identity systems, trusted actors can be authorised to review data and verify claims, leading to a more centralised model of verifiability. In decentralised verification, any organisation wishing to make or test a claim may do so, and anyone can verify it; however, this generally requires greater openness of data. To ensure authenticity and integrity, cryptographic techniques such as digital signatures can be used to validate the source and content of data, alongside hashing to maintain data integrity, fostering trust in such decentralised models. This also allows the verifier to be verified in an open and transparent manner, creating a trusted DPP ecosystem. DPP ecosystems must weigh the extent of verifiability, which also depends on the legal oversight framework in which the product operates, which can vary by country.

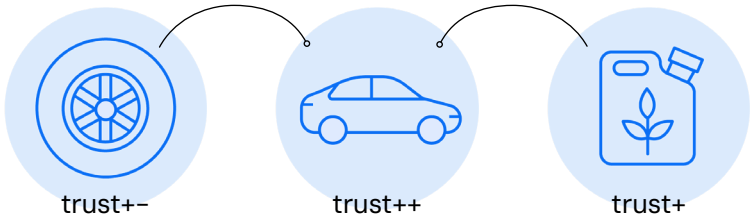
The DPP system is a complex web of interdependent components that involves far more design decisions than can be discussed here. There are various components not covered, such as data carriers, lookup mechanisms, or user interfaces, as they are less urgent to discuss regarding architectural decisions. One component not covered but extremely important for a well-functioning decentralised network is the incentive model, an essential part of a mechanism design from the field of game theory. Decentralised networks often need incentive models to promote desired behaviour, but these are particularly challenging to design effectively.

To clarify which architectural choices can be made for specific contextual characteristics, we have set out various scenarios in the next section around some of the product groups from Chapter 7.

8.4 Scenarios

We present several use cases in the form of scenarios to demonstrate the types of situations that may require a diversity of architectures.

The use cases in these scenarios have been chosen due to their varying scores from Chapter 6. The scenarios are high, average and low levels of trust. We chose, vehicle passports (high trust ++), bio-ethanol passports (medium trust +), and tyre passports (low trust +-). These product groups were also selected to on possible integrations between DPPs, as they require interoperability with one another. After all, bio-ethanol can serve as a fuel, while tyres are the only vehicle component that, according to the ESPR, still lacks sufficient ecodesign requirements.



CASE 1

Vehicle Passports

DPP WITH HIGH TRUST LEVEL ++

Vehicle passports require a DPP with a high level of trust due to factors such as life cycle complexity, significant societal value, and their connection to the transport of other products. Vehicles are relevant for circular economy models, where many components are repaired, recycled, or reused. Their frequent maintenance, updates, and configuration changes also necessitate a flexible, decentralised system that can accommodate multiple stakeholders, such as manufacturers, repair centres, and owners. Vehicles are often unique due to numerous configurations (especially in electric vehicles) and require transparency and security, particularly regarding ownership, maintenance history, and regulatory compliance. The potential for multiple owners and users over their lifespan further underscores the need for robust decentralised data management. Moreover, vehicles have a long lifespan and are subject to increasing regulation over time, making a DPP that ensures compliance, transparency, and data integrity essential. Given the high importance of trust, resilience, and transparency, a fully open, permissionless, and decentralised system is crucial to address and manage these diverse and complex requirements.

CASE 2

Bio-ethanol Passports

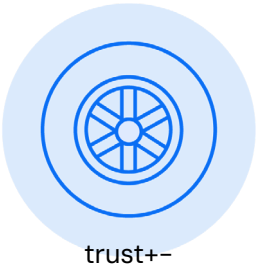
DPP WITH AVERAGE TRUST +

Bio-ethanol, a chemical product of biological origins, requires a medium level of trust for its DPP. While it is not fully circular, when used as a basis for fuels, it has some strong claims, particularly in terms of sustainability. Bio-ethanol is subject to strict regulations, and tracking its life cycle from production to use is crucial, especially to ensure transparency regarding environmental impacts and reduction claims. Although bio-ethanol does not require regular maintenance or upgrades like vehicles, as a batch product, it is vulnerable to issues such as fraud, making transparency around ownership and movement essential. Additionally, the supply chain often involves multiple international parties, and decentralisation can support transparent governance and accurate data exchanges. Another key aspect is the issue of "double-claiming" emissions reductions by different partners in the supply chain, which a decentralised system design can help prevent. Finally, bio-ethanol has diverse applications, such as fuel, an intermediate for green hydrogen, or as a base for bio-plastics, which requires interoperability and integration with multiple ecosystems. While top-down governance may support more centralised architectures, other characteristics of this product group suggest that a more decentralised DPP would be advantageous.

CASE 3

Tyre Passports

DPP WITH LOW TRUST +–



Tyre passports appear to have a lower need for trust, with a less complex life cycle. While circular tyres have a significant positive environmental impact, the value of tracking their reuse or recycling is less substantial than for vehicles. The economic value of tyres is not particularly high. Although some degree of sustainability reporting is required, a fully decentralised system may not be necessary, partly due to the small ecosystem involved, given the relatively limited interconnections with other DPPs. Tyres generally do not require regular upgrades or customised configurations, so a less flexible, more centralised system could be sufficient. The risk of theft or unique characteristics requiring verification is low, further reducing the need for a high-trust system. Although tyres have a reasonable lifespan and may fall under regulatory control, the interactions are less complex than those for vehicles or bio-ethanol, making a simpler, federated or centralised DPP more suitable for adoption. However, a decentralised approach could still prove valuable in the long term, especially if the DPP landscape leads to power concentration or if significant fraud by ecosystem participants is uncovered.

8.5 Comparing the cases to the criteria for adoption

The main insights from comparing Digital Product Passports for vehicles, ethanol, and tyres highlight the need for different approaches that take adoption into account.

To arrive at these insights, we conducted a structured comparison of the cases within each adoption criterion, as defined in Section 8.2. This comparison is available upon request from the authors.

Vehicle Passports involve the highest costs due to the complexity of their lifecycle, frequent updates, and regulatory requirements. Vehicles also require a high degree of flexibility because of frequent updates and component tracking, especially in electric vehicles. In terms of governance, security, and resilience, vehicles demand a complex system with multiple stakeholders, making them highly susceptible to data leaks and system failures. For vehicles, with their high demands on adaptability, governance, and security, a decentralised approach is crucial to manage the many stakeholders and sensitive data.

Bio-ethanol Passports incur medium to high costs, with a focus on sustainability and compliance. Few modifications are made, but there is a strong need to protect competitively sensitive information through data sovereignty. Ethanol products benefit from governance structures that ensure resilience, transparency, and security, though to a lesser extent than vehicles. Ethanol could, therefore, benefit from a hybrid system of centralised and decentralised components.

Tyre Passports, however, have moderate costs with lower complexity, requiring only minimal adjustments and operational expenses. There is also less interoperability with other products and little need for data sovereignty. Tyre passports can function effectively with a more centralised or federated system, keeping costs and complexity lower. However, risks may arise that could have been mitigated by decentralised architectures.

These findings highlight that the choice between a decentralised or centralised approach should be based on the specific needs of the product group, with different choices also made across various components. **This makes interoperability—both technical and semantic—between different DPP component providers crucially important.** Without an appropriate framework for interoperability agreements, DPP ecosystems will stagnate, and users of the systems will face significant administrative challenges, carrying serious business risks. It remains to be seen whether the first version of the DPP standard can reach this level and whether it will ever be fully complete, given the constant changes in reality. Therefore, a neutral space is needed where DPP ecosystems can practically address these interoperability issues.

Ecosystems of Interoperability

An example of an initiative that brings interoperability into practice is the Decentralized Identity Interoperability Profile (DIIP), which is hosted within FIDES. This profile integrates open and mature standards for digital identities into a framework that supports different providers of such systems. Similar to the DIIP but focusing on organisational identities is the Company Passport initiative, also hosted within FIDES. These profiles can serve as a model for developing an interoperability framework for DPPs and identities that supports flexibility while maintaining compatibility between systems.

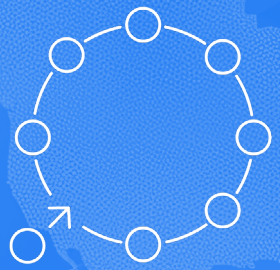
The UNTP is also a highly interesting initiative that already contains DPP foundations and is based on many of the same standards as the DIIP and the Company Passport. Furthermore, it is an international initiative, helping to foster further interoperability on a global scale. With the European initiative Trace4EU and the working group on interoperability within it, we are exploring a collaboration to use the UNTP as a basis.

While centralised architectures offer clear paths, they carry the risk of limiting flexibility, creating vendor lock-in, and establishing new concentrations of power. Therefore, a balanced approach is needed—one that combines decentralised identifiers, self-hosted data, and flexible governance models with more centralised solutions. This will foster more self-organisation around product identities and thus create a more dynamic, resilient, inclusive, verifiable, and therefore a trusted DPP ecosystem, contributing to the faster achievement of Europe's goals for a circular economy.

Conclusion on Architectures for tDPPs

In designing DPP ecosystems, trust must be the foundation, based on the structure of data, interactions, and governance among stakeholders. A balance between decentralised architectures for resilience, security, and interoperability, and centralised systems that enable simplicity, cost savings, and rapid adoption, is essential. However, the risks of vulnerabilities and power imbalances must not be overlooked. The success of DPPs, especially in complex ecosystems such as vehicles, depends on a practical, open, permissionless architecture that promotes inclusion and captures verifiable data. The degree of decentralisation depends on product complexity, stakeholder requirements, and regulatory demands.

Interoperability between centralised and decentralised systems is central to a robust, flexible, and scalable DPP ecosystem. Decentralised architectures typically promote interoperability as a fundamental design principle. Participants should be able to choose solutions that suit their unique needs. Standardisation of protocols, interfaces, and functionalities is necessary to ensure a cohesive ecosystem where centralised and decentralised components can work together. What the CEN/CENELEC DPP standard will encompass remains uncertain, but achieving seamless technical interoperability will continue to be a challenge. **Therefore, it is crucial to establish a neutral DPP ecosystem focused on interoperability as a core task.**



CHAPTER 9

Building Trust Together

WRITTEN BY:
Victor van der Hulst | Co-initiator FIDES - Accelerating Digital Trust

How will we anchor our position within a collaboration among like-minded parties?

The Importance of Collaboration for Trust

The internet, artificial intelligence, and other forms of digitalisation are rapidly transforming the world, offering significant opportunities and solutions to global challenges. However, they also introduce new challenges. Digital trust is therefore a continually evolving field that requires constant experimentation, development, testing, and implementation to adapt to new challenges and technologies. This process is costly and complex. Trust develops more quickly when there is freedom of choice between digital solutions, but these must be able to interact harmoniously. This necessitates broad adoption of open standards and interoperability profiles, which also applies to tDPPs.

As with many things, tDPPs do not function in isolation. They are closely interwoven with digital identities of both natural and legal persons. When you are not certain who you are communicating with, which organisation you are dealing with, or with which "thing" you are interacting, we miss the opportunities that digital technology offers. This interdependence highlights the importance of collaboration, interoperability, and joint experimentation.

Collaboration is essential to fully realise the potential of tDPPs. Rather than isolated "do-it-yourself" approaches, which often lead to fragmented and inefficient solutions, a "do-it-together" approach is needed. By working together from shared principles, initiatives—also across borders—can pool their strengths, share knowledge and resources, and experiment collectively. This accelerates the development and implementation of flexible and scalable solutions.

A collective initiative can act as a catalyst for innovation and standards. It can lead to the development of common protocols and breakthrough projects that enhance interoperability between different systems and platforms. Moreover, it fosters a culture of trust and mutual understanding, which is crucial for the long-term success of DPPs.

FIDES.

Accelerating
Digital Trust

FIDES is an international movement dedicated to the continuous improvement of Digital Trust on the internet. Supported by a non-profit foundation, FIDES facilitates collaboration in shared R&D (FIDES Labs), use cases (FIDES Open Sandboxes), interoperability events (FIDES Plugfests), and the connection of digital ecosystems (FIDES Ecosystems), based on the principles of the FIDES Manifesto.

A strong collective for the creation of DPPs

As a collective initiative, FIDES plays an essential role in accelerating the development and implementation of Digital Product Passports (DPPs). By providing a platform for collaboration among governments, businesses, and knowledge institutions, FIDES fosters a sustainable ecosystem dedicated to digital identity, including DPPs, and trust. The FIDES Manifesto forms the foundation for this collaboration, emphasising openness, transparency, and collective innovation. This enables the development of interoperable digital identities and trust frameworks that are indispensable for DPPs.

At the heart of FIDES lies a collaborative approach to R&D, allowing organisations to experiment and develop solutions for current and future challenges. Through FIDES Labs, breakthrough projects are promoted that centre on knowledge sharing and the development of 'trust-building blocks' through shared research. Collaboration in cross-domain projects creates a neutral, vendor-independent environment where trust and innovation go hand in hand. These cases are made available via FIDES Open Sandboxes, enabling everyone, globally, to test these applications themselves.

FIDES focuses on the international adoption of trusted digital identities for individuals, organisations, and objects. This aligns with new regulations such as eIDAS 2, the EU Digital Identity Wallet, and the ESPR for DPPs. In addition to FIDES Labs, FIDES organises Plugfests—events focused on interoperability that bring together providers to demonstrate integrated solutions. For example, in 2025, a Plugfest on tDPPs will be held to showcase working solutions to a broad audience.

Through collaboration and a shared vision, we can respond more quickly to the opportunities and challenges that the near future presents. FIDES accelerates this transition by fostering a sustainable, collaborative approach to the implementation of, and interoperability within, an ecosystem of Trusted Digital Product Passports as one of the pillars within the landscape of digital trust solutions.

Do you agree with the conclusions in this report?

Consider giving your support through:

FIDES.COMMUNITY

FIDES.
Accelerating
Digital Trust

YVO HUNINK
Lead Digital Product Passports

E info@fides.community