Exploring the Design Space and Research Directions for Digital Product Passport Systems

Stefan Kaser, Christian Lesjak
Connected Secure Systems
Infineon Technologies Austria AG
Graz, Austria
{stefan.kaser, christian.lesjak}@infineon.com

Rainer Matischek
Country R&D Office Austria
Infineon Technologies Austria AG
Graz, Austria
rainer.matischek@infineon.com

Christian Steger
Institute for Technical Informatics
Graz University of Technology
Graz, Austria
steger@tugraz.at

***Abstract*—In this paper, we identify three major technical dimensions of a Digital Product Passport (DPP) system: *data carrier*, *online storage for product information*, and *updating dynamic data*. For each dimension, we first explore the design space in terms of architectural options and technical challenges, and then propose corresponding research directions. Specifically, this paper discusses key challenges such as counterfeiting, interoperability, and data sovereignty, and calls for research in areas such as decentralized identity and granular access management.**

***Index Terms*—Circular Economy, Digital Product Passport (DPP), Data Carrier**

I. Introduction

As part of the European Green Deal, the Ecodesign for Sustainable Products Regulation (ESPR)[1] of the European Union (EU) mandates Digital Product Passports (DPPs) for high-impact sectors, requiring manufacturers to establish machine-readable metadata throughout a product's lifecycle, to promote sustainability, circular economy, transparency, and regulatory compliance. The vast possibilities for implementing DPP systems involve several technical hurdles: selecting durable on-product data carriers, designing future-proof, scalable data repositories, and handling dynamic data generated by sensors, software applications, and user interactions. Trade-offs between interoperability, accessibility, data privacy, security, ecological impact, and other factors require a systematic exploration of the design space.

II. Background and Related Work

The DPP is a structured, digital data set, which is associated with a physical product across its lifecycle, enabling transparency, regulatory compliance, and circular economy goals. DPPs support multiple stakeholders, e.g., the manufacturer, consumer, and third-party service providers, by providing verified information on origin, repairability, sustainability, and more. Technically, a DPP system comprises three core dimensions, as depicted in Fig. 1: (1) a data carrier, such as a Quick Response (QR) code or Near Field Communication (NFC) tag embedded in a product, (2) an online storage infrastructure for dynamic and detailed product data, and (3) authenticated updating mechanisms for tracking lifecycle events. Implementation models range from offline (local-only) to fully online (e.g., cloud-based) systems, as well as hybrid approaches. Ideally, the data carrier is accessible via a smartphone and stores a subset of the product's information, while the majority of data is stored online and referenced by the carrier. Throughout a product's lifetime, these data need to remain up to date. Stakeholders can access them either directly online or via the data carrier, which typically redirects to the corresponding online storage.

Related work can be found in EU projects like *CIRPASS*[1] and *Battery Pass*[2], as well as academic research into Digital Twins (DTs)[2], Asset Administration Shell (AAS)[3], secure identifiers, identity interoperability, Verifiable Credentials (VCs), and decentralized product information systems [4], [5], [6]. These works highlight the need for scalable, privacy-preserving, and interoperable DPP architectures.

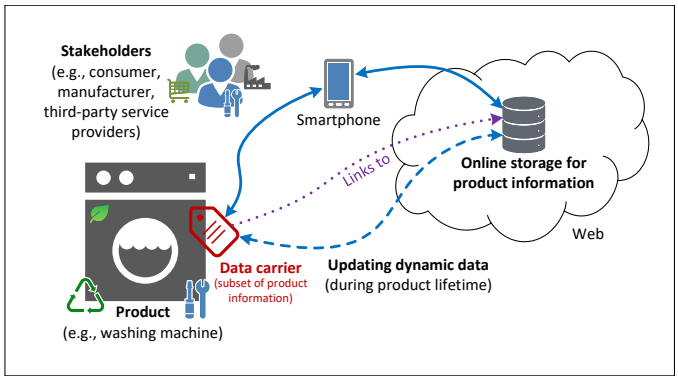

Fig. 1. Conceptual architecture of a DPP system.

In this paper, we discuss the design space and challenges for DPP systems and propose research directions for

- Data carrier (Section III),
- Online storage for product information (Section IV), and
- Updating dynamic data (Section V).

III. Data Carrier

The physical product is equipped with a data carrier, which links the product to digital product information, usually stored in a Web-based data repository. Data carriers encompass a

[1]https://cirpassproject.eu/, https://cirpass2.eu/
[2]https://thebatterypass.eu/

978-3-903176-75-1 ©2025 IFIP

wide range of technologies in the design space: Textual labels (e.g., plain text or a link), optical labels (barcode, DataMatrix, QR code) and electronic carriers (Radio-Frequency Identification (RFID) tag, NFC tag, smart card) are instances of applicable data carriers for DPP systems, of which electronic-based ones offer higher flexibility and can handle variable data.

A. Counterfeiting

Establishing trust in DPP systems requires effective measures to prevent fraud and counterfeiting. A key mitigation is the unique identification of each individual product – or, where appropriate, e.g., a model series or production batch – which the data carrier must support. This enables reliable traceability and secured linkage to digital information. Textual labels are prone to modification, whereas optical data carriers can include error correction, checksums for data integrity, or even digital signatures for authenticity and integrity, protecting the content.

Cloneability is another concern, common to both textual and optical labels, such as QR codes: Most of them can be easily duplicated and applied to counterfeit products, unless complex or costly printing technologies are used [7]. Electronic data carriers offer greater resistance to cloning and provide additional benefits in terms of data flexibility, security, and authenticity. Unlike basic RFID and NFC tags, secured microcontrollers and smart cards are specifically designed to prevent cloning, where hardware-based Secure Elements (SEs) are widely used. They can store and protect secret data – such as unique identifiers or cryptographic keys – and support hashing, digital signatures, and authentication operations.

Research Directions To further enhance identity trustworthiness, we recommend conducting research and development on the implementation of advanced security mechanisms, such as challenge-response protocols, Active Authentication (AA), Zero-Knowledge Proof (ZKP), and VC, at the data carrier level. This proactive measure will strengthen DPP systems against emerging security threats and achieve a high level of trust in system identity verification processes.

B. Multiple Stakeholders

Given the involvement of diverse stakeholders, access rights management is relevant at multiple levels, including the data carrier and the online storage. The diversity of industry standards for data carriers (e.g., QR codes, RFID, and NFC tags) poses interoperability challenges, since different stakeholders may adopt different standards or implementations. This makes approaches for standardization and decisions in consortia essential for seamless data exchange. Furthermore, since stakeholders have varying data needs, flexible architectures are needed to maintain data integrity and trust throughout a product's lifecycle.

Research Directions To facilitate seamless data exchange among stakeholders, we propose further research and development in interoperable standards for data carriers. Furthermore, flexible access control mechanisms must be researched, to accommodate varying stakeholder roles and data needs. Exploring and establishing robust governance models for tag issuance, updates, and end-of-life management is also crucial. Additionally, detailed investigation of stakeholder requirements and consortium standardizations can support the design of coherent DPP systems.

C. Accessibility

DPP data carriers should be accessible to people with disabilities, non-experts, and users in low-connectivity or resource-limited settings. Optical labels such as QR codes are well-established, widely recognized, and easy to use, making them a low-cost and universal access method. They support compatibility with older smartphones and legacy devices, allowing broad accessibility. Electronic data carriers, like NFC and RFID, utilize well-established communication hardware to provide reliable, contactless access. These technologies enhance user experience and also support offline access to essential product information. While NFC is widespread in today's smartphones, RFID-based carriers require dedicated reader equipment and are not accessible to most consumers. For an accessible DPP system, the choice of data carrier must reach the maximum possible audience.

Research Directions Research must account for technology available to the general public. While specific data carrier technologies may offer superior functionality, only privileged consumers may have access. Furthermore, to enable people with disabilities and non-expert users to interact with DPP data carriers effectively and independently, further research in fields like interface and feedback design (e.g., audio, haptic signals and visual guidance) must be conducted.

D. Storage Capacity

Data carriers for DPP systems have a significant variation in storage capacity, ranging from a few kilobytes (max. $\sim$3 kB) for QR codes[3] to tens or hundreds of kilobytes (max. $\sim$600 kB) for advanced NFC tags and secured microcontrollers[4]. The limited storage on most carriers requires hybrid architectures, where essential information is stored locally and detailed complete product information resides in remote repositories. This strategy introduces challenges in balancing offline accessibility, data sovereignty, privacy, as well as managing authenticated access rights. Storing more data locally, increases offline accessibility, data privacy and sovereignty.

Research Directions We recommend research into optimizing hybrid strategies to balance offline accessibility and privacy, including the use of selective disclosure. Additionally, we suggest exploring methods for specific access control to enhance privacy and user control over locally stored product information.

IV. Online Storage for Product Information

Storing product information online has several advantages, including the ability to update information dynamically, scalability to handle large datasets, and accessibility from various

[3]https://www.qrcode.com/en/about/version.html

[4]https://www.infineon.com/products/security-smart-card-solutions/security-controllers/tegrion-security-controllers

locations and devices. However, it also introduces challenges related to data sovereignty, access control, hosting, interoperability, and legacy integration.

A. Data Sovereignty and Access Control

Online product information management for DPP systems requires compliance with regional regulations, careful access control for different stakeholders, and strong measures to provide trust, data integrity, and privacy. A key component of this is data sovereignty, which encompasses control over data storage locations, access permissions, and governance policies. Achieving this, requires selecting suitable hosting environments, enforcing fine-grained access controls, and maintaining transparency around data usage and ownership.

Architectural choices play a significant role: Centralized storage offers simplicity and ease of management, but can introduce risks such as single points of failure, limited scalability, and vendor lock-in. In contrast, distributed architectures enhance resilience and scalability, though they bring challenges in maintaining data consistency, synchronization, and governance across multiple stakeholders.

In order to achieve best data availability and integrity, resilient backup strategies are essential. Additionally, implementing advanced cryptographic techniques and scalable, interoperable solutions are critical for reliable and secured data management across the DPP ecosystem.

Research Directions We propose to investigate and evaluate scalable frameworks that enforce data sovereignty and granular access control in online product information systems. In particular, hybrid offline-online architectures for DPP systems offer promising aspects for balancing privacy, control, and scalability. This includes exploring fine-grained access control mechanisms such as Attribute-Based Encryption (ABE) schemes, which enable selective disclosure of product information based on user attributes. Furthermore, integrating principles of Self-Sovereign Identity (SSI)[8] can empower individuals to manage their digital identities and associated data. In this context, Decentralized Identifiers (DIDs)[9] provide a compelling strategy for decentralized identity management, supporting secured and user-centric data governance.

B. Hosting

In Table I, we categorize hosting methods for DPP systems, addressing benefits and drawbacks. Centralized hosting stores product data on a server controlled by a single organization, such as a specific, dedicated DPP service provider. Federated hosting involves multiple trusted parties (e.g., industry associations, regulators), who jointly operate and govern the infrastructure. Cloud-based hosting usually uses established commercial cloud providers, such as Amazon Web Services (AWS) or Microsoft Azure for storage and additional services. Distributed Ledger or Blockchain approaches store product data – or references such as hashes – on a decentralized network. Hybrid hosting combines cloud or distributed solutions with local storage on the product. Each method has trade-offs regarding scalability, resilience, data sovereignty, cost, and ease of integration. The choice depends on stakeholder requirements, regulatory constraints such as General Data Protection Regulation (GDPR), and the desired level of decentralization.

Research Directions Future research needs to evaluate different hosting methods for DPP systems in detail, considering the aforementioned factors or specific constraints. This includes exploring hybrid approaches that combine local and remote storage, as well as Distributed Ledger Technologies (DLTs) for enhanced transparency and trust. In case hosting providers cease their operations, solutions for data migration and managing changes in ownership must be investigated.

TABLE I
HOSTING METHODS FOR DPP SYSTEMS.

Method	Benefits (+) / Drawbacks (-)
Centralized	+ Simple management, easy control – Single point of failure, vendor lock-in
Federated	+ Shared responsibility, improved resilience, no dependency on single operator – Coordination overhead
Cloud-based	+ Scalable, flexible, cost efficiency – Data sovereignty, long-term availability
Distributed Ledger / Blockchain	+ Verifiable integrity, better transparency, long-term data persistence – Scalability, privacy challenges
Hybrid	+ Low latency, offline access, resilience – Complexity, integration effort

C. Interoperability and Legacy Integration

Interoperability and legacy integration are crucial for the widespread adoption of DPP systems. Heterogeneous legacy systems with potentially proprietary components, inconsistent interfaces, and irregular data of possibly low quality remain major obstacles. Achieving cross-platform compatibility requires standardized data models, as well as DPP-compliant Application Programming Interfaces (APIs), where open standards and formats can be beneficial. Simple, effortless connectors can ease the integration for small and medium-sized enterprises (SMEs), enabling them to participate in DPP systems without substantial Information Technology (IT) investments. Using lightweight, robust protocols such as Representational State Transfer (REST) and Message Queuing Telemetry Transport (MQTT) can unify modern and constrained environments, enabling reliable communication and integration with existing Internet of Things (IoT) infrastructures. Key challenges include maintaining data quality, consistency, and version control, as well as managing secured access in multi-stakeholder environments. Furthermore, regulatory constraints, such as GDPR, increase the complexity. Solutions should balance immediate legacy compatibility with gradual modernization to keep product information accessible, trustworthy, and future-proof.

Research Directions We propose future research to address challenges in providing semantic data consistency, version control, and secured access management within multi-stakeholder systems. A key aspect is the investigation and

design of standardized, interoperable data models and APIs that enable smooth integration of legacy and modern infrastructures, while providing regulatory compliance. Further work should explore simple onboarding mechanisms for SMEs and robust connectors for heterogeneous IoT and enterprise systems. Additional research needs to investigate concepts and tools for automated data mapping and transformation to support seamless data migration between legacy and modern systems.

V. Updating Dynamic Data

Updating dynamic data concerns a product's lifecycle events, such as utilization, maintenance, repairs, or ownership changes. For instance, a battery passport may track the number of charging cycles and capacity degradation over time throughout its operational life. This process involves mechanisms for securely modifying both local and online product information, while providing data integrity, privacy and fulfilling access policies. It requires robust governance models to define who can read, write, or delete product information under which conditions. Update mechanisms for expiring or invalidating claims (such as end-of-life status or warranty expiration) also need to be established, allowing that outdated or revoked product information is reliably identified and handled throughout a product's lifecycle.

A. Connected Products

For connected products, such as smart home devices or industrial equipment, robust synchronization of product information can be useful. Lightweight protocols and event-driven services should take care that updates are sent efficiently and reliably to minimize resource consumption and network overhead. Scenarios with intermittent connectivity can pose challenges for maintaining up-to-date information. Data minimization principles could be beneficial to selectively disclose and send only relevant information, while data retention policies and responsibilities need to be clearly defined to comply with regulations and privacy standards. Effective update strategies should address version control, provenance, and the need for real-time or event-driven synchronization. Addressing these challenges is vital for maintaining trustworthy, up-to-date digital product passports across multiple usage scenarios.

Research Directions We propose to design and evaluate efficient update mechanisms for connected products, including real-time synchronization, event-driven architectures, version control, and selective disclosure strategies. Investigating the use of lightweight protocols and microservices for reliable data updates can also be beneficial. Additionally, exploring data retention policies and responsibilities in the context of DPP systems can help meet compliance with privacy regulations.

B. Non-connected Products

For non-connected products (e.g., computer monitors, power tools), updates may rely on secured local interactions, such as authenticated NFC transactions during events like repair, maintenance, or inspection activities. Updates may include, for example, operational hours, usage statistics, maintenance records, or component replacement information.

Research Directions We suggest exploring secured protocols for offline updates, usability studies for technician workflows, and mechanisms for conflict resolution when synchronizing offline and online data.

VI. Conclusion

In this paper, we explored the technical design space for DPP systems, focusing on data carriers, online storage, and dynamic data updating. We identified key challenges such as counterfeiting, interoperability, data sovereignty, and access control, and outlined research directions to address them. Our analysis highlights the need for solid, accessible, and future-proof DPP architectures that balance security, privacy, and interoperability, supporting diverse stakeholders throughout the product lifecycle.

Acknowledgment

This work is partly funded by the Lighthouse Project PACE-DPP by the Austrian Federal Ministry for Climate Action, Environment, Energy, Mobility, Innovation and Technology (BMK), supported by the Austrian Research Promotion Agency (FFG) under grant number 917177, as well as from the German Federal Ministry for Economic Affairs and Climate Action (BMWK), supported by the German Research Promotion Agency (DLR-PT).

References

[1] European Parliament and Council of the European Union, *Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 establishing a framework for the setting of ecodesign requirements for sustainable products*, Jun. 28, 2024. Accessed: Jul. 29, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/1781/oj.

[2] J. Monteiro, J. Barata, and S. Gentilini, "A digital twin-based digital product passport," *Procedia Computer Science*, vol. 246, pp. 4123–4132, Jan. 1, 2024, ISSN: 1877-0509. DOI: 10.1016/j.procs.2024.09.251.

[3] M. Pourjafarian et al., "A multi-stakeholder digital product passport based on the asset administration shell," in *2023 IEEE 28th International Conference on Emerging Technologies and Factory Automation (ETFA)*, IEEE, Sep. 2023, pp. 1–8. DOI: 10.1109/ETFA54631.2023.10275715.

[4] I. I. García, F. D. Muñoz-Escoí, J. A. Aroca, and F. J. F.-B. Peñuela, "Digital product passport management with decentralised identifiers and verifiable credentials," *arXiv:2410.15758 [cs]*, no. arXiv:2410.15758, Oct. 21, 2024. DOI: 10.48550/arXiv.2410.15758. arXiv: 2410.15758[cs].

[5] P. Maló et al., "From static records to smart passports: Evolving digital product passports toward product-service system integration," in *2025 21st International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*, IEEE, Jun. 2025, pp. 1087–1094. DOI: 10.1109/DCOSS-IoT65416.2025.00163.

[6] M. Hulea, R. Miron, and V. Muresan, "Digital product passport implementation based on multi-blockchain approach with decentralized identifier provider," *Applied Sciences*, vol. 14, no. 11, p. 4874, Jan. 2024, ISSN: 2076-3417. DOI: 10.3390/app14114874.

[7] J. Picard, P. Landry, and M. Bolay, "Counterfeit detection with QR codes," in *Proceedings of the 21st ACM Symposium on Document Engineering*, ser. DocEng '21, Limerick, Ireland: ACM, Aug. 16, 2021, pp. 1–4, ISBN: 9781450385961. DOI: 10.1145/3469096.3474924.

[8] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, vol. 30, pp. 80–86, Nov. 1, 2018, ISSN: 1574-0137. DOI: 10.1016/j.cosrev.2018.10.002.

[9] C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista, and M. Conti, "A survey on decentralized identifiers and verifiable credentials," *IEEE Communications Surveys & Tutorials*, pp. 1–32, 2025, ISSN: 2373-745X. DOI: 10.1109/comst.2025.3543197.