

Decentralised search and discovery of digital product passports for circular ICT goods

Javier Cano, Pedro Vílchez, Felix Freitag^[0000–0001–5438–479X], and
Leandro Navarro^[0000–0003–4775–5526]

Universitat Politècnica de Catalunya, Barcelona, Spain
<https://dsg.ac.upc.edu>
{javier.cano,pedro.vilchez,felix.freitag,leandro.navarro}@upc.edu

Abstract. The Digital Product Passport (DPP) is an emergent information system that will support conducting circular economy practices with information about a product’s hardware changes along its lifecycle. Diverse circular economy actors will add and use information to a product’s DPP. Actors include product manufacturers, and we explore how value chain operators, including repairers, refurbishers, and recyclers, can also update it, keeping updated product hardware information available to end users. This paper focuses on a distributed search and lookup service for DPPs. We have designed and prototyped this distributed search service within a DPP system for circular ICT goods. We show that the search service allows end users to find DPPs and validate the obtained information and actors involved in terms of integrity and authenticity. Our prototype is built with a set of microservices, where a verifiable data registry implemented with a DLT provides a shared source of truth and chain of trust for the different events and actors that modify the DPP information of a product item during the product’s lifetime.

Keywords: Digital Product Passport · blockchain · distributed search.

1 Introduction

As part of the effort to increase the sustainability of products, the Digital Product Passport (DPP) is a system aiming at improving the circularity and environmental sustainability of products. In July 2024, the “Ecodesign for Sustainable Products Regulation” (ESPR) entered into force, which in articles 9 to 15 draws the principal elements of the future DPP [1]. The DPP will be obligatory for various products, commencing with batteries and extending to electronic devices, textiles, etc. On the global scope, ITU-T recommendations about the DPP for ICT goods were published in [2] and [3], and there is an ongoing development of the UNTP B2B DPP [4].

The DPP will provide trusted product information related to sustainability, like environmental footprints, and circularity, like events on repairs or refurbishment for the second-hand market in a standardized format. The transparency of the data will facilitate the involvement of economic and independent actors in improving the circularity of their processes throughout a product’s lifetime. The capacity of the DPP system to deliver trust in the data is essential for every actor to make the correct informed

decisions. Then, information about a product’s environmental footprint can be accounted for, and more information and automation can improve the recycling process. Repair, refurbishment, and reuse of products may increase and improve quality.

However, the path to the large-scale deployment of DPP systems faces many challenges in becoming operational and effective. In [5], the issue of the many actors in a product’s supply chain is highlighted. For an effective circular economy monitoring, the DPP system must allow the diversity of actors (e.g., large manufacturers as well as small refurbishers) to operate on a product’s DPP data. In [6], the implementation of the future DPP is identified as a System-of-Systems, instead of a single technical system. This increases the difficulty of the architecture which not only requires technical, but also legal, semantic, and organizational interoperability. In [7], a set of six design principles (holistic data capture, data privacy, decentralized data administration, forgery-proof data, automated passport processing, and interoperability) are distilled to guide the development of DPP systems.

Applying a bottom-up approach, we have prototyped a DPP system for the circular management of ICT devices. Our prototype represents a DPP system where individual devices have configurations, associated documents, associated metadata, and sub-components. The prototype considers products at the item level of granularity. The device data and documents part of the DPP are stored on a device inventory service with multiple service instances. The system records proofs of the different events, such as operations on the product item on a verifiable data registry, leveraging a distributed ledger shared across all inventory service instances. Data adding and data retrieval involves a verifiability service that provides trust in the DPP data. DPPs evolve through newly issued DPPs that link to previous ones, according to an open-web model.

In this paper, we introduce the keyword and product identifier based search service publicly available to find the DPPs for a product model or product item. In an iterative process, we show how the user can refine the search process to obtain guarantees on the authenticity of the looked-up data and actors involved. Furthermore, we highlight key design decisions that can generalise a trusted distributed search service to multiple DPP systems.

2 Background and related work

Several authors have conducted survey works on the DPP. For instance, Wicaksono et al. [8] provide a recent review on DPP technologies and adoption. The authors look at the dimensions of technological enablers, the effects of the DPP on circular economy practices in the industrial sector, and the economic and regulatory implications of integrating the DPP. Their findings identify the Ecodesign for Sustainable Products Regulation (ESPR) as a central regulation on which adoption should be based in the EU. For data management, both the business perspective for handling sensitive information and the consumer’s for being provided with a user-friendly representation of data are remarked. Hence, DPP data along the product lifecycle should be shareable with humans and machine-readable. Regarding technologies, the role of Decentralized Identifiers (DIDs) anchored on a blockchain is highlighted.

In Zhang et al. [9], the use cases of the DPP for a circular supply chain management are investigated. For this, the authors performed a literature review. As part of the supply chain actor identification, the potential sustainability effect of the DPP when used by repair shops, second-hand goods marketplaces, and recyclers is analyzed. Several directions are identified to achieve sustainable and circular supply chain management. The findings indicate the need to improve user engagement and that increased trust in the supply chain would change user behaviour.

In the work of García et al. [10], the focus is on DPP management using DIDs and Verifiable Credentials (VCs). After analyzing the landscape of regulations and, in particular, the specific requirements of the ESPR, the authors argue for a technical solution based on DIDs and VCs. For this, they show to which extent the nine identified requirements can be addressed with these techniques. Experiments that measure performance are not part of this paper, but the technical issues and solutions are discussed theoretically.

The work of Voulgaris et al. [11] proposes a circular economy framework with integrated DPP characteristics. The topic is addressed from the perspective of data management. The authors review the technologies used for data collection, data curation, data sharing, and data leverage. The fields of IoT for data collection, AI for data curation, and blockchain for data leveraging and sharing are highlighted. The paper comments that a thorough evaluation of combining the enabling technologies is still lacking. At the same time, the adaptivity of the frameworks for the different industries and application fields may be an issue for further research.

Within the works that have included a Distributed Ledger Technology (DLT)-based verifiable data registry as part of the DPP prototype system, Nowacki et al. [12] presented a technical architecture for a DPP system. The system is described from the use case angle. It looks at the different stages of the lifetime of a product, resulting in a use case framework where various actors, such as producers, manufacturers, retailers, and consumers, are presented. The framework is mapped into a high-level technical architecture. While end users are stated, their interactions within the architecture of the DPP system are not further detailed. A DPP lookup function is introduced, however not related to a search, instead, it uses a DPP identifier.

In light of the above works, reporting practically working prototypes with technical operations seems to be still rather limited. While the works stress the importance of integrating the user needs, both economic actor and consumer, most works seem to focus on the economic actors of the supply chain while looking less at the end-user needs of the DPP.

3 System Architecture

We focus on a DPP system for electronic devices (ICT goods), specifically second-hand computers. The DPP system stores information about devices and records events during the device's lifetime in one among several inventory service instances. Each device is associated with some data, such as specific documents about its configuration, components, and environment data, and other product model-level documents, such as manuals and certificates.

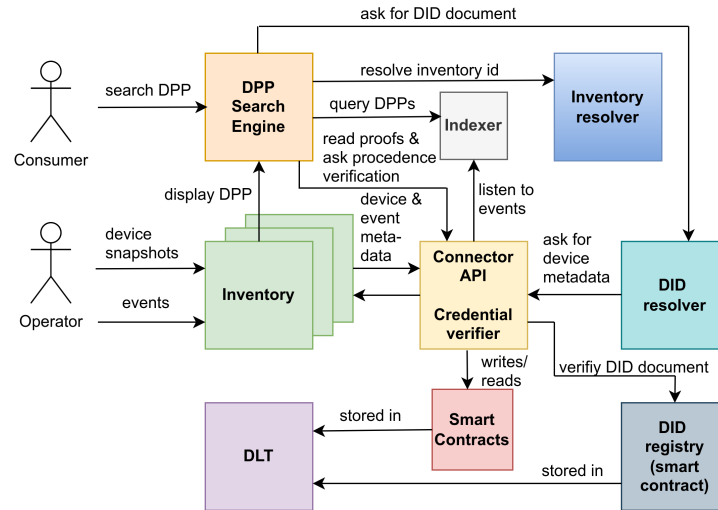


Fig. 1. Architectural components and main interactions.

Devices are abstracted away as a chassis that wraps specific child components that define a device configuration during its lifespan. Thus, DPPs in this system are resolved through an identifier that results from the composition of a unique chassis identifier (*CHID*) of the device (that is derived from the type, manufacturer, model, and serial number) immutable during the product lifespan, plus a configuration identifier, also known as product hardware identifier, (*PHID*) that can change when internal components are substituted. For instance, in the case of a laptop, its configuration depends on the brand, model, and serial number. Should a main component, such as its SSD drive, be changed, the physical chassis and its identifier will remain, while the hardware configuration will change, leading to a new identifier. Thus, a new DPP will have to be issued. This is a unique characteristic of this use case where the product, the overarching device incarnated by its chassis and particular configuration, is dynamic, flexible, and subject to eventual change.

Unique device identifiers (Chassis ID or CHID) can be looked up in the search engine to find the DPP for each device configuration (Product Hardware ID or PHID). The lookup process has been implemented in tandem with a DPP search engine.

The DPP system is operated by actors. We consider two main roles, an *operator* and a *consumer*. The operator interacts with an inventory-like Web-based component of the DPP system. The operator can create a new device (item level) in one inventory service instance without previous information about the device's identifier, typically the instance operated by the product owner or the product refurbisher. If the device already exists in the inventory system, the operator can add information about events in the device's lifespan, such as hardware changes. Operators authenticate and get authorised according to their credentials as qualified independent operators with the inventory system to report an operation that changed the product information and,

therefore, the item's DPP. The inventory system contains the DPP data. However, to be able to trust these data, additional services with which the inventory interacts must come into play to verify the authenticity of the data.

As part of the DPP system, many instances of the inventory system can exist under different administrative domains used by various operators. The DPP data stored in any inventory needs to be truthful, verifiable on integrity and authenticity. For data integrity, a common verifiable data registry shared by all inventory service instances is used. Each inventory then communicates summaries of the operations on the devices under their inventory with the corresponding data to a verifiable data registry as a ledger. Records about product-related operations stored in the verifiable data registry contain hashes and metadata relating verifiability information with the detailed DPP information on any DPP. For authenticity, operations and claims are signed, and the signatures must be verifiable. A device can be transferred to a new owner or operator and therefore its history and hardware configuration can come from multiple service instances. The ledger can inform about these, with the same *CHID* but different *PHIDs* and allow to find all and the current hardware configuration and inventory service instances involved.

The consumer can search for any DPPs identifier recorded in the ledger through a search service instance. A consumer can represent, for example, an end-user, auditor or inspector, or a market surveillance authority. The consumer, however, is not a registered user of an inventory system. The consumer's usage of the DPP system is to find DPPs, while an operator can write or modify the DPP data. For this, the consumer accesses a search service aware of the DPPs created in the different inventories. The approach we apply to make any search service knowledgeable about the DPPs is to track the DPP summaries that are written to the verifiable data registry. Therefore a search service instance feeds its index from the ledger as source of truth and complements it with additional details from the corresponding DPP inventory instances for each product item.

Figure 1 gives an overview of the system architecture. The two main actors, the operator and the customer, appear. They interact with different components of the DPP system. The inventory is built as a Web application that stores data about devices in DPPs. It contains a REST interface to interact with other components and a Web interface for the operator. Through the Web interface, the operator creates events and uploads device data, e.g., to create a new DPP if the item does not exist, or creates events, such as a hardware change on an existing DPP to issue an updated one (same *CHID* but different *PHID*). The smart contracts in the DLT component form the verifiable data registry, the ledger for summaries of the inventory's data. A blockchain-based implementation ensures the immutability of the data stored in the smart contracts. The connector API facilitates abstracting the specifics of different technological distributed ledger solutions.

The indexer component tracks metadata for the DPP search engine about DPP creation operations that are processed through the connector API. Based on this data, the search service can present DPP summaries to the consumer. On request, with that metadata in the smart contract summaries, the DPP search engine can query the inventory resolver to obtain the URL of the inventory instance containing the

DPP data. Furthermore, the DID resolver component provides the DID document to the search service to query the specific DPP about product details in the inventory.

For the authenticity of the data, we apply an European Blockchain Service Infrastructure (EBSI)-compatible Trust Framework [13]. The actors, e.g., operators, have DIDs. The DID document that contains an actor’s public key and its roles is signed by a trusted issuer. An actor’s operation, such as DPP creation or an event on an existing DPP, is signed with the key associated with the actor’s DID. The DID verifiable data registry contains the information to validate the signature and the role in the actor’s DID document (including accreditation for that role from an authority, a Trusted Authority Organisation (TAO) or Trusted Issuer (TI) in EBSI terms. When an operator conducts an operation, the signature and role are validated. Similarly, when DPP data is obtained by the search service, the authenticity can be verified by validating the chain of signatures.

4 Implementation

We have implemented a proof of concept prototype of the system architecture¹. In the following, we look more in-depth into the search function that the DPP provides.

4.1 Search user interface

Figure 2 shows the Web interface of the search service that is initially available to the consumer. The user can conduct keyword-based research for DPPs or introduce item-specific information to search for a specific DPP: the most recent associated to the chassis CHID, the current DPP, or the corresponding to a specific hardware configuration given by a CHID:PHID identifier.

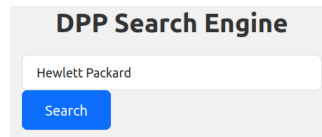


Fig. 2. Search service initial Web user interface, for keyword- or item-based search.

When a keyword-based search is performed, a list of DPPs that match the keyword (Figure 3) are returned. The user can click on one to obtain more details about that device.

Figure 4 shows a more detailed view of a selected device. The user can click on components to access detailed information or proofs to request data validation, as the basis for this information comes from the ledger as the source of truth. The search service provides a direct DPP inventory link. That will deliver the HTML-rendered DPP informative details.

¹ Source code: <https://gitlab.com/dsg-upc/ereuse-dpp/>

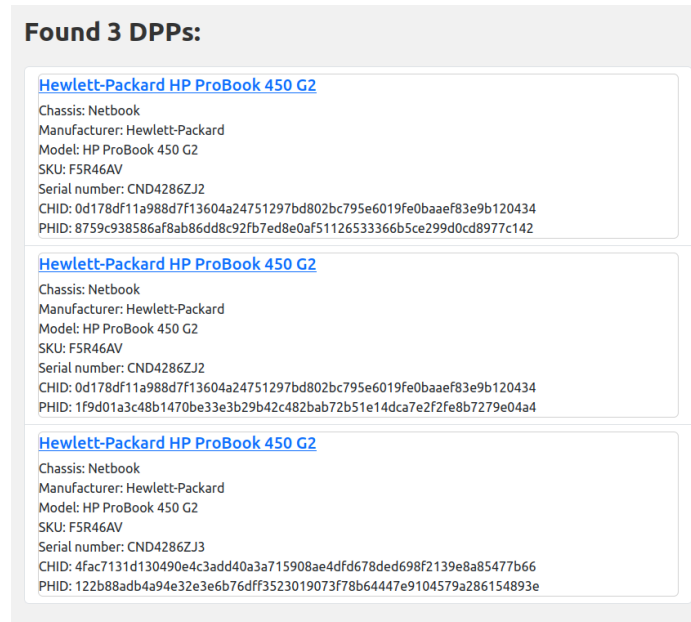


Fig. 3. Search service HTML rendering of information retrieved from indexer service.

Figure 5 shows the DPP product information retrieved from the inventory. Rendered in HTML, it is presented in a user-friendly format. As introduced in section 3, the search service’s knowledge of DPPs is gained from capturing DPP creation events recorded in the verifiable registry, specifically smart contracts in a blockchain-based distributed ledger. The product’s DPP metadata in the smart contract record contains the product identifier and inventory identifier, which allow the DPP Search Engine, with the help of resolver services, to resolve the path to the full DPP data.

Figure 6 exemplifies how the user can verify the DPP data through the search service as a trusted third party. Specific events that changed the DPP information, such as a DPP creation, can be verified by providing details about the event and the actors involved. Verification of the signatures related to the found DPP information is available through the trust chain validation.

4.2 Discussion of results

The DPP Search Service provides a trusted DPPs look-up function and a verification function. The verification process obtains information from different sources on the verifiable data registry. When an operator creates an event that is part of the product’s DPP, its signature and role are verified, and the event metadata is stored in a smart contract of a blockchain-based distributed ledger. Verifying the smart contract metadata demonstrates the authenticity of the data. Verifying the trust chain implies checking with a DID on the verifiable registry. Another smart contract is implemented

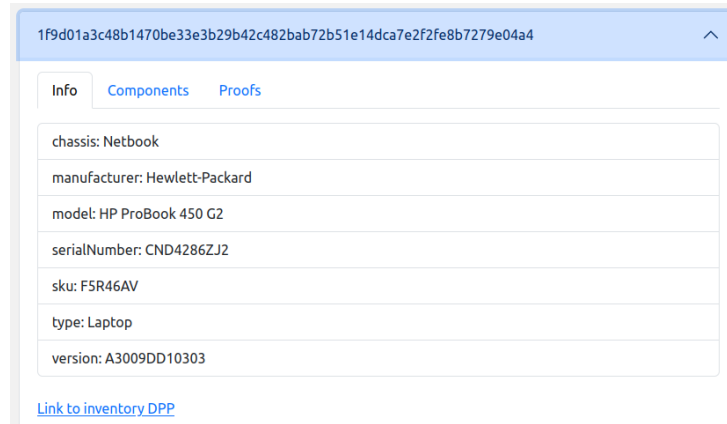


Fig. 4. The search service offers ledger details combined with extended product information from the corresponding inventory product item and a link to DPP details there.



Fig. 5. Rendering of the product's DPP in HTML format delivered by the inventory service.

in our prototype for this role verification. Still, in other implementations, the DID verification may be an external third-party service used by the DPP system.

Our search service prototype uses an indexer service to track the creation of DPPs when their metadata is written to the verifiable data registry. This demonstrates the lookup and verification capability. However, it can be expected that this functionality will be provided by a trusted DPP registry operated by regulators [1] following the EBSI model [13].

The search engine prototype allows global searching and finding DPPs of products starting from the metadata recorded in a verifiable data registry as the source for trusted information. This solution chosen achieves that the search service is not

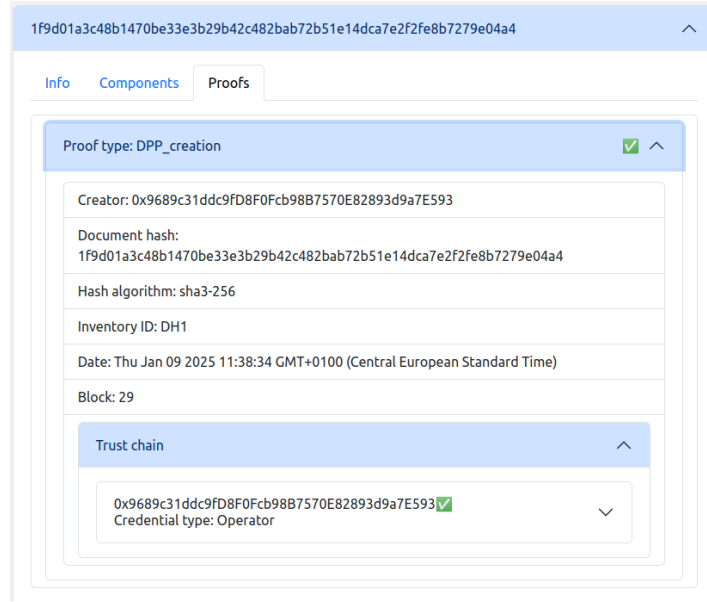


Fig. 6. The search service can validate for the user the DPP information it found.

restricted to the DPPs stored at a specific inventory instance but, through an inventory resolver, can discover any DPP associated to a given product chassis even with different hardware configurations at multiple inventory instances.

5 Conclusions

We presented a prototype of a trusted distributed search service that interacts with a DPP system to find product item DPPs based on a keyword- or item-based search for products that change along a long and circular lifespan. Starting from metadata taken from a trusted and common verifiable data registry, the service allows the users to obtain the complete and verified DPP information from DPP at multiple inventory service instances. The implementation consists of an operational prototype for demonstrating the search and verification functionalities.

Future work aims to understand the generalization opportunity of the search service for application to other emerging DPP systems of different products. This will involve analyzing which common source of truth and trust can be used and how third-party services, e.g. DID verifiable data registries and verifiable credentials, can be interconnected with the DPP system.

Acknowledgments. This work has been funded by the HORIZON-RIA Next Generation Internet Discovery and Search project (g.a. 101069364), and the Horizon Europe NEO-CYCLE project (g.a. 101138058), and the Spanish Ministerio de Ciencia Innovación y Universidades (g.a. PID2023-146066OB-I00, AEI 2023 Knowledge Generation Projects), and the Generalitat de Catalunya (g.a. 2021-SGR-01059).

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Commission, E.: Ecodesign regulation. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0303_EN.html (2024) European Parliament legislative resolution of 23 April 2024 on the proposal for a regulation of the European Parliament and of the Council establishing a framework for setting eco-design requirements for sustainable products and repealing Directive 2009/125/EC (COM(2022)0142 – C9-0132/2022 – 2022/0095(COD)). Accessed: 2025-02-22.
2. ITU-T, U.N.: ITU-T L.1070: Global digital sustainable product passport opportunities to achieve a circular economy. <https://handle.itu.int/11.1002/1000/15598> Accessed: 2025-02-22.
3. ITU-T, U.N.: ITU-T L.1071: A model for digital product passport information on sustainability and circularity. <https://handle.itu.int/11.1002/1000/15995> Accessed: 2025-02-22.
4. for Europe, U.N.E.C.: UNECE Policy Recommendation No. 49: 'Transparency at Scale'. https://uncefact.unece.org/download/attachments/231866398/UNECE_Recommendation_49_v1.6_plain_16.02.2025.pdf?api=v2 Accessed: 2025-02-22.
5. Rukanova, B., Ubacht, J., Tan, Y.H.: Border crossing and circular economy monitoring in a global context: Challenges and opportunities. In: Proceedings of the 25th Annual International Conference on Digital Government Research. dg.o '24, New York, NY, USA, Association for Computing Machinery (2024) 331–340
6. King, M.R., Timms, P.D., Mountney, S.: A proposed universal definition of a digital product passport ecosystem (dppe): Worldviews, discrete capabilities, stakeholder requirements and concerns. *Journal of Cleaner Production* **384** (2023) 135538
7. Heef, P., Rockstuhl, J., Körner, M.F., Strüker, J.: Enhancing trust in global supply chains: Conceptualizing digital product passports for a low-carbon hydrogen market. *Electronic Markets* **34**(1) (Jan 2024) 10
8. Wicaksono, H., Mengistu, A., Bashyal, A., Fekete, T.: Digital product passport (dpp) technological advancement and adoption framework: A systematic literature review. *Procedia Computer Science* **253** (2025) 2980–2989 6th International Conference on Industry 4.0 and Smart Manufacturing.
9. Zhang, A., Seuring, S.: Digital product passport for sustainable and circular supply chain management: a structured review of use cases. *International Journal of Logistics Research and Applications* **0**(0) (2024) 1–28
10. García, I.I., Muñoz-Escóf, F.D., Aroca, J.A., Peñuela, F.J.F.B.: Digital product passport management with decentralised identifiers and verifiable credentials (2024)
11. Voulgaridis, K., Lagkas, T., Angelopoulos, C.M., Boulogeorgos, A.A.A., Argyriou, V., Sarigiannidis, P.: Digital product passports as enablers of digital circular economy: a framework based on technological perspective. *Telecommunication Systems* **85**(4) (Apr 2024) 699–715
12. Nowacki, S., Sisik, G.M., Angelopoulos, C.M.: Digital product passports: Use cases framework and technical architecture using dlt and smart contracts. In: 2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT). (2023) 373–380
13. Commission, E.: Introducing ebsi. Available at: <https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home> (2024) Accessed: 2025-02-22.