CIRPASS 2
Digital Product Passport

D4.1 REFERENCE ARCHITECTURE

12/05/2025

Funded by
the European Union

D4.1 REFERENCE ARCHITECTURE

VERSION 1.0 (12 MAY 2025)

Work package	WP Number
Task	T4.1
Due date	15/05/2025
Submission date	12/05/2025
Deliverable lead	TNO
Version	1.0
Authors	Huib van Nieuwenhuijze (TNO), Kartik Chawla (TNO), Noah Smeets (TNO), David Roefs (TNO), Sjoerd Rongen (TNO), Jesper Kuiper (TNO), Rik Rurup (TNO), Mohammed Nacer Lazrak (TNO), Carolynn Bernier (CEA), Sebastien Gerard (CEA), Tiphaine Henry (CEA), Tanel Tammet (TalTech), Rain Eisler (TalTech), Alessia Matruglio (Innovalia), Marco Volpini (ExtraRed)
Reviewers	Jelte Bootsma (TNO), Pekka Raittila (IOXIO), Rik Holvoet (TripleR), Simen Kjellberg (Kezzler), Ann Dao (CEI), Marc-Andree Wolf (maki Consulting), Staffan Olsson (GS1), Marvin Böll (VDE), Kamila Anna Kocia (atma.io). Henna Suomi (IOXIO), Sebastian Schröder (DKE), Limara Hague (OBADA) & many other contributors from the CIRPASS2 consortium.
Abstract	This document describes the reference architecture of the DPP system. This architecture is intended to bridge the gap between the intentions of the European regulators, as expressed in the ESPR, and the companies developing components of the DPP system. The purpose of this architecture is to elaborate, reason and illustrate what the DPP system could look like, and enables the specification of programming interfaces and development of software components in the next steps of the CIRPASS-2 project.
Keywords	System architecture, Digital product passports, ESPR
Citation	van Nieuwenhuijze, H., Chawla, K., Smeets, N., Roefs, D., Rongen, S., Kuiper, J., Rurup, R., Lazrak, M. N., Bernier, C., Gérard, S., Henry, T., Tammet, T., Eisler, R., Matruglio, A., & Volpini, M. (2025). D4.1 Reference Architecture. CIRPASS-2 Consortium. https://doi.org/10.5281/zenodo.15388412

Document Revision History

Version	Date	Description of change	List of contributor(s)
0.1	26-11-2024	Creation of document	
0.2	14-02-2025	Major revision to structure of chapter “building blocks view”, such that application services are divided in a	

		design and run time view	
1.0	12-05-2025	Finalizing document based on feedback from the consortium	

CIRPASS CONSORTIUM

#	Participant Organisation Name	Short Name	Country
1	Commissariat A L´Energie Atomique Et Aux Energies Alternatives	CEA	France
2	Tallinna Tehnikaülikool	TALTECH	Estonia
3	Mindworks Industries Ou	MWX	Estonia
4	DIGITALEUROPE AISBL	DIGITALEUROPE	Belgium
5	E CIRCULAR APS	E CIRCULAR APS	Denmark
6	F6s Network Ireland Limited	F6S IE	Ireland
7	Global Textile Scheme GmbH	GTS	Germany
8	maki Consulting GmbH	MAKI	Germany
9	Ekodenge Muhendislik Mimarlik Danismanlik Ticaret Anonim Sirketi	EKODENGE	Türkiye
10	Stiftelsen Chalmers Industriteknik	CIT	Sweden
11	Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek TNO	TNO	Netherlands
12	BIO Innovation Service SAS	BIOIS	France
13	Technische Universiteit DELFT	TU Delft	Netherlands
14	Asociacion De Empresas Tecnologicas INNOVALIA	INNOVALIA	Spain
15	CBT Comunicacion & Multimedia SL	CBT	Spain
16	Asociacion Para Desarrollo De La Economia Del Dato	BAIDATA	Spain
17	GS1 In Europe	GS1 IN EUROPE	Belgium
18	AOC Innovation	AOC INNOVATION	France
19	+IMPAKT Luxembourg SARL	+IMPAKT	Luxembourg
20	Industrie 4.0 Osterreich - Die Plattform Fur Intelligente Produktion	PIA	Austria
21	FUJITSU Technology Solutions	FJBE	Belgium
22	Fraunhofer Gesellschaft Zur Forderung Der Angewandten Forschung EV	Fraunhofer	Germany
23	Extra Red SRL	EXTRA RED SRL	Italy

24	European Apparel And Textile Confederation Aisbl	EURATEX	Belgium
25	IOXIO OY	IOXIO OY	Finland
26	Suomen Tekstiili Ja Muoti Ry	FINATEX	Finland
27	KEZZLER AS	Kezzler	Norway
28	EON Cloud Technology KFT	EON	Hungary
29	Avery Dennison Atma GmbH	atma.io	Austria
30	Circular.Fashion UG	circ.fashion	Germany
31	TRIPLER	TripleR	Belgium
32	SCANTRUST BV	SCANTRUST BV	Netherlands
33	ARCELIK A.S.	ARCELIK	Türkiye
34	WHATT.IO AB	whatt.io	Sweden
35	Gorenje Gospodinjski Aparati DOO	GORENJE	Slovenia
36	Manufacture Francaise Des Pneumatiques MICHELIN	MICHELIN	France
37	COBUILDER AS	COBUILDER	Norway
38	DIN Deutsches Institut Fuer Normung EV	DIN e.V.	Germany
39	VDE Verband Der Elektrotechnik Elektronik Informationstechnik EV	VDE	Germany
40	Energy Web AG	Energy Web AG	Switzerland
41	WORLDLINE France	WORLDLINE FR	France
42	Physikalisch-Technische Bundesanstalt	PTB	Germany
43	Digital Data Chain Consortium GbR	DDCC	Germany
44	ZVEI e. V.	ZVEI e.V.	Germany
45	Association of Service and Computer Dealers International	ASCDI	US
46	Open Blockchain for Asset Disposition Alliance (OBADA)	OBADA	US
47	Green Electronics Council	GEC	US
48	Textile Exchange	TextileExchange	US
49	iPoint-Systems GmbH	iPoint	Germany

Grant Agreement No.: 101158775
Call: DIGITAL-2023-CLOUD-DATA-04
Topic: DIGITAL-2023-CLOUD-DATA-04-DIGIPASS
Type of action: DIGITAL Simple Grants

DISCLAIMER

Funded by the European Union under the GA No 101158775. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

COPYRIGHT NOTICE

OBJECTIVE OF THIS DOCUMENT

The purpose of this document is to propose a Digital Product Passport (DPP) system architecture, compliant with the Eco-design for Sustainable Products Regulation (ESPR). This document is intended for designers and developers of Digital Product Passport systems, as well as for the European Commission. The architecture describes the building blocks of a DPP system, the relationships between these building blocks, and an indication which types of roles would typically use each building block. In addition, it highlights commonly used standards relevant for building blocks. Furthermore, recommendations are made about DPP system aspects that benefit from ecosystem level collaborations and agreements. Finally, it describes key technical risks that arise when implementing the DPP system and mitigations to counter these.

Disclaimer

TABLE OF CONTENTS

LIST OF FIGURES

GLOSSARY & ABBREVIATIONS

Entries marked with " ⚖ " are based on their respective definition in Art. 2, ESPR.

'Actor' means an organization or individual (e.g. John Doe, TNO) that fulfils a role[1]. One actor can take on multiple roles.

'Application Service' means an application service represents an explicitly defined exposed application behaviour[2]. This means a specific technical service that the *DPP system* can perform (e.g. DPP data repository, redirection service).

'Availability' means a measure of performance obtained by dividing the time during which the equipment or system is operational by the total time during which it should have been operational [3].

'Building Block' is used as a synonym of 'Application Service' , but also includes governance logic, and interoperable data functions used to enable DPP system capabilities.

'Credentials Agency' ⚖ means a legal person that provides (professional) credentials to parties, which may be used to make and verify a variety of claims in the DPP (Art. 11, last paragraph).

'Confidentiality' means the property of ensuring that information is not made available or disclosed to unauthorized individuals, entities, or processes.[4]

'Data authentication' means ability to verify that data originates from a legitimate, authorized source, whether first-party (manufacturer, producer) or third-party (certifying bodies, regulators).

'Data reliability' means the ability to substantiate a claim or establish the right of an entity to make a claim about a product.

'Data carrier' ⚖ means "*a linear barcode symbol, a two-dimensional symbol or other automatic identification data capture medium that can be read by a device*" (ESPR article 2(29))[5]

'Data model' means a **"***structured representation of data elements and relationships used to facilitate semantic interoperability within and across domains*" as defined by DSSC[6]

'Delegated Act' are non-legislative acts in the EU, which in the context of the ESPR will be passed under to supplement or amend parts thereof, specifying, *inter alia*, obligations for economic operators, information requirements related to product aspects, requirements for specific product groups.[7]

---

[1] ISO 23234:2021
[2] ArchiMate® 3.2 Specification
[3] Availability (Wikipedia)
[4] ISO/IEC TR 27550:2019
[5] It is understood that the data carrier itself may contain only the unique product identifier or a web link which enables locating the DPP data. Should the data carrier not contain a web link, it is understood that dedicated means will be defined to construct one (e.g., a professional application used exclusively in B2B contexts or a DPP link search portal).
[6] Data Models - Blueprint v1.0 - Data Spaces Support Centre
[7] Delegated acts - EUR-Lex

'Digital Product Passport' (DPP) ⚖ **means "***a set of data specific to a product that includes the information specified in the applicable delegated act, and that is accessible via electronic means through a data carrier*" (Art. 2(28), ESPR).

'DPP Service Provider' (DPPSP) ⚖ **means "***a natural or legal person that is an independent third-party authorized by the economic operator which places the product on the market or puts it into service and that processes the DPP data for that product for the purpose of making such data available to economic operators and other relevant actors with a right to access those data under this Regulation or other Union law*" (Art. 2(32), ESPR).

'DPP system' means a set of building blocks and the roles that deploy or perform these services, as required for the ESPR's requirements for DPPs (e.g., Art. 9 and 10, ESPR) and additionally optional building blocks.

'DPP ecosystem' means the complete set of actors and systems that create or use DPPs, and the interactions between these actors and systems.

'DPP template' means a template which can be used when creating a DPP. Templates are based on a product-category specific set of available ontological elements to be used for a DPP of any specific product (on model, batch or item level) that belongs to the respective product category, but can be extended when desired.

'Economic Operator' ⚖ **means "***the manufacturer, the authorized representative, the importer, the distributor, the dealer and the fulfilment service provider*" (Art. 2(46), ESPR).

'End User' ⚖ means **"***any natural or legal person residing or established in the Union, to whom a product has been made available either as a consumer outside of any trade, business, craft or profession or as a professional end user in the course of its industrial or professional activities*" (Art. 2(2), Market Surveillance Regulation (EU) 2019/1020, as cited by the Art. 2 ESPR).

'EU Registry' ⚖ means the DPP registry to be set up by the European Commission to store in a secure manner at least the unique identifiers linked to products placed on the market or put into service in the EU (Art. 13(1) and Recital 41, ESPR).

'Granularity level' means the level at which DPPs are created, in accordance with the relevant delegated act. This can be at model, batch, or item level.

- **'Model level'** means a version of a product of which all units share the same relevant characteristics, e.g., all units being produced within a set of designated factories
- **'Batch level'** means a subset of a specific model composed of all items produced in a similar way, e.g., a group of products made in the same factory within a specific timeframe.
- **'Item level'** means a single unit of a model, e.g., an individual product.

'Data Integrity' means the ability to demonstrate that data in a DPP has not been altered, removed, or corrupted over time.

'Interoperability' means "*the ability of organizations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organizations, through the business processes they support, by means of the exchange of data between their ICT systems*"[8].

'Issuing Agency' means an organization tasked with providing identifiers to parties, in compliance and accordance with the appropriate requirements and standards, as required under Art. 12 (4).

'Link' means **"***a conceptual construct […] that represents a connection between two resources*"[9]

'Product Group' ⚖ *means* "*a set of products that serve similar purposes and are similar in terms of use, or have similar functional properties, and are similar in terms of consumer perception*" (Art. 2(5), ESPR).

'Public Authorities' means an entity or individual carrying out statutory duties or other public functions assigned to it by law, for instance a customs authority or a market surveillance authority.

'Redirection service'[10] means a building block that takes as an input a unique product identifier (or a weblink based a product identifier) and produces as output one or more 'active' weblinks that enable access to a (set of) other building block(s).

'responsible Economic Operator (rEO)' means an economic operator that has the legal obligation to create and/or to make available a DPP under Art. 9(2)(g) of the ESPR, and all associated legal obligations.

'Role' means a set of tasks typically performed by one *actor*. (e.g. rEO, Independent operator).

'Supply Chain Actor' means a legal person that performs an upstream activity or participates in a process of the product's value chain, up to the point where the product reaches the consumer.

'Unique facility identifier' ⚖ *means* **"***a unique string of characters for the identification of locations or buildings involved in a product's value chain or used by actors involved in a product's value chain*" (Art. 2(33), ESPR).

'Unique operator identifier' ⚖ *means* **"***a unique string of characters for the identification of an actor involved in a product's value chain*" (Art. 2(31), ESPR).

'Unique product identifier' ⚖ *means* **"***a unique string of characters for the identification of a product that also enables a web link to the DPP*" (Art. 2(30), ESPR). The term '*enables*' is understood to mean that, if needed, the unique product identifier can be used by a redirection service.

'Unique registration identifier' ⚖ means a unique string of characters associated with the unique identifiers uploaded by the economic operator to the EU registry for a specific product" (Art. 13(5), ESPR).

'User' means the actor which uses the DPP system to perform a task.

---

[8] European Commission, New European Interoperability Framework (2017)
[9] World Wide Web Consortium, HTML5 A vocabulary and associated APIs for HTML and XHTML (2014)
[10] In previous documents this was often referred to as a 'resolver'. As this term has a very specific meaning in certain contexts, this caused confusion. 'Redirection' more precisely covers the function required and aligns with Options for redirection (CIRPASS-2).

'User Story' means a short description from the perspective of a user that describes a result the user would like to accomplish, and involves an interaction with the system. In this document a user story follows the format: "as a <role>, I want <goal>, so that <benefit>".

'Voluntary data' means data which is added to a DPP, which is not required by the ESPR or a Delegated Act. Organizations have many reasons to include this data, such as certifications, instruction manuals or company-specific traceability data.

'Web portal' ⚖ means the publicly accessible and user-friendly digital product passport web portal to be set up by the European Commission which guarantees stakeholders, such as customers, economic operators and other relevant actors, the ability to search for and compare data included in DPPs in a manner consistent with their respective access rights (Art. 14 and Recital 42, ESPR).

Abbreviation	Full form
API	Application Programming Interface
B2B	Business-to-Business
CRUD	Create, Read, Update, Delete
DID	Decentralized Identifier
DPP	Digital Product Passport
DPPSP	DPP Service Provider
DSSC	Data Spaces Support Centre
EC	European Commission
eIDAS	electronic Identification, Authentication and Trust Services
EO	Economic Operator
EPREL	European Product Registry for Energy Labelling
ESPR	Eco-design for Sustainable Products Regulation
IAM	Identity and Access Management
IO	Independent Operator
JWT	JSON Web Token
LCA	Life Cycle Assessment

PKI	Public Key Infrastructure
RBAC	Role-Based Access Control
RDF	Resource Description Framework
rEO	responsible Economic Operator
RFC	Request for Comments
RFID	Radio-Frequency Identification
SME	Small and Medium-sized Enterprise
UPI	Unique Product Identifier
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUID	Universally Unique Identifier
VC	Verifiable Credential

1 INTRODUCTION

The purpose of this document is to propose a Digital Product Passport (DPP) system architecture, compliant with the Eco-design for Sustainable Products Regulation (ESPR). It also aims to increase the opportunities for commercial business beyond regulatory compliance. A DPP system can be seen as a set of interconnected building blocks using common technical specifications and standards, which facilitate interoperability of cross-sectorial DPPs. This document aspires to complement the ongoing standardization work done by CEN-CENELEC JTC 24 but should not be interpreted as reflecting the design choices of CEN-CENELEC JTC 24.

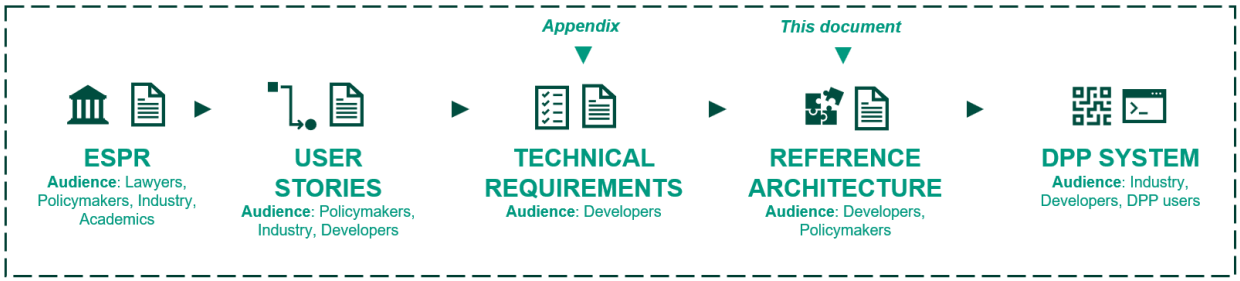


FIGURE 1: CONTEXT OF THE REFERENCE ARCHITECTURE DOCUMENT

Scope

The intended audience of this document are policymakers of the European Commission and developers of ESPR-compliant DPP systems. The reference architecture consists of the following parts:

1. A set of building blocks that support interactions between the DPP system and its users;
    a. Intent: This document is a follow-up on the DPP User Stories V3[11]. The User Stories describe the interaction between a DPP system and its users. These interactions relate to creating, accessing, updating, and deleting a DPP. This proposed system architecture describes the building blocks that must or should be part of the DPP system to support the interactions identified in the User Stories. The building blocks are grouped by 'role' (e.g., responsible Economic Operator, Independent Operator, etc.). The grouping is indicative and may be different in DPP system implementations. For each building block, the expected input, output, and recommendations for implementation are described.
    b. Intended use: gain a deeper understanding of which functionality a DPP system would typically offer and must offer.
2. A set of key architectural recommendations that aim to resolve challenges in implementing the DPP system architecture at an ecosystem level between DPP systems;
    a. Intent: to support the implementation of and interoperability between DPP system. The recommendations detail aspects related to the following concerns: semantic interoperability, identity and access management, DPP access, DPP integrity, data management, and display.

[11] User stories V3

b. Intended use: consider adopting the recommendations in DPP system implementations. Do note that these recommendations were made before the results of the EU standardization request for the DPP system by CEN-CENELEC JTC24[12] were published.

3. Key risks associated with the DPP system interactions and potential mitigations:
   a. Intent: the DPP system can be intentionally or unintentionally undermined by actors. The risks and mitigations chapter lists key risks. Potential mitigations for these actions are incorporated in the key architectural recommendations where possible. A more extensive description may be found in the companion document[13].
   b. Intended use: be informed about the potential ways in which actors may undermine a DPP system implementation.
4. Finally, the appendices consist of a list of requirements from the ESPR for the DPP system, and more detailed comparisons of options for some of the architectural recommendations.

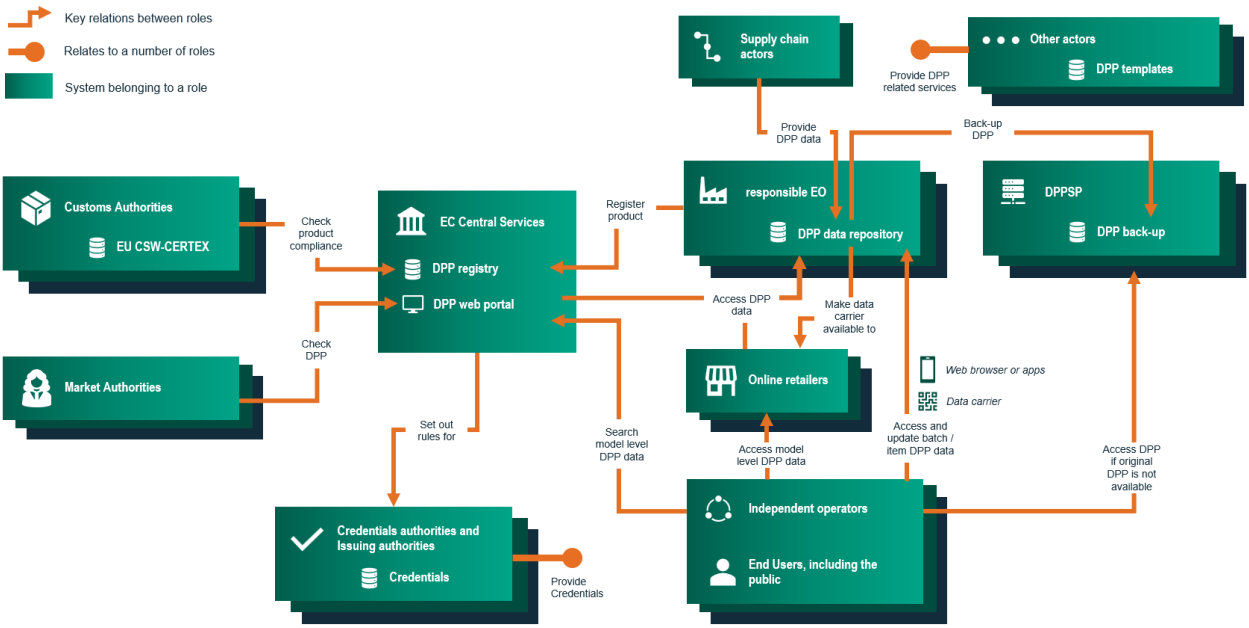


FIGURE 2: A ROLE-BASED VIEW OF THE DPP ECOSYSTEM

Figure 2 gives insight into the roles and their relations in the DPP ecosystem, elaborated on further in the following chapter. Each actor has to or may implement their own components (i.e. building blocks).

Topics not covered in this document are:

- The DPP data model, describing attributes of the data in the DPP, which will be defined in upcoming Delegated Acts. Support for this data model will be a separate result of the CIRPASS-2 project, as is an analysis of the requirements for the data model[14];

[12] CEN/CLC/JTC 24

[13] Risks and mitigations: a companion to D4.1 Reference Architecture

[14] Ontology requirements

- Detailed means for determining the web link based on the scan of a data carrier, as this will depend on the use case;
- Format and details of the data carrier;
- DPP Lifecycle API specifications, these will be defined in JTC24;
- The means for collecting data for DPPs, including the validation of the quality and validity of DPP data at the data source;

Changes with respect to CIRPASS proposal for the DPP system architecture

This document is an evolution of the DPP system architecture proposed in March 2024 by the CIRPASS project.[15]

HTTP vs DID architecture
The CIRPASS1 DPP System Architecture document proposed two parallel architectures, an HTTP-based architecture and a DID-based one. The current document recommends only the use of an HTTP-based architecture. Although the decentralized nature of DIDs is a clear strength, the accessibility and ease of use (as required by the ESPR, article 11(b)) of the DPP system which are provided by an HTTP-based system, both now and in the near future, led to this choice.
For more technically advanced use cases and economic operators the possibility of using DIDs in addition to the HTTP-architecture is possible. When applying DIDs as product IDs a specialized scanner can read and dereference the DID to retrieve the DPP data, either through HTTP-calls or directly from the DID-document. Using DIDs to identify an organization can be supported through the (recommended) use of Verifiable Credentials, for instance by having a trusted body issue a credential for a DID, providing proof of trust of relevant attributes for the organization without revealing additional information.

Identity management
In the CIRPASS1 DPP system architecture a clear distinction was made between credentials required for registering a DPP in the EU registry and accessing restricted data in a DPP hosted by an economic operator. This document recommends the use of a single identity credential, issued or backed by a trusted authority. This choice is made reduce complexity is the system, which would result from the need for multiple identities.

Resolvers
This document proposes that the EU Web Portal is used as the 'Default EU resolver', which was already part of the CIRPASS1 DPP System Architecture document. The 'rEO resolver', which was also proposed in the CIRPASS1 document has been split into smaller building blocks providing the different functions this resolver was expected to provide, the main building block addressing these functions is the redirection service. This decision was driven by the fact that the mandatory EU Web Portal is by its nature a very enduring part of the system, and by the desire to lower the complexity for Economic Operators.

Guiding principles

[15] CIRPASS DPP System Architecture

The guiding principles are a set of statements that shaped the design of the DPP reference architecture. These principles have been drawn from the ESPR (see Appendix A), from input by the pilot projects and experts, and from other (EU) initiatives for DPPs. These principles are not necessarily mandated by law, but are based on the spirit of the law.

- The DPP system should minimize administrative burden. This means that, in accordance with the 'once only' principle, DPP data should be exchanged in a manner that facilitates reuse by different public authorities and organizations.
- The DPP system architecture should be designed to be flexible to accommodate changing regulatory requirements.
- The DPP system should be based on and comply with applicable standards, such as the standards proposed by JTC24.
- The DPP system should allow for interoperability with international DPP standards, also outside the EU, as this is paramount for global success of DPP.
- The DPP system should be an open system which allows for freedom in design choices for DPP solutions, provides extensibility to allow for innovation, and at the same time recommends standards as necessary, e.g. for interoperability.
- DPP solutions should have the option of being as simple and low-cost as possible while also allowing flexibility for more advanced and complex non-mandatory functionality.
- The DPP system should be designed considering the perspective of all users of the system. Using the system must be convenient for every actor.
- The DPP system should support both human interactions and machine-to-machine interactions.
- The DPP system architecture should ensure appropriate security and trust.

Roles

This document uses the same definitions as used in the CIRPASS 2 User Stories V3. For reference, we reproduce these definitions below:

“An actor is a natural or legal person that 1) has to, or may, take on different roles in different DPP ecosystems, 2) has to, or may, take on multiple roles in each of these ecosystems, and 3) has to, or may, take on multiple roles during the lifecycle of a DPP.

There are many ways to conceptualize roles. In this document, a role is included based on two criteria: 1) the ESPR legislation refers to, or strongly implies the existence of, the role, and 2) a need that the DPP system should serve involves them.”

TABLE 1: DEFINITION OF ROLES

Icon	Role	Short description
	rEO	The responsible Economic Operator (rEO) refers to a legal person that is responsible for creating a DPP, and all legal obligations therewith
	End User	A natural or legal person in the EU to whom a product has been made available
	Independent Operator	Independent Operators are natural or legal persons that perform activities associated with the Circular Economy (i.e. R-Ladder activities)
	DPPSP	The DPP Service Provider (DPPSP) refers to a natural or legal person authorized by the rEO to provide DPP services, including keeping a DPP back-up
	Public Authority	Public Authorities refer to parties that are carrying out the duties assigned to them by law, such as customs authorities or market surveillance authorities
	Credentials Agency	A legal person that provides credentials to parties, which may be used to make and verify a variety of claims in the DPP
	Supply Chain Actor	A legal person that performs an activity in a product’s value chain up to where the product reaches the customer

2 BUILDING BLOCKS

The building blocks (or application services) are proposed technical services as part of the proposed DPP system architecture. The building blocks are based on a review of the User Stories V3 (see Table 2 below); they are software that enable or support the User Stories in their execution. The set of proposed building blocks is aimed to be sufficient to execute all user stories.

TABLE 2. USER STORIES V3.0 OVERVIEW

User story code	User story
1	As an rEO, I want to place my new product on the market and create its DPP, so that I can comply with the relevant delegated act
2	As an rEO, I want to link an existing DPP and data carrier to my new DPP, so that my product is linked to relevant other DPPs
3	As an End User, I want to retrieve DPP data via a data carrier physically on the product, so that I can make an informed decision
4	As an End User, I want to retrieve DPP data before online purchase, so that I can make an informed purchasing decision
5	As a Public Authority, I want to retrieve a collection of DPPs using the EU registry and Web Portal, so that I can monitor compliance
6	As an rEO, I want to ensure that my DPP back-ups, stored by the DPPSP, remain up to date, so that users will have access to up to date DPP data in case the original DPP is no longer available
7	As an Independent Operator without authorization by the rEO, I want to add to the item level DPP data, so that users can access detailed and updated product information
8	As an Independent Operator authorized by the rEO, I want to add data to the item level DPP data, so that users can access detailed and updated product information
9	As an Independent Operator, I want to indicate in the DPP that a product no longer exists, (e.g. after remanufacturing or recycling), so that others are informed of the state of the product.
10	As an rEO, I want to change my DPPSP, so that I can choose a vendor that provides my current needs

11	As a prospective rEO, I want to transfer all ESPR-related legal responsibilities for a product to my organization, so that I become the new rEO for this product.
12	As a DPPSP, I need to make available a back-up of the DPP that is no longer made available by the rEO, so that the DPP remains available
13	As an rEO, I want to stop making my DPP available when the expected lifetime of my product has passed, so that I no longer have to host the DPP

In order to provide context for each building block, they are grouped by role. The criteria for this grouping are that either a) this role must implement the functionality of the building block to comply with the ESPR, or b) there is a clear benefit if this role implements the building block. The grouping is meant to facilitate reading, it is not normative: different combinations of building blocks are expected to emerge over time.

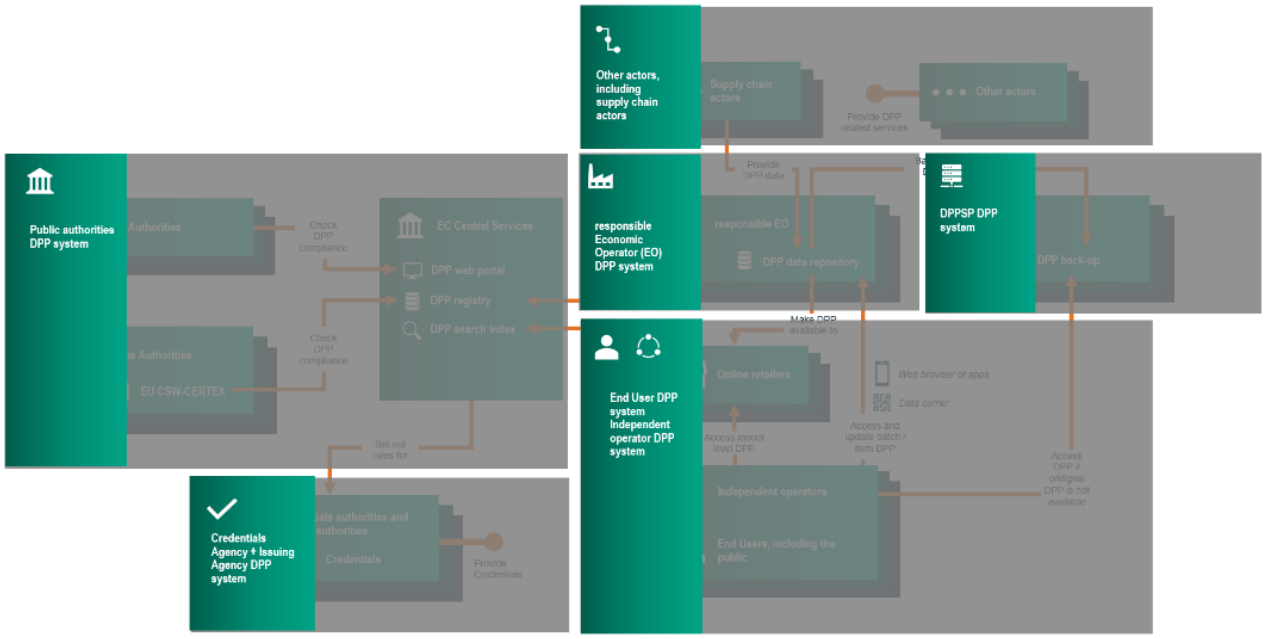


FIGURE 3: SIMPLIFIED ROLE-BASED VIEW - ROLES THAT PROVIDE SIMILAR BUILDING BLOCKS ARE GROUPED

For each of the roles, a figure is created that puts the building blocks in a context. Each figure is accompanied by a table that elaborates on the expected input, output, and recommendations for the implementation of each building block. The legend to the figures is provided in figure 4. Each building block is described only once, if it is applicable to multiple roles it is visually shown each time, but only textually described the first time it is encountered.

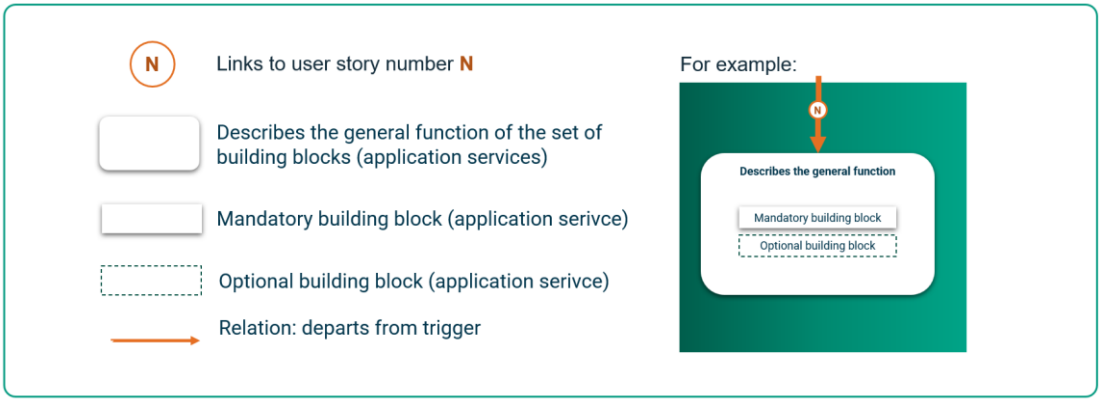


FIGURE 4: LEGEND TO ROLE-BASED BUILDING BLOCK FIGURE

RESPONSIBLE ECONOMIC OPERATOR

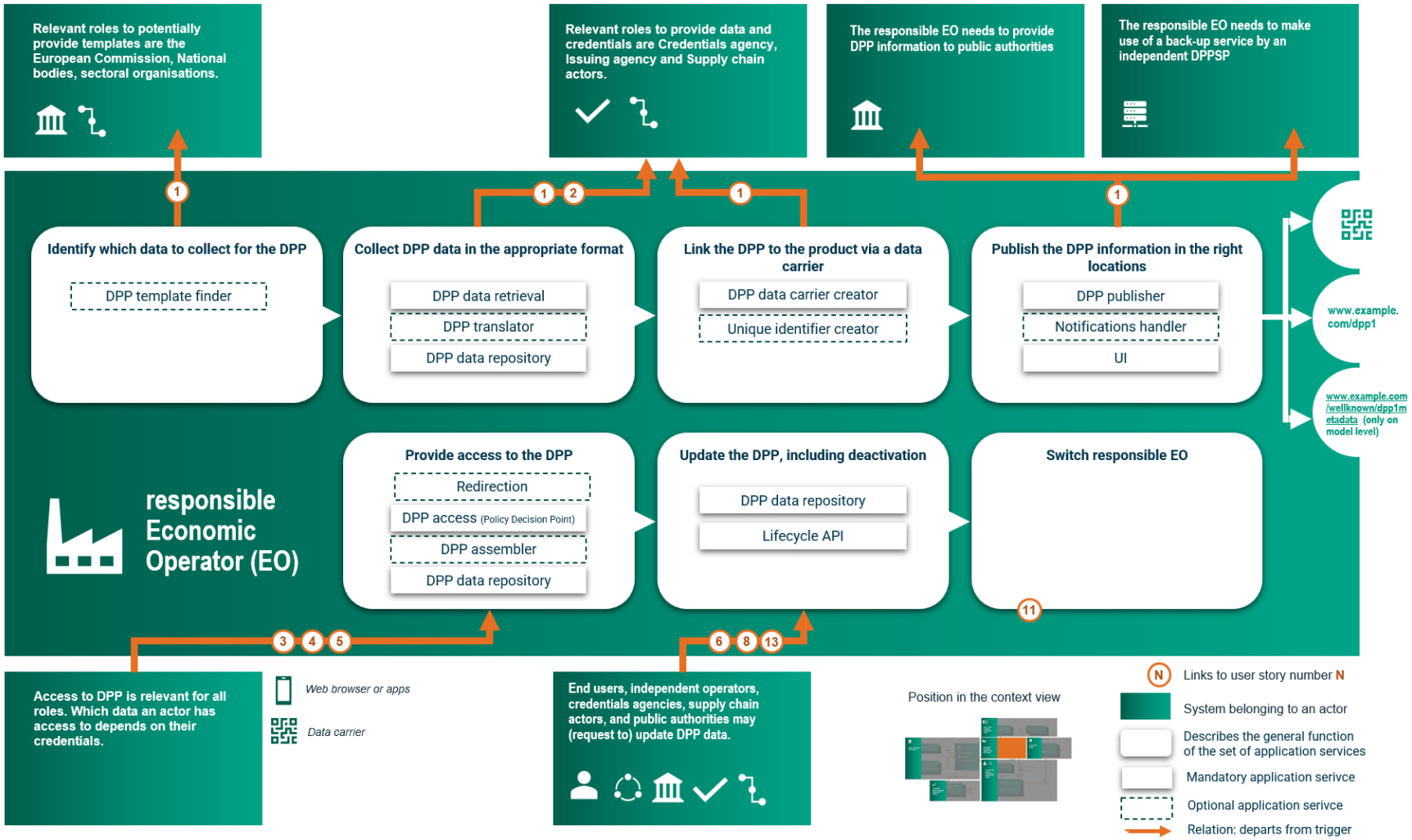


FIGURE 5: BUILDING BLOCKS FROM THE ECONOMIC OPERATOR'S PERSPECTIVE

DPP template finder (optional)	Identify relevant DPP data models – templates – for a certain type of product. Both mandatory and voluntary DPP data may be included.	• Product Type • Information regarding the use case	• A template relevant for this product • Metadata about the available templates	Templates can be provided by many different organizations. Public authorities may provide templates with the minimal legal requirements, sectoral authorities can extend these with sectoral agreements and (large) companies may extend these even further by adding their own preferred attributes. The DPP template finder makes these templates findable and searchable. This requires aggregation of information from many different organizations, which may be supported by: • A standardized way of describing (catalogues of) datasets, such as DCAT, the IEC 63278-Series etc.; • An aggregation and searchability layer over the set of standardized datasets. A template might take the format of JSON schemas (or other standardized formats), enriched with SHACL constraints allowing to perform schema and semantic validation over a DPP JSON-LD document. Relevant architectural recommendations: • Standardize the default exchange format as JSON-LD • Make use of modular DPP templates
DPP data retrieval (optional)	Collect data relevant for filling a DPP, including relevant data from supply chain actors.	• Connection details to a data source • Credentials to get access to the data source.	• The set of data, coming from the input source, providing information to create a DPP	Data may be retrieved from various actors in many ways and using several protocols, including HTTP, FTP, cloud-based file transfer protocols, smart contracts, gRPC, etc. to the building block retrieves data regardless the protocol used for the data provider to share them. Producing a DPP out of the retrieved data is done by the DPP translator service.. If the data is made available in a non-machine-readable manner, such as plaintext e-mails, PDF documents, etc., a data retriever to (manually) convert the data to a machine-readable format may be used. Agreements in the supply chain about the collection and sharing of information (e.g. using email, a DPP platform, a data space, …) is recommended to minimize effort. Further requirements may be set (partly) by the Supply Chain Act.

				Relevant architectural recommendations: • Standardize the default exchange format as JSON-LD
DPP translator (optional)	Convert DPP data across model and granularity levels using mapping capabilities and format conversion.[16]	• DPP data • Information regarding the target model (e.g. Data model xyz, Data model abc) • Information regarding the target format (e.g. JSON-LD, CSV, AAS) • Information regarding the target language (e.g. English, French, German)	• DPP data converted to the desired model • DPP data converted at the desired granularity level • DPP data with content localized with the desired language • DPP data in the specified format	This service might be needed when a DPP is accessed at read time in a custom format, or when input data is received from supply chain actors for the initial creation of the DPP. The preferred operation for this building block is to define mapping rules to the component and have an engine that automatically maps the incoming data to the target model according to the associated submitted rules. The target language may, for instance, be provided in the Accept-Languages header. The content can be localized on the server side via configuration files or settings with key value pairs where the value is the localized content and the key is a property name with a language code, so that content can be resolved at runtime. Relevant architectural recommendations: • Standardize the default exchange format as JSON-LD • Make use of modular DPP templates
DPP data repository	Store the actual DPP data. The DPP data repository is an abstraction referring to the point in the system where product data associated with an UPI is stored. This system should have interfaces to store new DPP data associated with a UPI, and must have interfaces to retrieve DPP data associated with a given UPI.	in the case of retrieval: • A given UPI to retrieve associated DPP data, metadata, and event data in the case of storage: • DPP data, metadata, and event data associated with a UPI	in the case of retrieval: • Data, metadata and event data associated with the given UPI in the case of storage: • *N/A*	Given its abstract nature the data repository might be represented by several technologies (e.g. a RDBMS, or a NoSQL, or an ERP or a Triple Store and so on). The most straightforward approach is probably to have the persistence layer made accessible through a REST API that accepts for write operation and provides for read operations DPP data already formatted according to the DPP model and as a JSON-LD. In case adapting the custom data models of an existing system to the DPP model and to the JSON-LD format is not a feasible solution, DPP translation is needed to map the custom models to the DPP one. For write operations (e.g. when creating a DPP) this conversion can

[16] The deliverables from CIRPASS-2 concerned with ontologies and semantic interoperability are expected to provide guidance on this building block, the 'advanced DPP toolset' to developed may provide technical support for this building block

				be performed with the DPP translation component as well. For read operation this might happen at the level of the DPP assembler component. Given the decentralized nature of the DPP platform, it may not be represented by a single IT system but by multiple ones. Given the probable need to allow only logical update or delete operations over DPP data (see also Lifecycle API block below), the repository can be conceived as an event store, and it may be worth implementing it following the event source design pattern. Relevant architectural recommendations: • Align back-up provider functionality with primary storage • Secure DPP entries with digital signatures/seals • Ensure immutability of DPP records as the responsible EO • Provide and record update receipts • Establish an EU repository with key DPP data for search • Adopt the standard lifecycle API proposed by JTC24
Unique identifier creator	Generate a unique identifier that links the physical product and the digital representation. A product identifier must be unique, specific to a product and harmonizable throughout the entire EU, Identifiers that need to be created include the Unique Product Identifier, the Unique Facility Identifier, the Unique Operator Identifier.	• N/A	• A unique identifier	Product identifiers to consider: • GTIN, which can be expressed as a structured path URI conformant to ISO/IEC 18975 • Pure dereferenceable URIs according to RFC3986 • Decentralized Identifiers (DIDs): As per the W3C DID Core Specification for self-sovereign identity. • UUID: Universally unique ID according to IETF standard 9562 • IEC 61406 Series: Identification Link.. Specifies minimum requirements for a globally unique identification of physical objects which also constitutes a link to its related digital information. Operator identifiers to consider: • ISO/IEC 15459:2015: Specifies a unique identification system for supply chain management. • GS1 Global Location Number (GLN): Used for identifying legal entities and locations.

				• IEC 61406 Series: Standards for industrial data and communication. • Decentralized Identifiers (DIDs): As per the W3C DID Core Specification for self-sovereign identity. • LEI, ISO 17442 Facility identifiers to consider: • GLN • ISO/IEC 15459:2015: For unique identification in the supply chain. • GS1 Global Location Number (GLN): For identifying facilities. • IEC 61406 Series: For unique identification of physical objects which also constitutes a link to its related digital information. • LEI, ISO 17442 • Decentralized Identifiers (DIDs): For facility identification. Relevant architectural recommendations: • Every product that needs updates requires an item-level UPI • To ensure compliance with the requirements of the ESPR, it is recommended to use operators that comply with JTC24 standards on identifier issuance.
DPP data carrier creator	Create a data carrier that holds the unique product identifier, or a weblink. This carrier can be used to access the DPP.	• A unique product identifier or weblink which will provide access to the DPP. • The format of the carrier (QR code, bar code, RFID etc.).	• A data carries that encodes the input.	Preferably a data carrier that can be read with consumer smartphones, although other data carriers may be better suited for specific B2B scenarios. Standards: ISO/IEC 18975, ISO/IEC 15459:2015 IEC 61406 Series: For unique identification of physical objects which also constitutes a link to its related digital information. Vulnerable consumers (users that are blind, physically disabled, or have dyslexia) might have trouble scanning the data carrier. For example, for blind people, an indicator of the location of the carrier in braille can help. Or the possibility to scan data carriers from several meters distance with mobile devices. The standard EN 301 549 “Accessibility requirements for ICT products and services” can be consulted Relevant architectural recommendations: • Establish a universal DPP symbol to place on the product

				• Create a data carrier for online, and pre-purchase use
DPP publisher	Make the DPP data, including updates to the DPP data, available for interested parties by providing a dedicated endpoint for retrieving a DPP. Publish an index that provides a link to every DPP that is made available through the publisher. Allow parties to update the DPP via an endpoint.	• UPI (for DPP registration) • Additional parameters to customize the generated URL (optional, for DPP registration) • Parameters to instruct the index creation. • A link to a DPP update (for a DPP update)	• An accessible URL that provides access to a specific DPP.	The DPP publisher is not the point where DPP's are stored, it is only making the DPP available for end users outside of the organization. For discoverability of DPPs it is strongly recommended that every Responsible Economic Operator hosts metadata specifying the location of available data at the level of the product *model* under the /.well-known/dpp/…. See IETF RFC 8615 'Well-Known Uniform Resource Identifiers'. Relevant architectural recommendations: • Provide a discoverable model level data endpoint • Adopt the standard lifecycle API proposed by JTC24 • Develop standardized DPP display templates and guidelines
Notifications handler (optional)	Dispatch notification related to DPP events to interested parties. For example: • Notify economic operator of a new DPP that replaces their old DPP • Notify economic operator that a product has been modified, updated, recycled. • Notify DPPSP that he needs to start providing the back-up as the 'active' DPP (i.e.in the case of insolvency of the economic operator).	• DPP data repository locations, other locations to keep track of for updates (in case of pull scenario) • Connection information about where dispatch events • Event Types to dispatch	• Notification to appropriate actor/consumer with relevant associated event data	Notifications can be generated as push notification to market authorities or custom authorities and implemented in a decentralized system. These can be of several types: in-app messages, push notifications, email notifications. *Notifications can be dispatched with several mechanism, for instance:* • Using message brokers to which allowed party can connect and receive streams of message. • By allowing the configuration of web hooks as a set of listeners represented by URL to invoke on event. The service should allow configuring which kind of event to dispatch and to whom. The service should take into account the risk of large volumes of notifications being sent, possibly to a single recipient, if bulk updates of DPPs are possible. Events might be intercepted by the notification handler for being dispatched in one of the following ways: • handlers pull it actively performs requests towards the repository checking for updates to DPP. • repository push: events get pushed to it from the repository Relevant architectural recommendations: • Align with existing APIs for value-added services

UI	Provide a user interface to allow the end-user to view DPPs.	• DPP data	• A visual representation of DPP data	Relevant architectural recommendations : • Create a universal symbol set for key DPP data • Develop standardized DPP display templates and guidelines
Redirection	Route a product's URI to one of a set of appropriate resources or additional services, such as the product's DPP itself. In addition, facilitate the post-hoc mutation of the set of appropriate resources and additional services that are accessible or routable from a product's URI.	• A product's URI	• Resolved URI or URIs pointing to further resources or specific services	The redirection service could work as a simple proxy that transparently forward request and response between the data requestor and their actual location or it can make use of traditional redirect semantics using appropriate HTTP redirection mechanism (HTTP 300 codes and Location HTTP Headers) where the actual URL is provided. The decision to what resource or service to redirect to should be automated based on user-provided or contextual information. This service might return a list of available locations for the data that the user, given the appropriate access rights, could select from. Relevant architectural recommendations: • Ensure UPI-to-URI redirection as the responsible EO • Establish a fallback EU UPI-to-URI redirection service
DPP access (Policy Decision Point)	Evaluate a DPP request against authorization policies, thereby granting or revoking access – depending on the credentials provided with the request – to specific DPP data or to update/append data related to a DPP.	• Subject, credentials • Object, DPP resource to access • Operation: create, read, modify, append	• A Permit or Deny decision for the given subject–operation–object triplet	The relevant delegated act defines who has rights to access which data. The roles definition will be based on EU defined base roles, that can be extended to allow a more fine-grained control by the rEO on data access rights. The policy decision point will use role-based access control (RBAC), based on a set of EU-defined generic roles that can be extended. The subject comprises Selective Disclosure JSON Web Tokens (SD-JWTs) or plain JWTs whose claims can be used to retrieve roles and/or other user properties to authorize access and information as needed. Relevant architectural recommendations: • Utilize an eIDAS 2.0-compliant wallet to store credentials • Utilize eIDAS 2.0 Verifiable Credentials for identity • Utilize eIDAS 2.0 Verifiable Credentials for role management • Ensure credentials are issued by trusted bodies

				• Utilize trusted third parties for anchoring trust
DPP assembler	Assemble a DPP when access is requested. This can consist of retrieving a complete DPP, which has been created earlier, from storage or assembling a DPP from data stored across several repositories belonging to the rEO and even belonging to independent operators. This means that the assembler might need to pull the data required from several sources to assemble the DPP. The service will provide data according to the requested format, if provided, or as an HTML page otherwise. • If credentials are provided in the request, restricted data may be provided in the output. By default, the output contains only public data.	• A unique product ID; • (Optionally) a specific format for the DPP; • (Optionally) a specific subset of the data in the DPP • (Optionally) credentials allowing access to restricted data. • (Optionally) The date of the (historical) DPP to retrieve	• DPP data formatted according to the required format if provided, or as an HTML document otherwise	Implementation wise, a choice must be made between having the assembler retrieve a pre-assembled DPP, pull the data from multiple sources every time DPP access is requested, or pull data from a single storage location where a copy of all the data is maintained. Using multiple sources implies higher latency and the need for a strategy to deal with (temporary) unavailability of data sources. Using a single source with copied data implies data duplication and thus additional storage, as well as a strategy to keep the duplicated data up to date with source data. A compromise is to have mandatory/publicly data available in a single storage under the control of the rEO, while keeping downstream value chain data in the Independent Operator repositories. This allows access to a single data point when the default HTML DPP representation is requested, ensuring that mandatory data doesn't depend on availability of multiple resource endpoints. This would probably avoid the need for data synchronization as the single repository would host DPP data related to the upstream value chain providing certainty that this data will not be modified once the product is put into service. On the other hand, the downstream value chain data will be retrieved every time by the decentralized repository and assembled on the fly, providing up-to-date data but introducing the risk of data being modified or becoming unavailable. Assembling a DPP with data from various sources implies that the assembler requires data mapping capabilities to align to the DPP model and the data from the various sources (the DPP data translator building block). The full DPP must be returned, without any links which must be resolved by the retrieving party, unless these are links to DPPs for components of the product. Relevant architectural recommendations: • Link to Product Component DPPs • Develop standardized DPP display templates and guidelines
Lifecycle API	Provide a set of APIs to manage the lifecycle of a DPP allowing to: • Create a DPP • Update a DPP	• Create operations: ○ Payload representing DPP data • Read operations: ○ UPI ○ Alternative search	• Create operations: ○ Appropriate Http Status code (e.g. 201) ○ Generated UPI (optional if the API generates it automatically)	The specifications of the API are not in scope of this document. The expectation is that JTC24 will define the appropriate lifecycle API specifications. Reasonably the Rest API will provide resources endpoints to perform CRUD operations over DPP data following the standards

	• Access a DPP • Delete a DPP • Ensure DPP portability (backup, transfer) Since it is recommended that DPP data is immutable, ‘update’ operations should not modify data but only append it, without replacing the original data. The same applies to delete operations, that mustn't delete original information but flag it as “deleted”. The API should provide a mechanism for an Independent Operator to forward data updates to the rEO and to give to the latter a mechanism to safely provide access to read and write operation performed from an Independent Operator,(e.g.,. implementing data authenticity checks).	params to retrieve DPP data • Update Operations ○ UPI ○ Payload or a link to the data representing the update ○ A timestamp ○ Additional information to allow data authenticity checks (e.g., a hash of the data payload in a signed JWT) • Delete Operations ○ UPI ○ A timestamp • Portability ○ DPP data ○ Information regarding the target data sink	• Read Operations: ○ The DPP data (possibly encoded as a JSON-LD) • Update Operations: ○ Appropriate HTTP Status code (e.g. 200,202...) and response message to communicate the operation result. • Delete Operations: ○ Appropriate HTTP Status code (e.g. 204, 200...) • Portability: ○ An appropriate HTTP Status code or an operation result message. ○ A link to the backup (for backups operation)	http verbs (POST, PUT, PATCH, DELETE, GET). Write operations are those consisting of data updates or logical (or physical) deletion of a DPP (e.g., when recycling occurs). It is recommended that endpoints for ‘write’ operations accept parameters to perform an authenticity check for the updated data. To support interoperability, it is also recommended that the encoding format for request and response payload is JSON-LD. Relevant architectural recommendations: • Assign storage of DPP updates to the responsible EO • Secure DPP entries with digital signatures/seals • Ensure immutability of DPP records as the responsible EO • Provide and record update receipts • Adopt the standard lifecycle API proposed by JTC24

PUBLIC AUTHORITIES

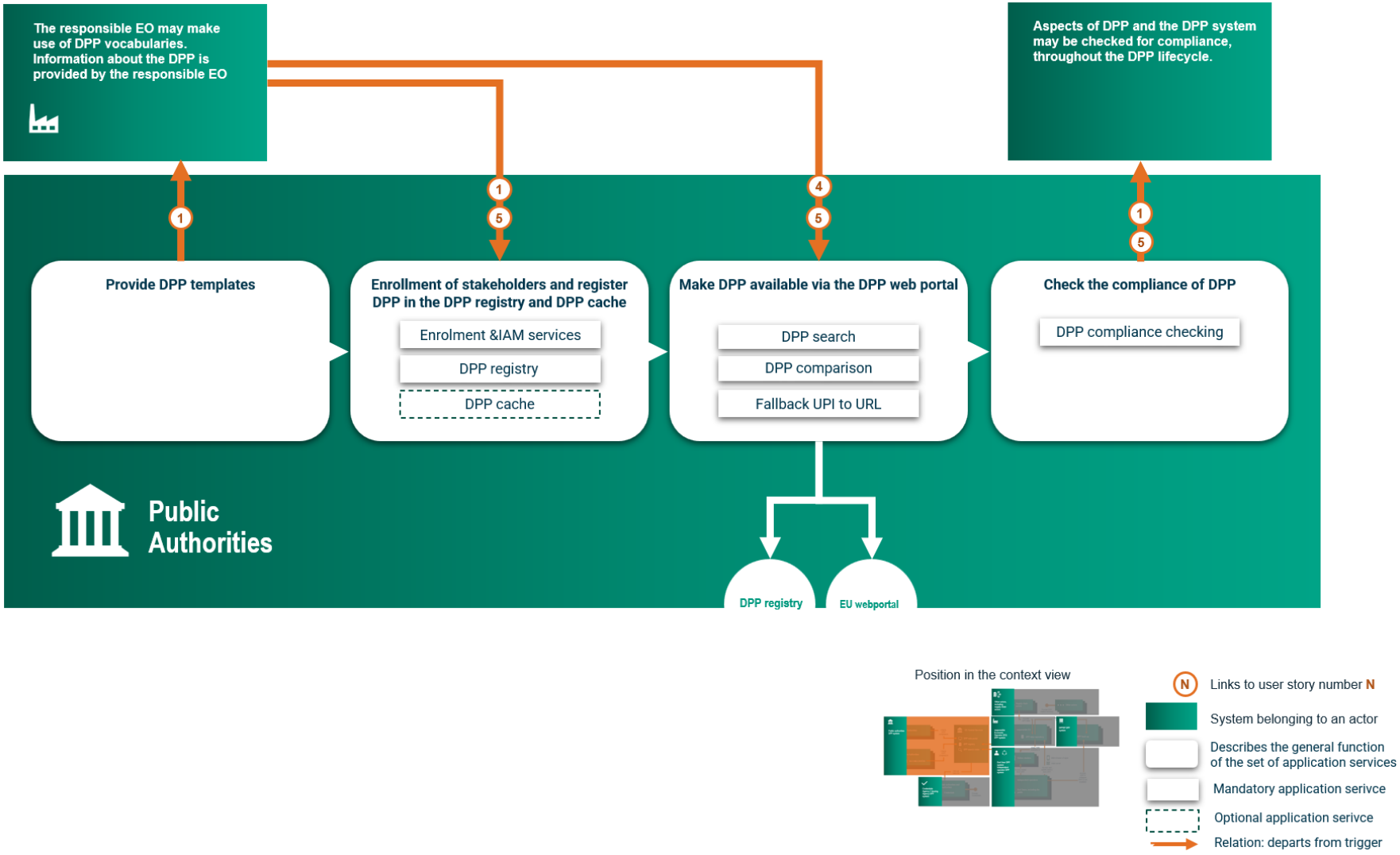


FIGURE 6: BUILDING BLOCKS FROM THE PUBLIC AUTHORITIES' PERSPECTIVE

Building block name OPTIONAL = NOT STRICTLY MANDATORY BUT HELPFUL TO SUPPORT INTERACTIONS WITH THE DPP SYSTEM AS DEFINED IN THE USER STORIES V3	Description WHAT IS THIS SERVICE SUPPOSED TO DO?	Input WHAT DOES THE SERVICE TAKE AS AN INPUT TO PERFORM ITS FUNCTION?	Output WHAT IS THE RESULTING OUTPUT OF THIS SERVICE?	Considerations RECOMMENDATIONS FOR APPLICATION SERVICES, INCLUDING WHAT IS NEEDED FOR INTEROPERABILITY
(EU) DPP registry	Register all DPPs issued in the common market and store a minimal set of information as the Product ID, rEO id, Facility ID, location of DPP and the current lifecycle state.	• Responsible Economic Operator ID • Facility ID; • Product ID; • DPP location. • Product Life Cycle State (end-of-life marking in case the product ID is at item level)	• Confirmation of successful registration or failure • Unique registration identifier.	This service will be provided by the EC and may be used by public authorities. The registry should verify the operator identifiers before accepting DPP in the registry (A6, A7) Next to registering in the EU DPP registry. If the EC decides to implement the “fallback EU UPI-to-URI redirection service”, the product ID and DPP location should also be registered there. Similarly, if the EC decides to require specific key DPP data for search EU web portal, this data should be registered with the EC as well. Consider combining these into a single service for simplicity. Relevant architectural recommendations: • Establish a DPP reporting system to report incorrect DPPs • Establish a fallback EU UPI-to-URI redirection service • Establish an EU repository with key DPP data for search
DPP Compliance checking	Check a set of DPP data for compliance with appropriate rules, regulations, and agreements. This could include, for instance, checking whether the relevant DPP data has been disclosed as required by the law or could also include checking the product itself for compliance with conformity requirements.	• DPP data belonging to one or multiple DPP in JSON-LD format • (Optionally) the identification of the template the DPP is based on. • A SHACL template (or a reference to a template) to evaluate against the DPP data and validate it	• The result of the validation. • If validation fails, information that allows the user to understand the reason for the failure (e.g. List of not valid fields and the reason why each field is not valid)	Validation should occur on data at the level of granularity that the requester is granted access to. Depending on the corresponding DPP delegated act, the validation might comprise: • Structure validation • Data type validation (e.g. number, string, boolean) • Constraint validation (e.g. Nullability of fields, date and date time formats...) • Relations between fields (e.g. If field ‘a’ has value = ‘something’ then field ‘b’ must be equal to ‘some other value’), The implementation of this service could be a SHACL template applier. It might need to support retrieval of the template or DPP data if they are provided as HTTP URLs. Another option, although probably less flexible, could be to have the compliance check tool to directly store the relevant SHACL

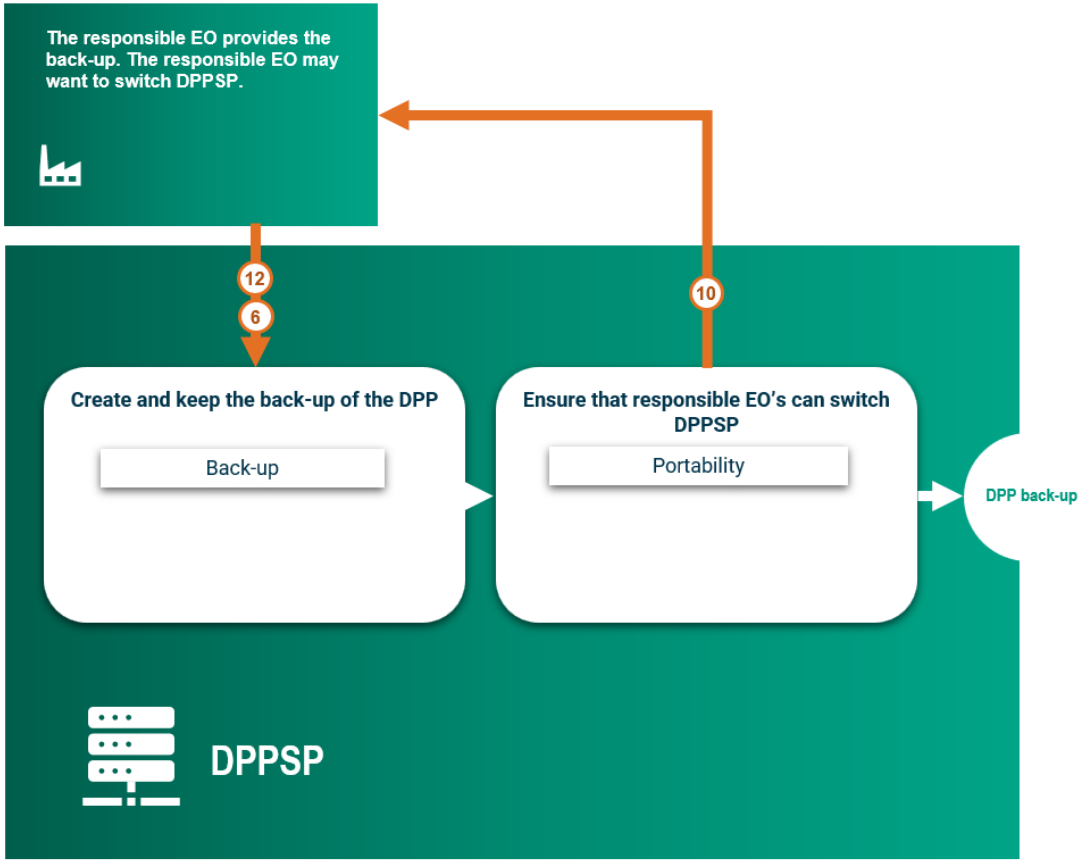
				template to validate DPP data. In this case the service should provide ways to add, update and remove templates. Relevant architectural recommendations : • Make use of modular DPP templates
DPP Search	Search DPP data according to input search criteria to retrieve (i) model level DPP data or a complete DPP	• Search criteria Example search criteria for model level information: • Brand name • Model name • Registration number Example search criteria for full DPP: • Product type • Performance class • Economic operator name • Economic operator identifier • Unique location identifier	• Model level DPP data • Full DPP data	DPP search functionality is central to the Web Portal as it has been conceived by ESPR, The implementation complexity of the service depends on the type of search criteria allowed to perform a search operation. If search criteria comprise fields that are stored centrally in the EU registry (e.g. rEO identifier, Location identifier) the implementation is trivial. But if search keys might comprise fields' names that are stored in the decentralized repository a strategy to handle efficiently DPP searches needs to be evaluated. Below a list of the proposed implementation options[17]: • Create a centralized search index for all the mandatory model level data • Create a centralized search index including all mandatory search keys (corresponding to desired search criteria). The index creation and update implies either a manual upload of DPP data by the rEO or an EC service that automatically and periodically scans the DPP repositories to retrieve index information from the decentralized repository. Relevant architectural recommendations: • Establish an EU repository with key DPP data for search • Provide a discoverable model level data endpoint • Adopt the standard lifecycle API proposed by JTC24 • Align with existing APIs for value-added services
Fallback Product UPI to URL	Provide the location as the correct weblink for a UPI. .	• Unique Product Identifier (a unique product	• A single weblink	This service is meant for automatically determining the location of a DPP. For manual searching based on a Product

[17] Based on the document 'Options for EU web portal search'

		identifier can be a weblink)		ID the EU web portal is available. This service should be provided by the EC or by parties to which this responsibility has been delegated. • Where the UPI is provided as a simple identifier, ideally following the procedures set out in ISO/IEC 15459 that guarantees uniqueness within Automatic Identification and Data Capture systems, then there are no additional standards that need to be applied directly. • A service accepting UPIs weblinks must follow a standard, which allows for discovering the UPI by parsing the URI (ISO/IEC 18975 or IEC 61406), to handle cases where a UPI weblink no longer functions. • Note that, in contrast to the structured path approach defined in ISO/IEC 18975, IEC 61406 explicitly does not support parsing to extract identifiers offline as part of the standard, but it is usually possible anyway. Examples : Given a UPI of “ABC1234”, the service could return any URL with that as a query such as https://upi-uri-service.example?upi=ABC1234 • Given a GS1 Digital Link URI (conformant to the structured path approach defined in ISO/IEC 19875) https://example.com/01/09506000164908/21/1234, the UPI is readily found:: o GTIN (01) 09506000164908 o Serial number (21): 1234 o In this case, a new URI can be created by simply replacing ‘example.com’ (which is not part of the UPI) with the internet address of the backup UPI to URI service. Relevant architectural recommendations: • Establish a fallback EU UPI-to-URI redirection service
DPP comparison	Compare data between at least two (possibly multiple) DPPs on relevant criteria. This might be useful for a consumer before product purchase.	• A set of DPP data belonging to multiple DPP • Comparison options (e.g. preferred ranking,	• A visual comparison of DPP data, possibly customized, interpretable for the user.	Relevant architectural recommendations: • Align with existing APIs for value-added services

	Product comparison will be enabled by the EC Web Portal.	relevant fields to compare the DPPs...)		
Enrolment & IAM services	Assign an identifier, an identity and roles to an EO. This step is necessary for two processes: - To enable credential issuance as they will be based on identity and role information generated a registration time - To ensure that an Economic operator has a valid identifier needed at DPP registration time	• EO personal and company information (e.g.. Company, country, email) • The role that the EO plays or wants to play in the DPP system.	• A message or a consistent HTTP Status communicating the operation outcome. • The identifier and/or roles assigned to the operator.	This service should be implemented by the EC. It can be implemented as a classic web app that allows to perform Create, Read, Update, Delete operations over EO data persisted in a storage. The service should be equipped with a WebUI and expose a (REST) API to allow programmatic access to some of the exposed resources. Relevant architectural recommendations: • Utilize an eIDAS 2.0-compliant wallet to store credentials • Utilize eIDAS 2.0 Verifiable Credentials for identity • Utilize eIDAS 2.0 Verifiable Credentials for role management • Ensure credentials are issued by trusted bodies
DPP cache (optional)	A DPP cache is an optional component meant mainly to facilitate DPP searches by centralizing (model level) DPP data.	• DPP data to be cached	• DPP data saved to the cache	Caching data which will be accessed often enhances the stability and performance of a system. Both EO's and authorities which have a need to access large amounts of DPPs or very frequently access specific DPPs can facilitate this by caching data. As a cache that centralizes access to data that would be otherwise decentralized, a mechanism to keep cached data in synch with the original data needs to be put in place. This can be achieved either by auto-scanning the decentralized repository periodically and updating cached data or by requesting the rEO to send update information to the cache. A hybrid approach might allow the cache to be notified of an update event, that will cause the automatic pulling of the updated data from the decentralized repository, based on the event information., Given that this component should not simply be a centralized repository for a subset of the decentralized DPP data, it should apply some kind of retention policy of the data, probably based on the life cycle of the product. Relevant architectural recommendations: • Implement caching for high volume/frequency access • Ensure immutability of DPP records as the responsible EO

DPPSP



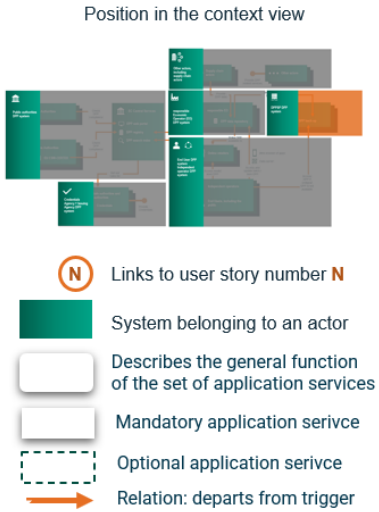
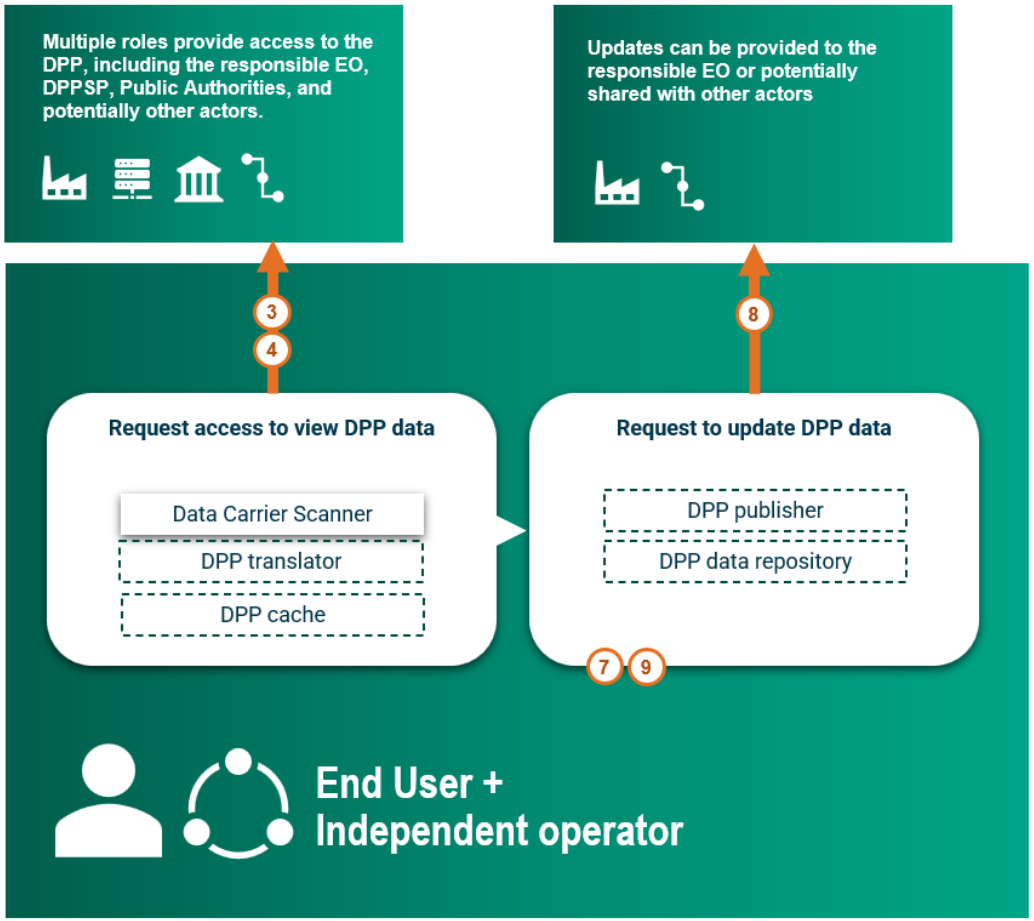


FIGURE 7: BUILDING BLOCKS FROM THE DPP SERVICE PROVIDER'S PERSPECTIVE

Building block name OPTIONAL = NOT STRICTLY MANDATORY BUT HELPFUL TO SUPPORT INTERACTIONS WITH THE DPP SYSTEM AS DEFINED IN THE USER STORIES V3	Description WHAT IS THIS SERVICE SUPPOSED TO DO?	Input WHAT DOES THE SERVICE TAKE AS AN INPUT TO PERFORM ITS FUNCTION?	Output WHAT IS THE RESULTING OUTPUT OF THIS SERVICE?	Considerations RECOMMENDATIONS FOR APPLICATION SERVICES, INCLUDING WHAT IS NEEDED FOR INTEROPERABILITY
Back-up	Store, and accept updates to, DPP data independently from the responsible economic operator.	• All mandatory DPP data; • Any access restrictions on the DPP data; • (Optional) Additional DPP data to be stored (based on the capabilities of the service provider and agreements between economic operator and service provider). • Updates to DPP data	• Confirmation of successful storage or failure • The location of the backup. • The DPP data	This building block refers to the mere storage and access of backup data. Data transfer, in this document, is foreseen to be provided by the DPP portability service (see below). Relevant architectural recommendations: • Standardize the default exchange format as JSON-LD • Align back-up provider functionality with primary storage • Adopt the standard lifecycle API proposed by JTC24
DPP portability	Transfer DPP data entirely or partially, including back-up data and potential links to updates, between entities, and remove it from its original location as far as possible. This service is primarily meant for: • DPP data transfer for backup. • Change of DPP service provider.	• Mandatory DPP data. • Any access restrictions on the DPP data. • (Optional) Additional DPP data to be stored (based on the capabilities of the service provider and agreements between rEO and service provider).	• Confirmation of successful transfer; • The location of the DPP data.	This service must ensure that Product identifiers and information are transferable from one software system to another, having interoperability between systems. The service can be conceived as a tool to provide automatic data transfer between systems, upon request. Relevant architectural recommendations: • Standardize the default exchange format as JSON-LD • Align back-up functionality provider with primary storage • Assign storage of DPP updates to the responsible EO • Ensure immutability of DPP records as the responsible EO • Ensure UPI-to-URI redirection as the responsible EO • Adopt the standard lifecycle API proposed by JTC24

END USER AND INDEPENDENT OPERATOR



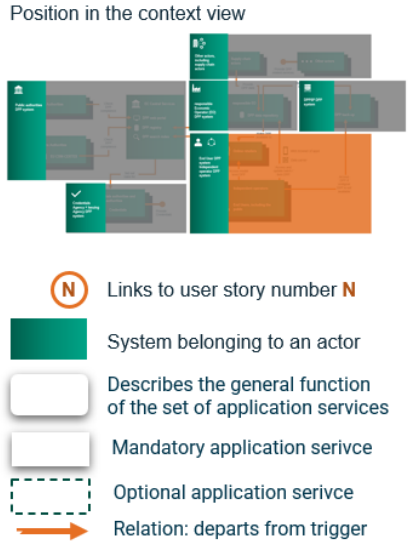
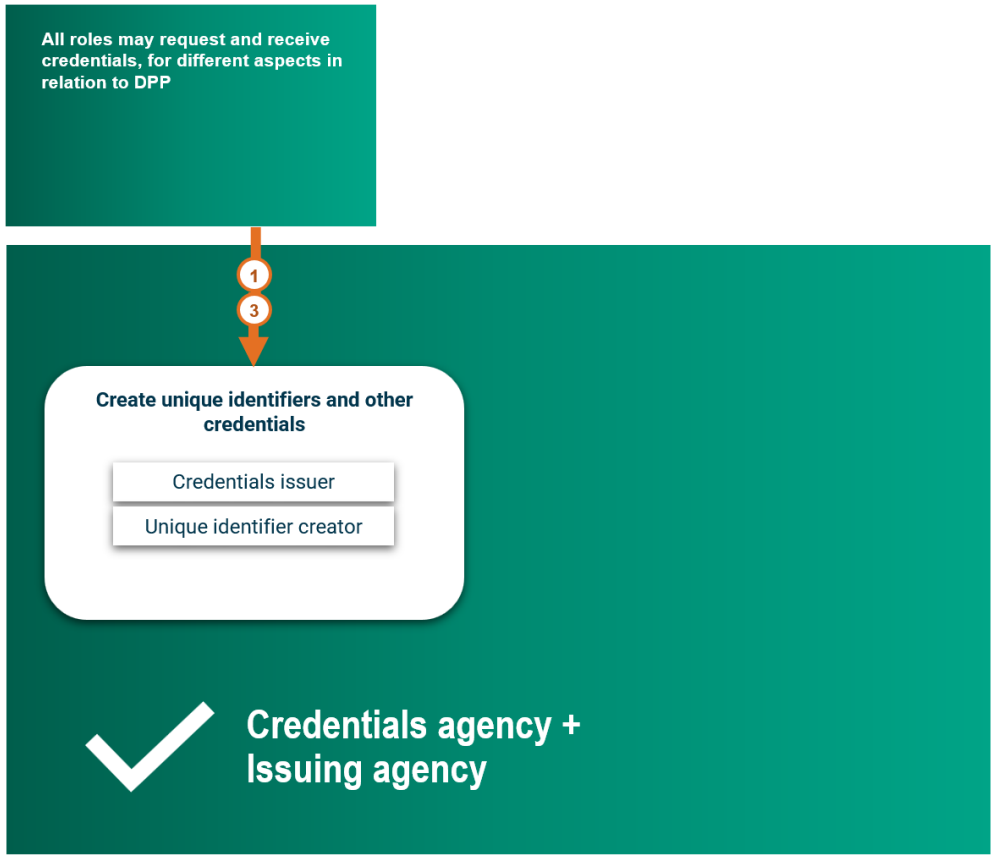


FIGURE 8: BUILDING BLOCKS FROM THE END USER AND INDEPENDENT OPERATOR'S PERSPECTIVE

Building block name OPTIONAL = NOT STRICTLY MANDATORY BUT HELPFUL TO SUPPORT INTERACTIONS WITH THE DPP SYSTEM AS DEFINED IN THE USER STORIES V3	Description WHAT IS THIS SERVICE SUPPOSED TO DO?	Input WHAT DOES THE SERVICE TAKE AS AN INPUT TO PERFORM ITS FUNCTION?	Output WHAT IS THE RESULTING OUTPUT OF THIS SERVICE?	Considerations RECOMMENDATIONS FOR APPLICATION SERVICES, INCLUDING WHAT IS NEEDED FOR INTEROPERABILITY
Data carrier scanner	Read the data contained in the data carrier on a product. Process it either by reading the unique product identifier, or by constructing or following a link to an online location from which the product's DPP is accessible.	• A product's data carrier that at least encodes the product's UPI and/or a weblink through which access to a DPP can be achieved	• The decoded and resolved UPI and/or weblink, and any additional data contained in the data carrier	A typical mobile phone's native camera should be sufficient to locate a DPP, if a QR Code contains a URL that is automatically resolvable to the DPP itself. If the url needs to be construct based on the information available on the data carrier or other kind of operation is needed before invoking a URL, then a DPP aware application, or an ad hoc device, is needed. Implementation wise, if we limit to consider QR Code and Data Matrix Code, there are much software libraries that allow to quickly integrate scanning capabilities in a Smartphone app or even in Web UI. Relevant architectural recommendations: • Create a data carrier for online and pre-purchase use

CREDENTIALS AGENCY AND ISSUING AGENCY



Position in the context view

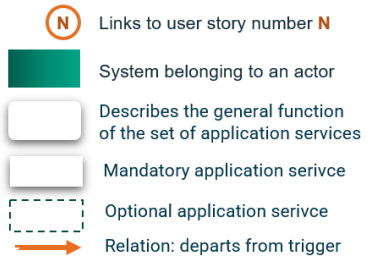
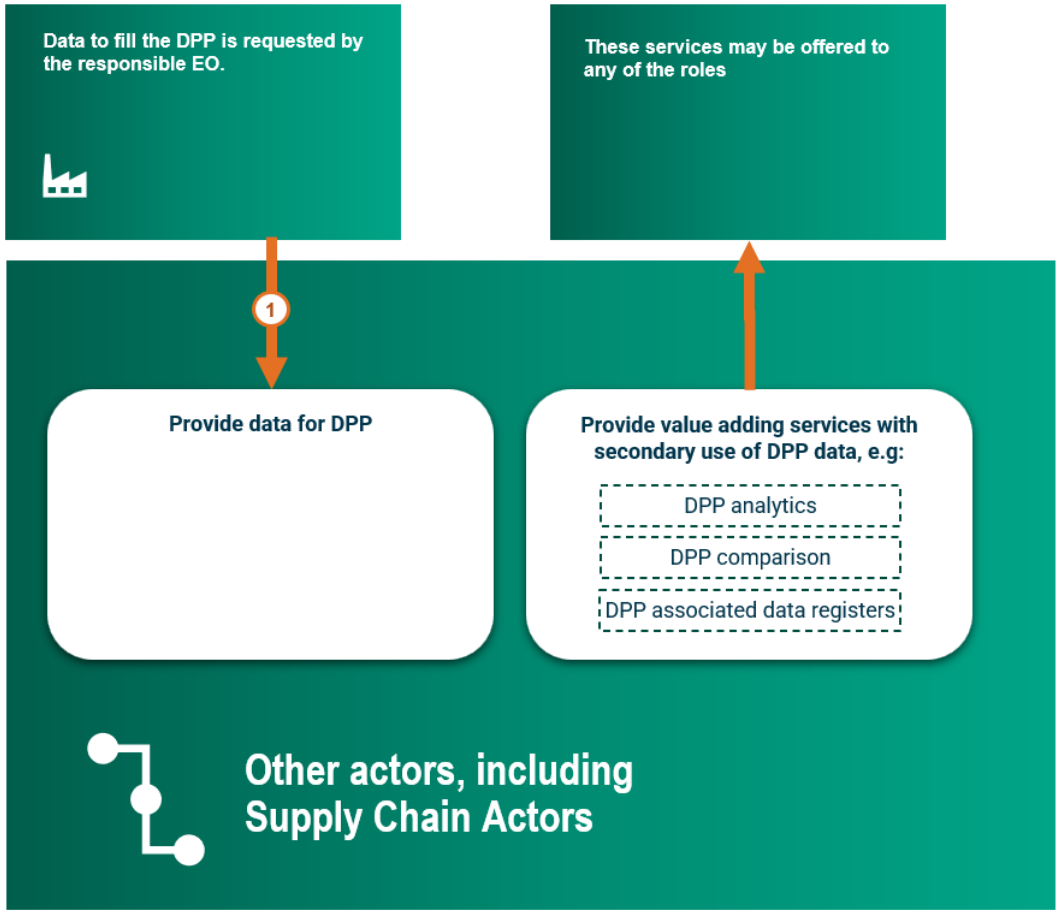


FIGURE 9: BUILDING BLOCKS FROM THE CREDENTIALS AND ISSUING AGENCY PERSPECTIVE

Building block name OPTIONAL = NOT STRICTLY MANDATORY BUT HELPFUL TO SUPPORT INTERACTIONS WITH THE DPP SYSTEM AS DEFINED IN THE USER STORIES V3	Description WHAT IS THIS SERVICE SUPPOSED TO DO?	Input WHAT DOES THE SERVICE TAKE AS AN INPUT TO PERFORM ITS FUNCTION?	Output WHAT IS THE RESULTING OUTPUT OF THIS SERVICE?	Considerations RECOMMENDATIONS FOR APPLICATION SERVICES, INCLUDING WHAT IS NEEDED FOR INTEROPERABILITY
Credentials issuer	Evaluate requests for credential assignment and assign credentials, including assigned roles, to authorized actors. These credentials and assigned roles then provide scoped access to the DPP ecosystem.	• Proof of the identity of the requesting actor	• Credentials in the appropriate format (e.g. SD-JWT in case of OIDC4VC). • A message or a code (e.g. HTTP status code) if the credentials issuance is declined.	Credentials based on delegated acts may be issued by public authorities (at multiple levels) and sectoral organizations. A responsible EO may issue additional credentials to be used for their specific use cases and systems. If verifiable credentials are used as means of authentication, the credentials are assigned from a credential issuer (based on the user information provided at user registration time) and then stored by the user requesting it in a wallet on its device. The credential issuer should keep a list of revoked, expired credentials. The credentials assignment might be performed by: 1. a credentials agency compliant with eIDAS 2 as a SD-JWT Verifiable credential 2. a rEO identity provider as a plain JWT Relevant architectural recommendations: • Utilize eIDAS 2.0 Verifiable Credentials for identity • **Error! Reference source not found.** • Ensure credentials are issued by trusted bodies

OTHER ACTORS, INCLUDING SUPPLY CHAIN ACTORS



Position in the context view

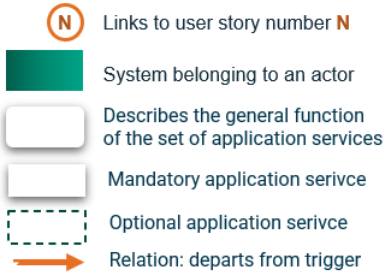


FIGURE 10: BUILDING BLOCKS FROM THE OTHER ACTORS PERSPECTIVE

Building block name OPTIONAL = NOT STRICTLY MANDATORY BUT HELPFUL TO SUPPORT INTERACTIONS WITH THE DPP SYSTEM AS DEFINED IN THE USER STORIES V3	Description WHAT IS THIS SERVICE SUPPOSED TO DO?	Input WHAT DOES THE SERVICE TAKE AS AN INPUT TO PERFORM ITS FUNCTION?	Output WHAT IS THE RESULTING OUTPUT OF THIS SERVICE?	Considerations RECOMMENDATIONS FOR APPLICATION SERVICES, INCLUDING WHAT IS NEEDED FOR INTEROPERABILITY
DPP comparison	Compare data between at least two, (possibly multiple) DPPs on relevant criteria. This might be useful for a consumer before product purchase. Product comparison will be enabled by the EC Web Portal.	• A set of DPP data belonging to multiple DPP • Comparison options (e.g. preferred ranking, relevant fields to compare the DPPs...)	• A visual comparison of DPP data, possibly customized, interpretable for the user.	Relevant architectural recommendations: • Align with existing APIs for value-added services
Analytics (optional)	Use DPP data to provide some specific insight(s). Analytics might be useful for: • An rEO to get insights on product lifecycle and improve future product design • Public authorities for market surveillance operations and compliance checks.	• The DPP data, specifications of the required output or analysis type.	• Required information	Given that a DPP is a knowledge graph based on ontologies, an analytics service might take the form of a semantic reasoner working as a suggestion system. Relevant architectural recommendations: • Standardize the default exchange format as JSON-LD • Align with existing APIs for value-added services
DPP associated data registers (optional)	Stores voluntary data to supplement a DPP	• Additional DPP data • DPP UPI / URL	• Registered DPP associated information	Information about a product which is not mandatory and which is not stored by the EO responsible for the DPP can be stored by other organizations. Examples of such data can include reviews, independent data about product by NGOs or consumer advocacy groups or repair data which is not legally required to be part of a DPP. Relevant architectural recommendations: • Align with existing APIs for value-added services

3 KEY ARCHITECTURAL RECOMMENDATIONS

The building blocks outline the components which jointly form the proposed DPP system architecture. We expect that various actors in the DPP ecosystem will provide (a subset of) the building blocks in their own (unique) system. For the benefit of all DPP stakeholders, these systems need to interoperate, supporting seamless and secure interactions between different or multiple DPP systems. Achieving interoperability requires agreements and/or standards on specific aspects of the system, particularly those aspects that, without alignment, would impose undue additional effort for users that interact with different or multiple DPP systems. For each aspect we identified that would require an agreement at the ecosystem level, we make a recommendation about what we believe the agreement should be. The recommendations are aimed to align with the guiding principles discussed in the introduction, and are aimed to collectively address the remaining legal requirements of the ESPR regarding the DPP system.

The topics discussed in this chapter were selected based on conversations with different stakeholders, were identified by the pilot projects, or were considered crucial in the CIRPASS proposal for the DPP system architecture or in other relevant architectures[18]. The recommendations we make on these topics draw on these sources:

- CIRPASS: The CIRPASS deliverables, mainly D3.2 'DPP System Architecture'[19]
- Process: These issues were identified during the creation and intermediate validation of the architecture and the user stories
- Options for search[20]: deliverable 'Options for EU web portal search' by the CIRPASS-2 project
- Options for redirection to the mandatory DPP backup copy[21], by the CIRPASS-2 project
- DPP User Stories V3[22], by the CIRPASS-2 project.

The recommendations are divided in 5 categories: Semantic interoperability, Identity and access management, DPP integrity, DPP access, and Data Management, and Display. For each of these 5 categories a visual is presented in which the various recommendations are placed in the context of their application. These provide one way of thinking about how the recommendations relate to each other and are added to improve the readability and understanding. More details on the considerations to determine these recommendations may be found in the appendices.

[18] Such as those in the benchmarked architectures from CIRPASS: Benchmark
[19] CIRPASS System Architecture
[20] Options for EU Web Portal Search
[21] Options for redirection to the mandatory DPP backup copy
[22] DPP User Stories V3

INTEROPERABILITY

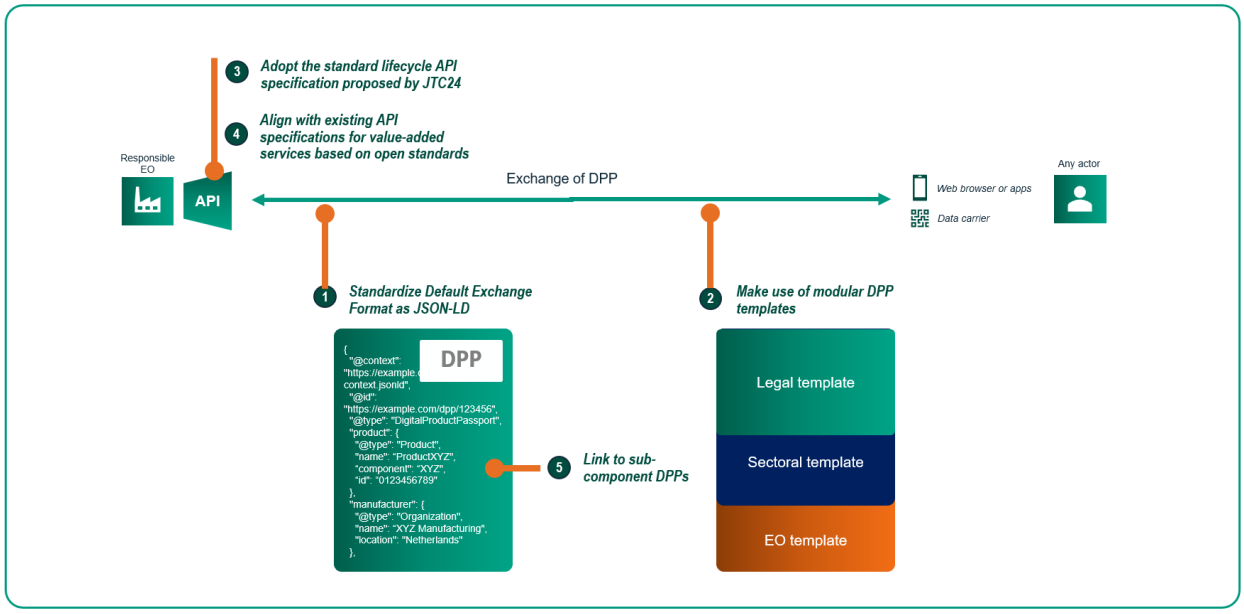


FIGURE 11: RECOMMENDATIONS ON SYNTACTIC AND SEMANTIC INTEROPERABLIITY

1. STANDARDIZE THE DEFAULT EXCHANGE FORMAT AS JSON-LD

Recommendation

Use JSON-LD as the default data exchange format for all DPPs. While other formats may be optionally supported by EOs, providing the DPP in JSON-LD format upon request or exchange should be default.

Problem

DPP data must be based on open standards and an interoperable format, machine-readable, structured, and searchable. A standardized default format is crucial for achieving system-wide interoperability and reducing implementation burden for actors interacting with multiple DPPs.

Rationale

JSON-LD enables semantic interoperability as it allows the inclusion of meaning with the contents and it fully supports RDF/knowledge graphs. Additionally it leverages the widespread tooling and familiarity of JSON (lowering the adoption barrier), and is an open standard.

Implementation guidance and considerations

- All APIs that are intended for interorganizational use, should provide at least JSON-LD.
- EOs remain free to choose their internal storage format.
- EOs are free to provide DPP data in other formats, for instance XML, plain JSON or AAS (Asset Administration Shell) or any other format, in addition to JSON-LD
- Tooling specific to linked data/RDF features within JSON-LD may be used for advanced use cases.

2. MAKE USE OF MODULAR DPP TEMPLATES

Recommendation

Responsible EOs should, where available, make use of predefined, extendable, open DPP templates to promote semantic interoperability.

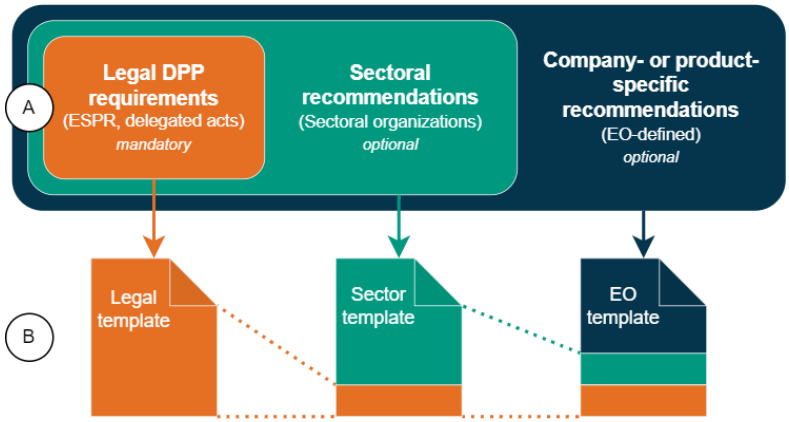


FIGURE 12: INHERITANCE STRUCTURE OF DPP TEMPLATES

DPP templates (as visualized in this diagram) can be seen as empty DPPs with a list of all the required fields ready to be filled in. As illustrated in this image, different sources of requirements (in Part A) can result in different data fields being 'required' in Part B. A template, as illustrated in Part B, is provided as a machine-readable file that defines all these mandatory and optional fields, collected from the different requirements. That is, from the sets of DPP requirements depicted in part A, DPP templates can be distilled for the various levels in part B.

The delegated act for each product category will specify the mandatory data for a DPP, and the required detail level of the DPP. A DPP may be required on the level of a product model, on the level of a batch (or production run) of a product, or for each individual product. Where the Delegated Acts will specify the mandatory data for a DPP, an economic operator may choose to add additional, optional, data at each of these levels. This data can be a part of the template issued by a sectoral organization or economic operator, for example, to include information relevant to their business processes.

The use of DPP templates is recommended to improve semantic interoperability throughout the DPP system, as well as maintain compliance with relevant (legal) DPP requirements.

Problem

DPPs must incorporate data requirements from multiple sources (ESPR, Delegated Acts, other legislation, sectoral standards, company voluntary data). Managing this complexity while ensuring compliance and machine readability requires a structured approach.

Rationale

The use of modular templates offers an approach for consistent compliance across all required data, facilitates semantic interoperability, allows structured integration of different data granularities, and supports extensibility as requirements evolve.

Paired with our recommendation to use JSON-LD, DPP templates can take the shape of a JSON Schema enhanced with a set of SHACL[23] shapes. The JSON schema provides the syntactic validation rules, the data in the JSON-LD document refers to internationally standardized vocabularies, and the SHACL provides the semantic validation rules for the RDF graph that is encoded in the JSON-LD DPP. A 'vocabulary service'[24] may store and provide these templates and additionally may provide support for translating between DPPs based on different templates.

Implementation guidance and considerations

- Any role may offer templates
- Alignment with other templates and standardized data models should be pursued.
- Templates should contain sections specifying sets of data fields, based on the Delegated Act for the product type concerned
- Templates should be offered in JSON-LD format, and we recommend using technologies like JSON Schema (for syntax/structure) combined with SHACL (for semantic/RDF validation) to define machine-readable templates.
- Requires a service for managing, validating, and distributing these templates.

3. ADOPT THE STANDARD LIFECYCLE API SPECIFICATION PROPOSED BY JTC24

Recommendation

Adopt the standardized set of core APIs to manage the DPP lifecycle, which will be defined by JTC24 standard 8. Such an API is expected to Minimally include operations for READ (accessing DPP data), CREATE (initiating a DPP), UPDATE (adding information, respecting immutability), DELETE (managing lifecycle status, not physical deletion of mandatory records), and BACKUP/TRANSFER (ensuring data portability).

Problem

Essential DPP operations need to be performed consistently across different DPP provider systems. Standardization is required for basic interoperability to access and update DPP data.

Rationale

Guarantees baseline functionality and interoperability across the DPP ecosystem. Alignment with relevant standards, especially the results of JTC24, is key to interoperability. Facilitates the data portability of DPP data.

Implementation guidance and considerations

- Detailed OpenAPI specifications for the APIs would allow for easier interoperability

[23] W3C standard
[24] As defined by the International Data spaces association: Vocabulary hub

4. ALIGN WITH EXISTING API SPECIFICATIONS FOR VALUE-ADDED SERVICES

Recommendation

Adopt (or align with) commonly used additional, optional API specifications leveraging the DPP infrastructure (identity, data, core APIs) to support voluntary data exchange, integration with external systems (LCA tools, ERPs, repair platforms), and as a tool to reduce the burden of reporting for other (EU) regulations.

In addition, partake in – and utilize results of - forums for (international or sector-led) standardization of optional APIs.

Problem

The DPP infrastructure provides a foundation that can support business processes far beyond basic compliance. Facilitating standardized ways to extend functionality will utilize its potential value.

Rationale

Alignment with commonly used, additional and/or optional API specifications allows for wider and easier access to more data. Providing more data, and particularly standardized data, promotes innovation and unlocks further economic value from the DPP ecosystem. This enables richer data sharing and service integration (e.g., detailed circularity tracking, predictive maintenance, automated reporting) using trusted mechanisms. Supports evolution towards (sector-specific) data spaces.

Implementation guidance and considerations

- Prefer alignment with API specifications based on open standards
- Make use of REST APIs
- API design might include parameters for requesting specific views or segments.
- Support batch retrieval of DPP data
- Support business-to-business search capabilities (possibly limited to trusted partners)
- Publish detailed OpenAPI specifications for newly created APIs
- APIs should provide data (at least) in the standard exchange format JSON-LD
- Ensure API design respects data immutability
- Ensure API extensions remain compatible with the core DPP system. Participation and use of these API specifications is voluntary.
- Design all DPP data to inherently support granular access control, enabling retrieval or modification of specific data segments based on the verified identity and role(s) of the requesting actor.

- An ecosystem of API specifications and agreements about the APIs can potentially evolve into a Data Space[25], which contains a framework of agreements that relate to data discovery, access control, usage control etc.

5. LINK TO PRODUCT COMPONENT DPPS

Recommendation

If a product incorporates a component with its own DPP ('sub-DPP'), the parent product's DPP should store a verifiable, persistent *link* to the sub-DPP, not merely a static copy of its data. In addition to a link, an up to date embedding of the data can be considered.

For components *without* their own DPP, relevant data must be stored directly in the parent DPP.

Templates for DPPs should have a standard method to represent product-component relationships where components have independent DPPs, ensuring access to the authoritative, up-to-date sub-DPP data.

Problem

The DPP for a compound product must contain all relevant data for the product itself and, we expect, for all sub-components. Keeping the data up-to-date for more complex products will require significant effort. If sub-components have their own DPP, linking to this DPP will provide a convenient way to ensure correct data, as the responsible economic operator for the sub-component is bound by similar legal requirements regarding correctness.

Rationale

Linking to the DPP of a sub-component ensures that users can trace components and access their most current (DPP) data. It avoids data duplication, staleness, and inconsistency issues inherent in copying, and supports traceability.

Implementation guidance and considerations

- Links should be stable identifiers, leveraging the redirection service.
- DPP templates need fields for sub-DPP links.

[25] Data Spaces Support Centre

IDENTITY AND ACCESS MANAGEMENT

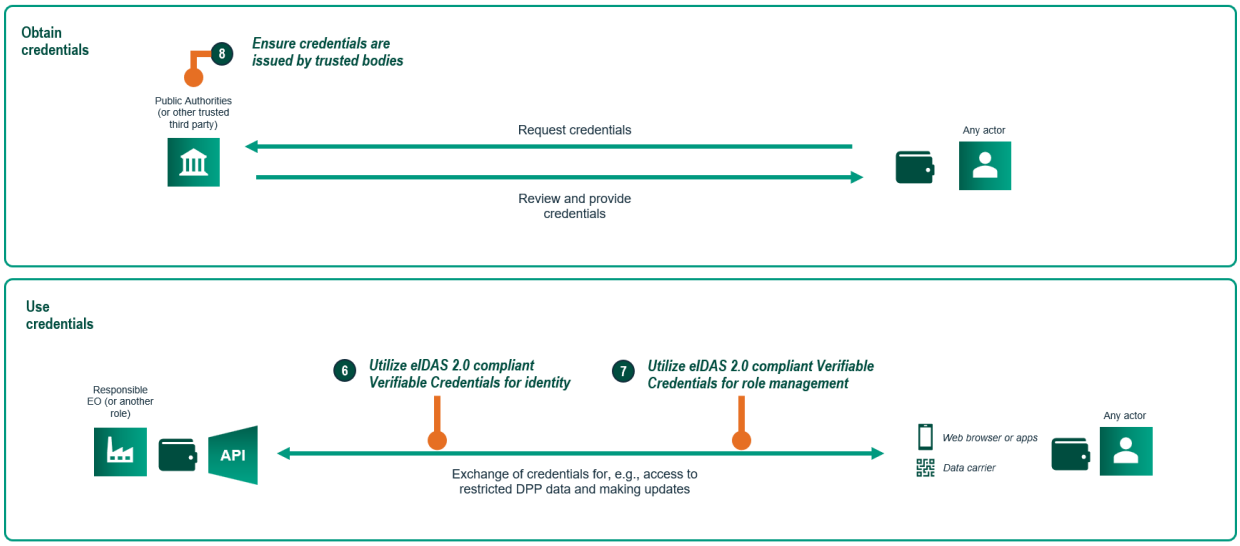


FIGURE 13: RECOMMENDATIONS ON IDENTITY AND ACCESS MANAGEMENT

6. UTILIZE CENTRALLY ISSUED VERIFIABLE CREDENTIALS FOR IDENTITY

Recommendation

The DPP system requires organizations to be able to provide a reliable and trustworthy identity. We recommend using Verifiable Credentials for the DPP system for correct and reliable functioning. Verifiable Credentials are digital identities issued by trusted third parties that can be independently authenticated and digitally verified. These Verifiable Credentials should be issued by EU trusted credential issuers and should be conformant to the SD-JWT based Verifiable Credential specification[26].

The party requesting the credentials for its own usage should store them in a wallet on its device. We strongly recommend using an eIDAS2.0 compliant wallet[27], even if no eIDAS 2.0 identity credentials can (yet) be used.

1. Where possible, eIDAS 2.0 verifiable credentials should be used, to promote interoperability across sectors and member states. If this is not possible for a sector or product type, implementing identity management which provides a migration path to eIDAS 2.0 is strongly recommended.
2. The issuance of identity identifiers by a (centralized) trusted body is recommended, as this will enhance trustworthiness of these identities and avoid the administrative burden required if each economic operator issues its own identifiers.

[26] SD-JWT-based Verifiable Credentials (SD-JWT VC)
[27] EUDI Wallet

3. We recommend that access of non-EU supply chain actors, for instance suppliers of textiles to an EU-based garment manufacturer, to the DPP system is taken into account where necessary.
4. Identities for organizations should either be issued by trusted bodies or authenticated by trusted bodies to support Self Sovereign Identity
5. Identifiers for facilities should have the same level of trust as those for organizations, meaning that issuance by (centralized) trusted bodies is preferred, although it is not required.

Problem

To ensure data quality, authentication, confidentiality and integrity, it is crucial that organizations that need to access restrict DPP data can

6. be reliably and verifiably identified, and
    a) can use these credentials easily and conveniently in the entire system across the EU.

This requirement exists both for the initial registration of a DPP in the EU registry, where the EC needs to ascertain the identity of the organization involved, and for accessing sensitive information contained in a DPP, when the responsible Economic Operator needs to ascertain the identity.

The use of a verifiable and trusted identity allows organizations, individuals, and the EU to determine the level of trust for organizations and the data supplied by them. Since existing systems for digital identity are not always interoperable, we recommend an EU-backed solution, making digital identities usable across the EU.

At the same time, the ESPR requires the DPP system to be open and accessible to a wide variety of actors. To maximize opportunities without introducing excessive risks for economic operators, consumers, and countries, a careful balance must be struck between openness and access control.

The issuance of identifiers for facilities by a (centralized) trusted body is recommended, as this will reduce the administrative burden, both for economic operators and for the EC, which will be present if each economic operators assigns its own identifiers for facilities.

Rationale

A third-party ensured digital identity ensures the reliable and verifiable identification of an actor interacting with the DPP system. This digital identity must be issued by a trusted party and must be verifiable to avoid abuse.

eIDAS 2.0 compliant Verifiable Credentials provide the required balance between openness and access control. As long as eIDAS 2.0 is not yet fully operational, using a technology which provides a relatively straightforward upgrade path to eIDAS 2.0 should be used.

Implementation guidance and considerations

- Access of non-EU supply chain actors, for instance suppliers of textiles to an EU-based garment manufacturer, to the DPP system should be taken into account.

7. Identities for organizations should be guaranteed by trusted bodies. This means that an identity can be issued by a trusted body, or a trusted body can validate a self-issued identity (by issuing a verifiable credential for the self-issued identifier), supporting the use of self-sovereign identity.

- As eIDAS 2.0 has not yet been widely implemented, a phased approach to identity and access management can be adopted by organizations. As eIDAS 2.0 will support verifiable credentials in a JSON Web Token (JWT, based on SD-JWT[28]), it is strongly recommended to implement identity management using a wallet using the OpenID for Verifiable Presentations protocol[29].
- A less advanced option is to base identity management on JSON Web Tokens, with an operator providing their own identity management for all organizations they have a relationship with. JWTs are very widely used and supported, and adopting JWTs will facilitate the adoption of eIDAS 2.0 tokens later. If this option is implemented, the access control mechanism can be based on the type and issuer of the supplied token to support both eIDAS 2.0 and custom schemes.
- For economic operators considering a temporary solution until eIDAS 2.0 is adopted universally in the EU, sufficient key management techniques exist using JWT's. Organizations providing identity management can, for instance, implement digital signing for JWTs and limit the usability by specifying the intended audience and setting a limited lifetime for each token. Since the provenance of these signing keys is not government-backed as eIDAS 2.0 is, additional measures, such as signature verification, may be required.

7. UTILIZE ROLE-BASED ACCESS CONTROL BASED ON GENERIC ROLES

Recommendation

For digital third party authenticated roles, as for identities, we recommend using Verifiable Credentials. These verifiable credentials should preferably be issued by one or more EU trusted credential issuers as 'Qualified Electronic Attestation of Attributes (QEAA)', as proposed in the eIDAS 2.0 regulation, and be conformant to the SD-JWT based VC specification[30].

The party requesting the credentials for its own usage should store them in a wallet on its device; we strongly recommend the use of an eIDAS 2.0 compliant wallet.

1. We recommend a generic set of roles to be defined at the level of the EC and detailed further, where necessary, under the upcoming delegated legislation, as per Art. 10(g) and 11(f).
2. We recommend the use of role-based access control (RBAC) as the access control mechanism in the DPP system.
3. We consider access of non-EU value chain actors to the role issuance to be optional

Problem

Access to specific information in a DPP can be limited to organizations, based on the relevant delegated acts for mandatory data and optionally on the permissions granted by the economic operator for voluntary data. Permissions to provide updates to a DPP will certainly be limited.

These restrictions require a system for economic operators to recognize and verify organizations in order to ensure confidentiality of sensitive information as well as the data quality, authentication

[28] SD-JWT-based Verifiable Credentials (SD-JWT VC)
[29] OpenID for Verifiable Presentations - draft 24
[30] SD-JWT-based Verifiable Credentials (SD-JWT VC)

and integrity of any data provided by third party. Such a system must be technically feasible and economically viable for each economic operator that provides a DPP.

Rationale

Many different access control mechanisms are in use in digital systems. Requiring any organization performing a role in the DPP system to support different access control mechanisms is inefficient and expensive. We therefore propose the introduction of a generic system for role assignment in the DPP system and the use of role-based access control.

We expect that there will be different categories of data with different degrees of access rights in the DPP system. Access rights could be different for the general public, public authorities, economic operators with legitimate interest, specific partners and affiliates of an economic operator, independent operators, and possibly other types of actors as well.

Although the ESPR does not explicitly mention role-based access control, roles are the only criterium mentioned regarding access rights. A more comprehensive and detailed method for access control, like Attribute-based access control, does therefore not seem legally required. Of course, economic operators may choose to implement more fine-grained access control based on multiple attributes, but as roles are recognizable, can be backed by trusted bodies (see our recommendation to that effect), are commonly used for access control, and can easily be integrated in more fine-grained access control systems, we believe role-based access control provides the optimal balance between complexity, (regulatory) compliance and ease of use for access control.

Using Verifiable Credentials for the DPP system to provide verified roles to organizations in the DPP system can provide a generic system for role management. These verifiable credentials should preferably be eIDAS 2.0 credentials, but if this is not possible they should conform to the SD-JWT based VC specification. SD-JWT tokens allow the Verifiable Credentials owner to selectively disclose information about itself, ensuring the verifier only receives roles and information that are needed to grant access to a specific resource. On the other hand they preserve traditional JWT properties like the provisioning of roles and other user properties (e.g. name, organization, country) as claims (key value pairs in the JSON token). This will allow for an easier adoption of Verifiable Presentation in more traditional JWT authorization mechanism based on roles on other user assertion stored in claims.

Supporting different categories of data accessible to different roles only seems feasible if a common set of roles is specified at the European level, possibly further differentiated per product group in the delegated acts, as required by Art. 10(g) and Art. 11(f). Such a common set of generic role descriptions and definitions facilitates interoperability across product categories and sectors, while the more detailed definition in delegated acts allows for access rights tailored to product types. These definitions should be extensible and interoperable, in order to allow flexibility. For instance, a generic role definition may provide attributes for ‘repairers’, which can be extended at product group level to refer to ‘battery repairer’ or ‘textile repairer’.

At the most granular level an economic operator can choose to assign additional roles to an organization, granting them extra access. such as access to voluntary product-specific data on the DPP system to their preferred or certified repairers. A common, extensible EU-level core of definitions of roles and associated access rights is a basis for verifying DPP access requests at scale. The assignment of roles to organizations can be performed by governments or government-mandated organizations. Trade organizations or comparable institutions can play an important role as well, by certifying that an organization is qualified to perform a certain role. eIDAS 2.0 provides a well-defined mechanism to enable role assignment using ‘Qualified Electronic Attestation of Attributes (QEAA)’, in which ‘Qualified trust providers’ can issue credentials.

Implementation guidance and considerations

- Using the 'Qualified Electronic Attestation of Attributes (QEAA)' as proposed in the eIDAS 2.0 regulation provides a trustworthy system for role assignment. We propose using technology which provides a relatively straightforward upgrade path to eIDAS 2.0, until eIDAS 2.0 is operational and Qualified Trust Providers are capable of providing assigning these attributes.
- Access of non-EU supply chain actors, for instance suppliers of textiles to an EU-based garment manufacturer, to the DPP system should be taken into account.
- Official roles for organizations should be guaranteed by trusted bodies, like a public authority, trade association or sectoral organization.
- As eIDAS 2.0 has not yet been widely implemented, a phased approach to role management can be adopted by organizations. As eIDAS 2.0 is expected to support verifiable credentials in a JSON Web Token (JWT, based on SD-JWT[31]), it is strongly recommended to implement roles using a wallet using the OpenID for Verifiable Presentations protocol[32].
- An alternative option for situations where eIDAS 2.0 is not (yet) usable or feasible, is to base role management on JSON Web Tokens or individual access token (API keys). This requires each operator to provide their own role management for all organizations they have a relationship with.
    - JWTs are very widely used and supported, and using these now will facilitate the adoption of eIDAS 2.0 tokens later. If this option is implemented, the access control mechanism can be based on the type and issuer of the supplied token to support eIDAS 2.0 and different schemes.
    - For economic operators considering this solution until eIDAS 2.0 is adopted universally in the EU, sufficient key management techniques exist using JWT's. Organizations can, for instance, implement digital signing for JWTs and limit the usability by specifying the intended audience and setting a limited lifetime for each token. Since the provenance of these signing keys is not government-backed as eIDAS is, additional measures, such as signature verification, may be required.
    - The option to supply trusted partners with a specific, individual access token (or API key) is of course always available to enable access control. As these types of tokens usually do not expire, these require even more additional measures to maintain security.

[31] SD-JWT-based Verifiable Credentials (SD-JWT VC)
[32] OpenID for Verifiable Presentations - draft 24

8. ENSURE CREDENTIALS ARE ISSUED BY TRUSTED BODIES

Recommendation

Use the digital identity for organizations as provided by eIDAS 2.0. Use Qualified Electronic Attestation of Attributes, as proposed in eIDAS 2.0, for other credentials, such as roles. These credentials are issued or guaranteed by government, providing the maximum amount of trustworthiness.

As elaborated in the earlier recommendations, public authorities are the preferred parties to issue, or guarantee, identity credentials and role credentials, since these can then be used across Europe and across organizations.

Problem

As described in the previous recommendations, guaranteeing trust is crucial for the correct working and the adoption of the DPP system. Credentials used in this system must therefore be trustworthy.

Rationale

Guaranteeing trust can be achieved when using, where possible, credentials issued, or backed, by recognized and trusted bodies. Both the identity and the roles/qualifications of an organization should be backed by government, or government-mandated, organizations.

Implementation guidance and considerations

- As long as eIDAS 2.0 is not fully used, relying on other trusted bodies must be considered. A national Chamber of Commerce may be able to provide identity assurances, sectoral organizations can provide assurances on expertise, official certifications from educators and certification authorities are all trustworthy.
- If no widely trusted organization can provide assurances, a fallback scenario is for an economic operator to issue its own credentials, or to form bilateral or multilateral agreements with other economic operators, forming a web of trust.

DPP INTEGRITY

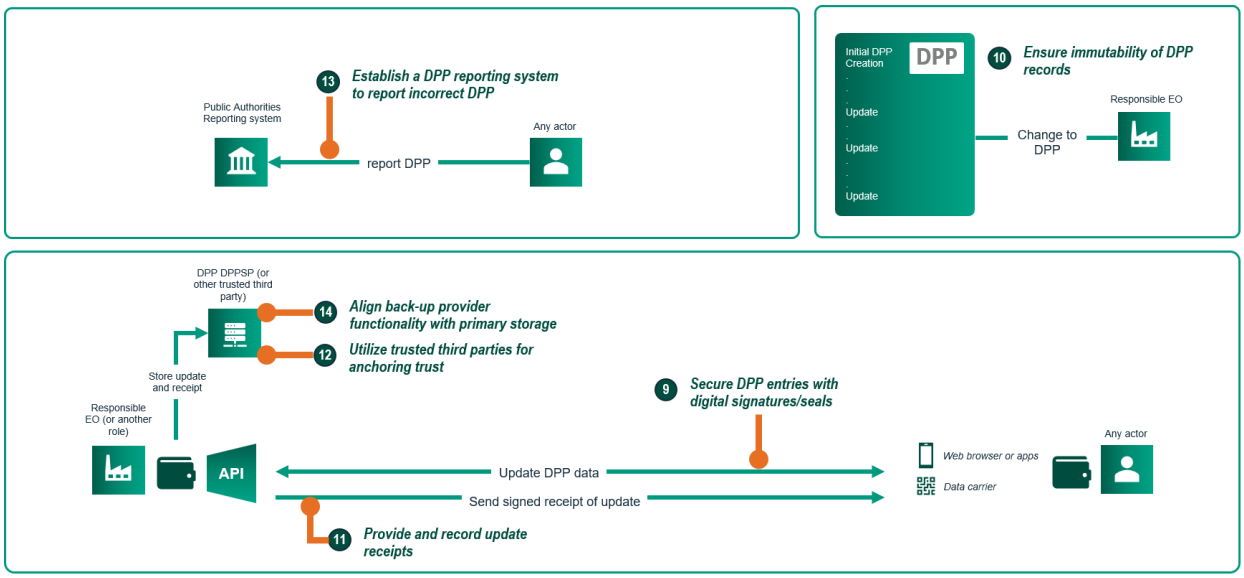


FIGURE 14: RECOMMENDATIONS ON DPP INTEGRITY

9. SECURE DPP ENTRIES WITH DIGITAL SIGNATURES/SEALS

Recommendation

Each immutable DPP data entry (initial DPP created by an EO and subsequent updates by authorized parties) should be cryptographically secured using mechanisms like digital signatures or electronic seals to guarantee authenticity (verifiable origin) and integrity (tamper-evidence). Prioritize alignment with and migration towards eIDAS 2.0 mechanisms (e.g., Qualified eSeals for EOs).

Problem

DPPs need strong, verifiable proof of data origin (authentication) and assurance that data has not been altered (integrity) to ensure trustworthiness of the data and guarantee usability.

Rationale

Digital signing provides robust cryptographic guarantees essential for trust. Alignment with eIDAS 2.0 leverages an EU-wide framework for trust services, ensuring interoperability and legal recognition.

Implementation guidance and considerations

- Use techniques that align with eIDAS 2.0
- Requires PKI and key management, linking identities (IAM) to keys. Until eIDAS 2.0 solutions are widespread and affordable for all (esp. SMEs), interim solutions like standard digital signatures (potentially linked to VCs) combined with third-party anchoring are needed.
- JWTs can carry signed hashes for updates.

- Integrate signing/sealing into DPP creation/update workflows.
- When DPP data is displayed in a non-default way, for instance in another language, the provided signature will not correspond to the displayed data. When displaying DPP data and signatures, the difference between "source data" and "displayed data" must be made clear.

10. ENSURE IMMUTABILITY OF DPP RECORDS

Recommendation

DPP systems should ensure that the initially created DPP record and all subsequent updates are treated as immutable entries. Modifications should be recorded as new, separate, timestamped entries linked to the DPP's history, not by altering previous records.

Problem

Allowing modification of historical DPP data undermines integrity, data traceability, and the ability to ensure data is "accurate, complete and up to date" based on a verifiable history.

Rationale

Allowing changes to the data in the original DPP creates many risks, both for (accidental) non-compliance and for fraud. Maintaining all data as created and providing all updates as separate events creates a tamper-evident, auditable trail of all information added to the DPP over time. This also guarantees the integrity of each data entry and allows reconstruction of the DPP's state at any point in time. We consider this recommendation to be foundational for trust.

Implementation guidance and considerations

- Storage systems and APIs should enforce write-once or append-only logic, with each entry requiring a digital signature / seal.
- Technologies like immutable databases or distributed ledgers can support this, but the principle applies regardless of technology.

11. PROVIDE AND RECORD UPDATE RECEIPTS

Recommendation

When a responsible EO's system stores a DPP update provided by an authorized third party, the system should generate and provide a digitally signed receipt back to the submitting party. This receipt should confirm reception and include verifiable proof of the submitted content (e.g., signed hash). Both parties should retain this receipt.

Problem

Third parties submitting (potentially valuable) update data need verifiable proof of submission and content integrity. Relying solely on the EO's record creates risk of disputes or data loss/manipulation claims. Mutual proof is needed for trust and non-repudiation.

Rationale

Creates a verifiable, non-repudiable audit trail of the update transaction for both submitter and receiver. Enhances trust, accountability, and resolves potential disputes regarding updates. Mitigates risks of responsible EO data manipulation.

Implementation guidance and considerations

- Requires definition of a standard format/protocol for update receipts, preferably adopted by the EC. Integrate receipt generation, signing (by EO system), and delivery into the update workflow.
- Consider anchoring receipt evidence with a third party

12. UTILIZE TRUSTED THIRD PARTIES FOR ANCHORING TRUST

Recommendation

Implement mechanisms to store cryptographic evidence of DPP data authenticity and integrity (e.g., signed hashes of original DPP entries, updates, and receipts), as well as other claims in or about the DPP with an independent trusted third party.

Problem

Relying solely on the data holder (EO) for integrity proof will not be sufficient for high-assurance scenarios or dispute resolution. Trust requires independent verification.

Rationale

Provides an independent anchor point for verifying data provenance and integrity over time. Increases overall system trustworthiness, especially important during the transition to full eIDAS 2.0 mechanisms.

Implementation guidance and considerations

- Use techniques that align with eIDAS 2.0
- Agreements about which parties are considered trusted have to be made in e.g. the nation, sector or value chain. This includes making decisions on:
    - Clarify the roles and requirements for anchoring services.
    - The specific cryptographic evidence to be anchored (e.g., hash trees, signed roots).
    - Specify protocols for submission to and verification against the trusted third party.
- As each DPP must be registered in the EU registry, the most trustworthy partner to store such cryptographic evidence would be the EC. Making this evidence available to the public would require additional effort for the EC.

13. ESTABLISH A DPP REPORTING SYSTEM TO REPORT INCORRECT DPPS

Recommendation

A system should exist to register the status of a DPP, allowing parties to indicate that a DPP is incorrect or invalid.

- As the EU Web Portal can be used to retrieve all DPPs this might provide a way to register concerns regarding an individual DPP.
- A system for reporting mass DPP problems, for instance at the product level, should be made available to market authorities and market surveillance authorities.

Problem

DPPs can contain errors and can even be completely fraudulent. Without a mechanism to flag these situations, the trust in the DPP system can be seriously degraded.

Rationale

Errors can occur at every stage of the DPP lifecycle. As DPPs are adopted more widely and usage increased, also the temptations for abuse increase. This risk can be mitigated by providing a system to flag incorrect DPPs.

Providing a reporting system for individual DPPs is necessary. A system to invalidate or flag DPPs at scale is strongly recommended for authorities, but access to such a system must be controlled as this introduces additional possibilities for large-scale abuse.

Implementation guidance and considerations

- As DPPs must be compliant with the relevant regulations, it is expected that relevant market surveillance authorities will be designated to ensure this compliance. In addition, consumers can also ne abled a possibility to flag possible violations in the DPPs, perhaps through the EU Web Portal.

14. ALIGN BACK-UP PROVIDER FUNCTIONALITY WITH PRIMARY STORAGE

Recommendation

DPP backup providers (DPPSPs) should store all DPP data managed by the EO, including optional data, and should keep the back-up up-to-date. They should enforce the same access control rules.

Problem

Backups should be functionally equivalent to the primary system regarding data completeness, security, and (ideally) dynamic updates to be truly effective substitutes. Discrepancies may render the backup obsolete if updates aren't mirrored.

Rationale

Ensures the backup provides a complete and usable reflection of the primary DPP data and access rights. The responsible economic operator is legally required to ensure that at least one independent third party (a DPP service provider, ‘DPPSP’) hosts a back-up of the DPP. This backup must be complete and up-to-date at the moment the DPP is created and registered with the EU. Since access to some data in a DPP may be limited, depending on the relevant regulations, a backup provider must provide similar access controls as the responsible economic operator, to avoid sensitive data becoming available from a backup.

Implementation guidance and considerations

- Define clear technical and contractual requirements for DPPSPs covering data scope, exact mirroring of access controls, and mechanisms for receiving/applying updates.

DPP ACCESS

FIGURE 15: RECOMMENDATIONS ON DPP ACCESS

15. ENSURE UPI-TO-URI REDIRECTION AS THE RESPONSIBLE EO

Recommendation

The responsible EO should ensure the operation of a redirection service that translates a product's Unique Product Identifier (UPI) from its data carrier into the current network location (URI) of its DPP data. Data carriers should resolve to an entry in this redirection service.

Problem

Directly encoding DPP location URIs onto physical data carriers is inflexible; locations change over time (system migration, company changes), rendering static links obsolete. Data carriers have limited capacity/format constraints. Reliable, persistent access is needed.

Rationale

Using a redirection service decouples the persistent product identifier from the potentially changeable data location, providing essential long-term flexibility and resilience. Allows DPP URIs to be updated without modifying physical products. Supports scenarios like migration, divestiture, or fallback to backups and the EU UPI-to-URI redirection service.

Implementation guidance and considerations

- The responsible EO should use a redirection service that remain available after the responsible EO ceases operations.
- Each redirection service provider should ensure that their service remains even in the case of insolvency.
- Redirection service providers should allow for easy portability to other redirection services.

- EOs are responsible for maintaining correct target URIs for their products' UPIs in the service.
- The EC or the entities that provide redirection services should consider to create a catalogue of the redirection services offered by different entities, to aid the discoverability of DPPs.

16. ESTABLISH A FALLBACK EU UPI-TO-URI REDIRECTION SERVICE

Recommendation

The European Commission should operate, or ensure the operation of an independent and persistent UPI-to-URI redirection service for the entire DPP system. EOs can and should utilize other redirection services, provided that their DPP products' UPIs are also resolvable via the EU redirection service as a minimum requirement for a reliable fallback.

Problem

The DPP system is product-centric: a DPP is tied to a product and accessing the DPP will be based on the unique product identifier. This means that a clear and reliable way to use the unique product identifier to determine the location of a DPP is required. A guaranteed, vendor-neutral fallback mechanism (a ‘redirection service of last resort’) is recommended for system stability and long-term data access.

Rationale

Economic operators are required to assure access to the DPP of their products. Making sure that this redirection service remains operable for the required time span is difficult and can fail for many reasons outside the control of the economic operator. In this case only the UPI will be available, the fallback redirection service can then identify where the relevant DPP is stored. In case the responsible EO and the DPPSP are both not available, the fallback redirection service could ensure that scanning the data carrier still leads a customer (or other users) to the appropriate DPP.

Implementation guidance and considerations

- EC to define infrastructure, governance, operational model, and APIs for this fallback service.
- Include policies for managing entries, especially updates when the original EO is non-responsive (e.g., pointing to backup via DPPSP).

17. PROVIDE A DISCOVERABLE MODEL LEVEL DATA ENDPOINT

This Recommendation

Economic Operators should make generic, model-level DPP information publicly discoverable via a standardized .well-known URI endpoint on their primary website. The suggested structure is "*https://<operator_website>/.well-known/dppdata*".

Problem

General discovery of DPPs benefits from standardized, machine-readable discovery mechanisms. Making data discoverable carries, however, the risk of exposing commercially or strategically sensitive information.

Rationale

Making model level data discoverable provides a predictable, automatable mechanism for finding DPP data. It facilitates compliance with information requirements for online sales and general product discovery. The /.well-known/ endpoint is simple and widely adopted. This also promotes the decentralized nature of the DPP system rather than (only) relying on a central component.

By limiting the discoverable data to the model level, the undesired exposure of data is prevented. Providing data on batch or even item level enables the disclosure of commercially sensitive (and even strategically sensitive) information like item quantities and sales numbers of suppliers and manufacturers.
For batch or item level data, responsible EOs could consider providing information about ranges or averages to interested parties

Implementation guidance and considerations

- The standard for the document served at this endpoint should be set and adopted by the EC as the recommended standard. I.e. the format in which links to model level data should be provided should be standardized. Providing a proposal for this is out of scope of this document.
- Responsible EOs should implement and maintain this endpoint.
- Responsible EOs may add batch and item level DPP data via the endpoint as well, keeping in mind that the aggregate of this data may be considered sensitive data.

18. CREATE A DATA CARRIER FOR ONLINE AND PRE-PURCHASE USE

Recommendation

For providing access to DPP data in contexts *other than* the physical product itself (e.g., online marketplaces pre-purchase, physical store displays), utilize a separate data carrier that resolves to the model-level data and provides an indication of what batch / item level data can be expected for an instance of the product.

Problem

Information access is needed in various scenarios (online retail, comparison) before gaining access to an instance of a product.

Rationale

Provides appropriate access points for model-level data in relevant contexts without cluttering the physical product. Leverages existing channels like websites, or potentially EPREL-like labels.

Implementation guidance and considerations

- Responsible EO to generate a separate data carrier or link pointing to the model-level DPP URI.
- Do not place a second data carrier on the product itself, as this would mean there are two data carriers on the product, possibly creating confusion. A model-level QR code could be placed on an EPREL-like label, or on in-store displays.

DATA MANAGEMENT

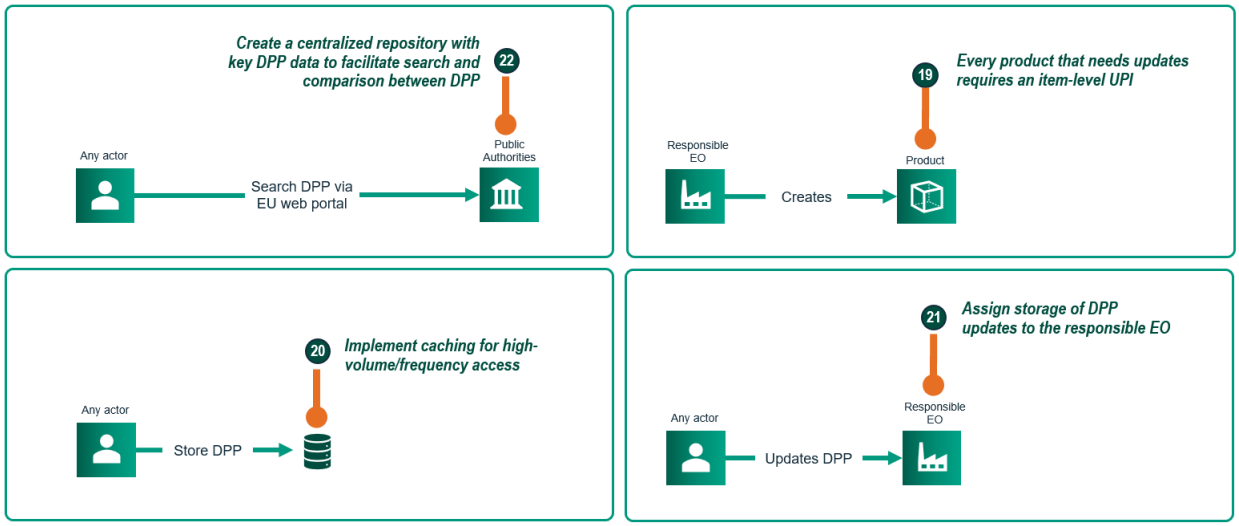


FIGURE 16: RECOMMENDATIONS ON DATA MANAGEMENT

19. EVERY PRODUCT THAT NEEDS UPDATES REQUIRES AN ITEM-LEVEL UPI

Recommendation

Products for which lifecycle events, such as repairs, are expected or required must have a unique identifier for each individual product. This allows the registration of these lifecycle events, since these occur for a specific product and not for a collection of products.

- Issue product-level identification for products which will require life cycle events
- Follow the recommendation for UPI-to-URI redirection, to allow redirection from the unique identifier to the correct DPP (which may initially be a common DPP for a product model, until the data for a specific product changes)

Problem

If repairs, modifications or usage events are expected to occur for specific products, these cannot be registered if no DPP for the specific item exists.

Rationale

Delegated acts can specify that a DPP is required only for a model, without requiring each individual product to have its own DPP. This legal requirement must of course be fulfilled, but Economic Operators may decide to issue product IDs and DPPs at a more granular level, if there is a (economically) valid reason to do so. Supporting life cycle events can be such a reason, if this were not foreseen in the Delegated Act.

Implementation guidance and considerations

- If no item-level DPP is required, all product IDs for specific items can be routed to one generic DPP. As soon as a lifecycle event is registered for a specific product, a separate

DPP can be created for that product, after which the product ID should resolve to this specific DPP

20. IMPLEMENT CACHING FOR HIGH VOLUME / FREQUENCY ACCESS

Recommendation

Parties requiring frequent or bulk access to DPP data (e.g., market surveillance, large repair networks, asset managers) should consider implementing local caching/repositories of relevant DPPs. Any updates made to the products should be shared with the responsible EO.

Problem

Direct, repeated querying of primary EO repositories for each access can be inefficient, slow, and burdensome for both the requester and the EO, especially for frequent operations. Bulk access for, for instance, analytical purposes can similarly be very costly.

Rationale

Maintaining a local cache of DPPs improves access performance, reduces load on primary EO systems, enables offline capabilities, and facilitates large-scale analysis. This comes at the cost of keeping the cached data up-to-date, requiring a balanced caching strategy.

Implementation guidance and considerations

- Caching parties are responsible for maintaining their cache, such that it remains up to date. They should consider to implement mechanisms to check for/retrieve updates from the responsible EO.
- The EO repository remains the single source of truth. Cached updates should ideally be reported back to the responsible EO.

21. ASSIGN STORAGE OF DPP UPDATES TO THE RESPONSIBLE EO

Recommendation

Similar to the storage of the initial DPP, the responsible EO should store relevant updates to their DPPs throughout the product lifecycle, ensuring data remains accurate, complete, and up-to-date. We recommend to include all updates, including updates that are not mandatory, so that a complete view of the product is maintained and the value of the DPP is increased.

Problem

DPP data may need updating after initial creation (e.g., repairs and usage data) to remain accurate and useful. The responsibility for storing the updates is currently not assigned.

Rationale

Storing updates with the DPP best serves the DPP's intended purpose to capture the relevant information about a product to maximize its value throughout the lifecycle (for instance by helping with lifecycle assessments regarding usage and quality aspects), by making the data easily accessible. Additionally, it improves the overall usability of the DPP, as the product history is properly preserved even after a change of ownership.

Implementation guidance and considerations

- DPP data repositories need mechanisms to receive, validate, associate, and store updates linked to the original DPP, respecting immutability principles.
- Independent update storage services could emerge but the primary recommendation is for EO storage.
- A third party providing an update must be identified properly
- For each update a confirmation, preferably providing proof of the contents and the time of the update must be provided to the party providing the update.
- To provide additional trust in the correctness and validity of updates, a responsible EO can provide additional data for each update, such as a 'reliability score'. Updates from certified and/or known repairers could, for instance, be rated as very reliable, where updates from unknown parties could be rated as less certain.
- All updates should be stored, not just updates from some parties. Limiting the updates to specific parties will lead to incomplete DPPs.

22. ESTABLISH AN EU REPOSITORY WITH KEY DPP DATA FOR SEARCH

Recommendation

We strongly recommend the creation of a centralized repository containing key attributes of DPPs as 'search keys' to support the web portal, making it possible to quickly and efficiently find DPPs.

Problem

A search facility will be provided by the EC, the 'Web portal' (Art. 14, Recital 42). In addition to targeted searches for the DPP of a specific product, this portal will provide search capabilities across the DPP system.

Creating a fully distributed infrastructure for search across all DPP repositories has been suggested, but creating such a system which is reliable, efficient, exhaustive and responsive is very complex and will pose a larger barrier for adoption (particularly for smaller organizations). We therefore recommend to *not* implement such an infrastructure.

Rationale

While the search portal is outside the scope of the DPP system, it does have significant consequences for the design of the DPP system. A separate document 'Options for the EU Web portal search'[33] is available, which contains the opinions of the participants in the CIRPASS2 consortium on the relationship between searchability and storage of DPP data.

[33] Options for the EU Web Portal Search

Implementation guidance and considerations

- Data Protection: The ESPR requires the possibility to search for a DPP. It does not require a search possibility for multiple DPPs (of one or more Eos). From a data protection viewpoint, it is of utmost importance that a search function for multiple DPPs is not generally available. Such a function enables the disclosure of commercially sensitive (and even strategically sensitive) information like item quantities and sales numbers of suppliers and manufacturers. For batch or item level data, responsible EOs could consider providing information about ranges or averages to interested parties.

DISPLAY

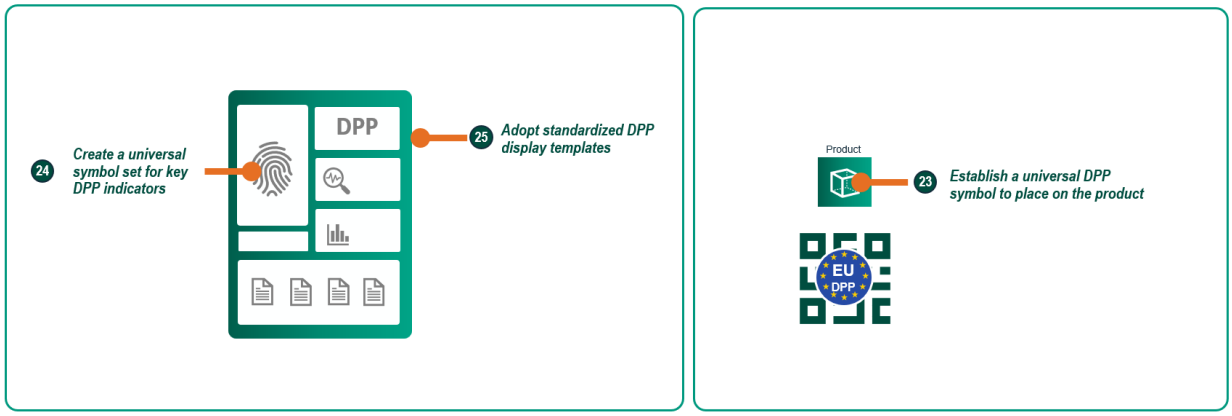


FIGURE 17: RECOMMENDATIONS ON DISPLAY

23. ESTABLISH A UNIVERSAL DPP SYMBOL TO PLACE ON THE PRODUCT

Recommendation

The European Commission should design and promote a universal symbol that clearly identifies a data carrier as the access point to the official Digital Product Passport.

Problem

Products and web pages may contain multiple QR codes or links; users need an unambiguous visual cue to identify the specific one leading to the DPP.

Rationale

Improves usability, reduces user confusion, and creates a recognizable identity for the DPP system access point.

Implementation guidance and considerations

- Promote its recommended use adjacent to DPP data carriers and in digital interfaces pointing to DPPs.
- Avoid having multiple QR codes or links on products where possible

24. CREATE A UNIVERSAL SYMBOL SET FOR KEY DPP DATA

Recommendation

The European Commission should create or commission to create a universal, standardized set of easily recognizable symbols or icons to represent key mandatory DPP data points or indicators (e.g., concerning sustainability, circularity, safety).

Problem

The most relevant information within a DPP needs to be conveyed quickly, effectively, and independently of language. Text labels alone may not suffice for rapid comprehension or comparison.

Rationale

Establishes a consistent visual shorthand for important information, improving understandability and comparability across the single market. Builds on successful precedents like energy labelling symbols.

Implementation guidance and considerations

- Define symbols through delegated acts, and keep these symbols consistent (where applicable) across delegated acts.
- The symbol set should be integrated into display templates and data standards.
- The accessibility of these symbols should be in accordance with relevant regulations (for instance EN 301 549 “Accessibility requirements for ICT products and services”)

25. DEVELOP STANDARDIZED DPP DISPLAY TEMPLATES AND GUIDELINES

Recommendation

The European Commission should develop or commission the development of standardized display templates or clear guidelines for presenting DPP information visually to end-users. This is particularly relevant for access to a DPP without using a dedicated DPP application.

Problem

Inconsistent presentation formats hinder the user’s ability to easily find, understand, and compare DPP information across different products and brands. Dark patterns may also be used.

Rationale

Creates a consistent, predictable, and user-friendly experience, significantly improving usability and comprehension.

Implementation guidance and considerations

- Develop templates/guidelines adhering to common design principles, but potentially varying by product category.
- Could involve defining standard layouts, terminology, and possibly reference implementations (e.g., CSS/HTML snippets).
- Ensure that represented information and user interactions consider vulnerable consumers for which the standard EN 301 549 “Accessibility requirements for ICT products and services”, can be consulted (e.g. the blind, physically disabled, dyslexia and other vulnerabilities).

4 RISKS AND MITIGATIONS

The building blocks described in the previous chapters create a functional system for other actors to build upon. In practice, there will be actors who, due to negligence or malicious intent, can cause harm to DPP systems or users of the system. This must be prevented; therefore, an inventory of risks that exist for the system as a whole has been conducted. Mitigations have also been established. The risks and mitigations are documented separately in the "Risks and Mitigations" document[34].

The technical risks that are relevant to designers and developers of non-central parts of ESPR-compliant DPP systems are described in this chapter. It is essential to sufficiently mitigate these risks. The proposed mitigations can be used for this purpose. Implementations of the DPP system may carry risks that are not covered in this document, because the risks stem from design choices that are not specified in the reference architecture, such as chosen libraries. Therefore, risks arising from these design choices should be considered before such a system is implemented.

The list of core technical risks and possible mitigations can be found below. Every technical risk is preceded with a number, with which the risk can be identified in the "Risks and Mitigations" document, which is more extensive as it considers both technical and non-technical risks in the system. For every risk mentioned, possible mitigations are listed.

Events occurring during the creation of the DPP and product

4. [6A.] A (fake) rEO submits a DPP with bogus information to the system, e.g. the EU registry.
    - Possible mitigation: Only authenticated and authorized EO's can submit a DPP.
    - Possible mitigation: EO's can be (temporary) denied of submitting DPP's.
    - Possible mitigation: Submitted DPP's can be altered, removed or (partly) hidden by a trusted administrator.
5. [7A.] The rEO submits an excessive amount of DPP’s to perform a Denial-of-Service attack.
    - Possible mitigation: A system is in place to limit the number of DPP's submitted by an EO per day.
6. [9A.] An actor intercepts the information that is submitted on creation.
    - Possible mitigation: Use an encrypted and authenticated connection.

Events occurring during the Storage of the DPP and the product

7. [18A.] The DPP host is target of a cyber-attack which has the objective to steal the DPP information.
    - Possible mitigation: Take appropriate cybersecurity measures.

[34] Risks and mitigations: a companion to D4.1 Reference Architecture

- Possible mitigation: Some information is not included in the DPP but can be requested. Instead of the data, a proof is provided which can proof data that is given on request is bound to the DPP.

Events occurring during the retrieving the DPP

8. [26A.] An actor intercepts the DPP information.
    - Possible mitigation: Use an encrypted and authenticated connection.
9. [27A.] An actor intercepts and modifies the DPP information.
    - Possible mitigation: Use an encrypted and authenticated connection.
10. [28A.] An actor performs a Man-in-the-Middle attack, acting as both a DPP host and a DPP requester.
    - Possible mitigation: Use an encrypted and authenticated connection.

Events occurring during the updating of the DPP

11. [39A.] The DPP is updated by an actor that performed a successful cyber-attack on an actor that has the right to update the DPP.
    - Possible mitigation: Take appropriate cybersecurity measures.

APPENDIX A: ESPR REQUIREMENTS FOR DPP ARCHITECTURE

Requirement ID & Source	ESPR Requirement	Relevant for	Additional comments (if any)
ESPR.10	The DPP architecture **should** support changes in standards for Unique Operator Identifiers, Unique Facility Identifiers and Data Carriers.	DPP System	
ESPR.10.1.a.	DPPs **must** be connected through a data carrier to a persistent Unique Product Identifier (UPI).	DPPs	
ESPR.10.1.b.	Data Carrier **must** be physically present on product, it's packaging or on documentation.	DPPs	As a corollary, the data carrier must be representable on a physical product. To be further specified in the delegated acts.

ESPR.10.1.c.	Data Carrier and UPI **must** comply with standards listed in ESPR Annex III and, when released, harmonized standards.	DPPs	Standards of Annex 3 are ISO/IEC 15459-1:2014, ISO/IEC 15459-2:2015, ISO/IEC 15459-3:2014, ISO/IEC 15459-4:2014, ISO/IEC 15459-5:2014 and ISO/IEC 15459-6:2014
ESPR.10.1.e.	A DPP **won't** store customer personal data without their explicit consent.	DPP System	In general, all DPP architectures and associated systems must comply with the GDPR. The ESPR does not override the GDPR.

ESPR.10.1.f.	DPPs **must** be of appropriate granularity at the product, batch or item level.	DPP	Specific requirements to be specified in upcoming delegated acts.
ESPR.10.1.g.	DPPs **must** regulate access in alignment with access rights specified in the applicable delegated acts.	DPP System	To be specified in the delegated acts.
ESPR.10.1.Modifications	Data carriers and identifiers **should** be designed to be compatible with future changes in standards.	Data Carriers & Identifiers	The requirements for GTINs and the relevant standards for identifiers and data carriers may change.
ESPR.10.3.a.	DPPs **should** be made accessible via a digital copy of the data carrier or the UPI for online marketplaces.	Economic operator	

ESPR.11.a.	All DPPs **must be** interoperable with all other DPPs required by other delegated acts.	DPP System	This includes ensuring technical, semantic and organisational interoperability for end-to-end communication and data transfer.
ESPR.11.b.1.	DPPs **must** be accessible easily.	DPP System	
ESPR.11.b.2.	DPPs **must** be accessible free of charge.	DPP System	The DPP system and its components should therefore be cheap to maintain and create.
ESPR.11.b.3.	DPPs **must** regulate access in alignment with access rights specified in the applicable delegated acts.	DPP System	

ESPR.11.c.	DPPs **must** be stored by rEOs or DPPSPs.	rEO	
ESPR.11.Cert	The DPP architecture **may have to** allow for the issuance and/or verification of digital credentials.	DPP System	may have to' because while this is not a 'must' yet, it becomes a 'must' if set out in the delegated acts.
ESPR.11.d.	The DPP architecture **must** allow for DPPs to be linked.	DPP System	A new DPP for a product that already has a DPP must be able to be linked with the old DPP.
ESPR.11.e.	DPPs **must** remain available for specified durations, even in cases of insolvency, liquidation, or other cessation of activity of rEO.	DPPs	

ESPR.11.f.	DPPs **must** be modifiable or updateable only with appropriate access rights.	DPP System	To be specified in the delegated acts.
ESPR.11.g.1	The DPP architecture **must** ensure that the appropriate data can be authenticated.	DPP System	
ESPR.11.h.1.	DPPs **must** be designed to ensure high levels of security.	DPP System	
ESPR.11.h.2.	DPPs **must** be designed to ensure high levels of privacy.	DPP System	
ESPR.11.h.3.	DPPs **must** be designed to avoid fraud.	DPP System	
ESPR.12.1.	Data Carrier and UPI **must** comply with standards listed in ESPR Annex III and, when released, harmonized standards.	Data Carriers & Identifiers	Data carriers and identifiers should be designed to be compatible with future changes in standards.

ESPR.12.4.b	The DPP **must** allow EOs to create their own Unique Identifier and Data Carrier.	DPP System	
ESPR.12.5.c.1.	The Data carrier and Unique Identifier **must** be reliable.	Delegated Act	Specific requirements to be specified in upcoming delegated acts.
ESPR.12.5.c.2.	The Data carrier and Unique Identifier **must** be verifiable.	Delegated Act	Specific requirements to be specified in upcoming delegated acts.
ESPR.12.5.c.3.	The Data carrier and Unique Identifier **must** be unique globally.	Delegated Act	Specific requirements to be specified in upcoming delegated acts.
ESPR.12.5.d	Authorized parties **could** have the ability to create maintain update and withdraw UIs and Data carrier	Delegated Act	

ESPR.13.2.a.	The DPP architecture **must** allow for verification of the DPP through the DPP registry.	DPP System	Specific requirements to be specified in upcoming delegated acts.
ESPR.2.28.2	A DPP **must** be accessible through electronic means through a data carrier.	DPP System	
ESPR.27.1.c	The manufacturer **must** ensure that a backup copy of the most up-to-date version of the DPP is available with DPPSP.	Manufacturers	The DPP architecture could include some procedure to synchronize the back-up.
ESPR.29.2.c	The importer **must** ensure that a backup copy of the most up-to-date version of the DPP is available with DPPSP.	Importers	The DPP architecture could include some procedure to synchronize the back-up.

ESPR.9.2.b.	The DPP architecture **must** support at least one data carrier.	Delegated Act	There may be more than one data carriers to be used specified in the delegated legislation.
ESPR.9.2.f.	The DPP architecture **must** allow for Role-based Identity and Access Management.	Delegated Act	This includes allocation of creation, access, and update rights, which will follow from the delegated acts.
ESPR.9.2.g.	The DPP architecture **must** support introducing and updating data.	Delegated Act	This requires a specification of which 'actors' are to introduce data to or update data in the DPP, which is to be specified in the delegated acts.

ESPR.Anx3.b.	A DPP **must** contain an appropriately granular Unique Product Identifier.	DPPs	
ESPR.Anx3.IDs.	The Data Carrier, UPI, UOI, or UFI **must** comply with specified standards, if relevant.	Data Carriers & Identifiers	These standards may change in the future.

APPENDIX B: RECOMMENDATIONS BACKGROUND

For many of the architectural recommendations in chapter 3, additional arguments and information is provided in this chapter. This information is based on extensive discussions in the CIRPASS-2 consortium, with subject matter experts and industry representatives from the pilot projects.

PRESENTATION OF CREDENTIALS

Context

Controlling access to the data in a DPP is mandated in the ESPR (in articles 9, 10 and 11). This requires a system by which the party requesting access can provide credentials, which will determine the allowed access.

The DPP system must be accessible and usable for all parties involved in the circular economy. This specifically includes SME's, for which both technical knowledge and budgets may limit the possible solutions. The proposed architecture therefore consists of a model in which a simple and cheap solution is available, but more advanced solutions (providing more functionality) are supported where desired.

Different actors in the circular economy have different requirements regarding access to a DPP. These access rights concern both the data which is available to an actor and the permissions available. Some examples which have been discussed in the consortium meetings are:

- Details about the chemical composition of materials, being a commercial secret of the producer, is crucially important for recyclers and should not be available to other parties (particularly not to competitors of the producer);
- The right to modify a DPP should be granted to a limited set of parties, but this set could include some certified repairers with additional access rights.

In order to be able to provide the correct access rights a requester must provide the required credentials. Several methods have been considered for this exchange.

Proposed solution

Although this paragraph focuses on providing access to read the data in a DPP, the process and considerations are similar for modifying a DPP.

As JSON Web Tokens (JWT) are widely used and well supported, we propose to adopt this technique for the presentation of credentials. The proposed solution requires an organization which is making a DPP available (either the rEO or a service provider for the rEO) to check if the request contains a token and, if a token is present, provide access based on the type and contents of the token.

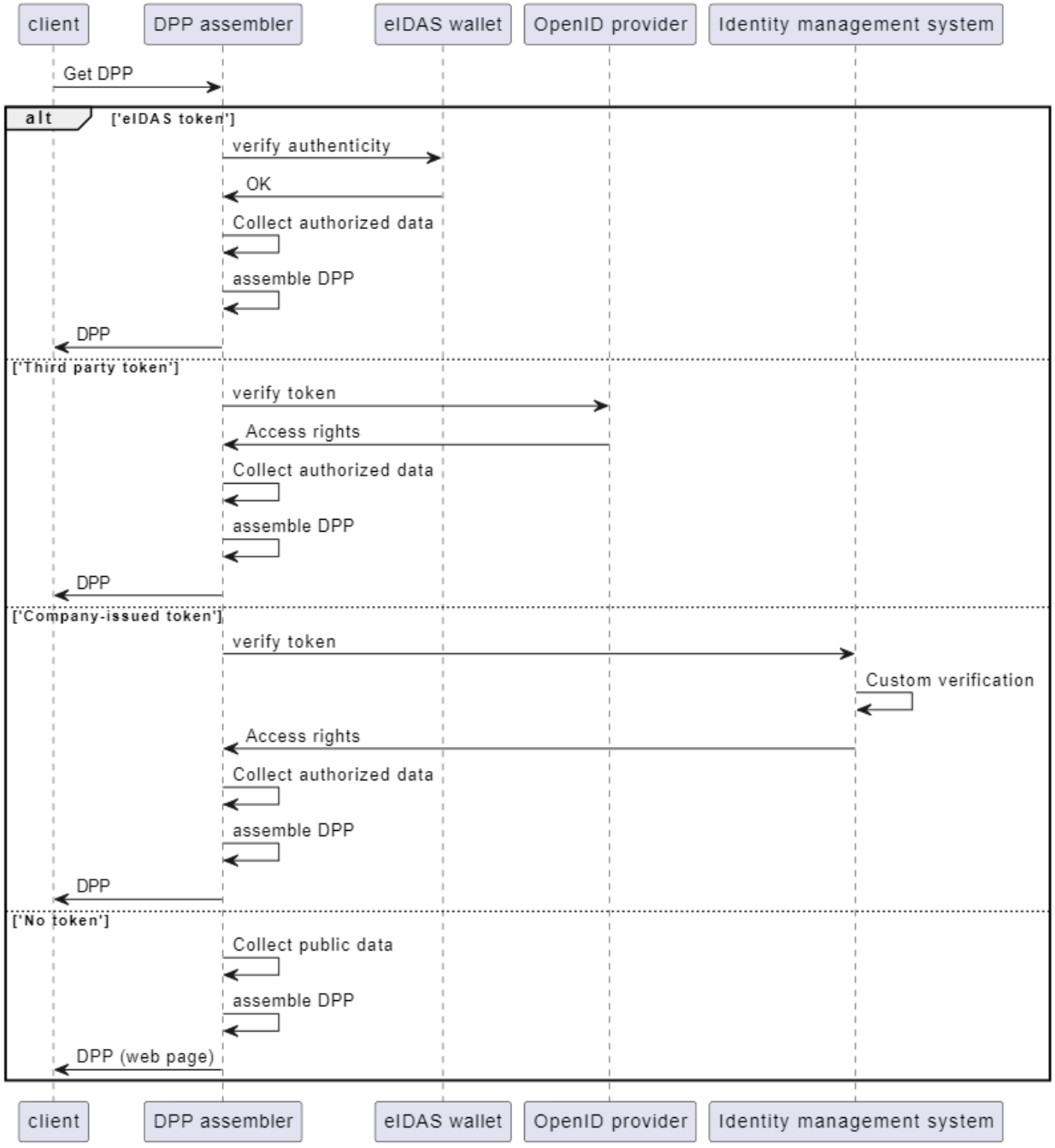


FIGURE 1818: CREDENTIALS PRESENTATION FLOW

Types of credentials

None

Since a DPP must be easily accessible it must be possible to request a DPP without credentials. An rEO may choose to:

- Provide all available data without any requirements for additional credentials, *if all data is public*;
- Provide a DPP containing all *public* data.

'Login with <cloud identity provider>'

Several large identity providers provide the option to use their system for identity management and (more or less limited) credential management. Commonly used providers for organizations are Google and Microsoft. Even if these systems are (configured to be) limited to proving the identity of a person (representing an organization), this could be sufficient as a minimal credential which allows the rEO to determine the authorized data, optionally by applying their own access control mechanism.

Organization-specific OpenId / OAuth2 provider

If an organization provides its own access control system based on OAuth2, they can issue credentials to organizations they cooperate with and use these for authorization purposes. Since such solutions do not need to be as generic as those provided by a cloud identity provider, allowing additional information such as roles to be added more easily. Using systems based on OAuth2 and OpenID, as well-known standards, ensures interoperability.

Verifiable credentials / verifiable presentations

Supplying 'verifiable credentials' in a JWT is being adopted by multiple initiatives. Both the eIDAS 2.0 Architecture reference framework and the Distributed Claims Protocol as used in the Eclipse Dataspace Components provide these. The use of verifiable credentials provides maximal guarantees about veracity and integrity of credentials, we therefore strongly prefer this option.

Criteria

Criteria which have been considered for the comparison of the exchange methods:

Easy to adopt

In order to keep the barrier for entry to the DPP system as low as possible, a credentials mechanism should be easy to adopt for companies of all sizes. .

Rich functionality

Many different types of credentials will exist in the wider DPP system. A system which supports the inclusion of multiple different credentials is preferable over a system with less possibilities.

Applicable across companies and member states

The DPP system is meant to be used widely. A system for credentials management which is specific for, or tied to, one company is not preferred.

Extensible

The identity of an organization is preferably confirmed by the EU or a member state. For specific sectors or even rEO's more specific credentials may be required. If a credentials management system can support these, this is an advantage.

Based on official standards

In order to make the DPP system as widely applicable as possible and as future-proof as possible, official and open standards are preferred over custom solutions.

Secure and trustworthy

Is the authenticity of the credentials verifiable? Using JWT provides the option for digitally signing credentials, making them verifiable without necessarily requiring a shared system (such as a central party or shared ledger).

	Ease of use	Functionality	Broad application	Extensible	Standards	Security
None	++	--	++	--	+-	--
Cloud login	++	+-	++	-	+	++
OIDC / OAuth2	+	+	++	+-	++	+
VCs	+	++	+-	++	++	++

ROLES AND PERMISSIONS

Context

Since controlling access to the data in a DPP is mandated in the ESPR (in articles 9, 10 and 11) and is of crucial importance to guard commercially sensitive information in a DPP, a well-defined system for access control is required.

Maintaining confidentiality of some data in a DPP is required, based on the access controls defined in the relevant delegated act (or possibly by a sector-specific organisation). It is to be expected that some types of data are mandatory and public, others exclusively for public authorities, according to a delegated act, so that it is likely that also trade secrets for the rEO's are included that will have to be shared with the authorities but not with competitors.

At the same time, access management cannot be used to limit access to DPP data to rEO's approved dealers or repairers, by commercial agreements.

This only seems feasible if a common set of roles is specified (possibly differentiated per product category / Delegated Act). Defining this set of roles would need to be organized at a European level.

A future delegated act may address the exact issue of roles and access control. This architecture document considers the subject from the point of view of the DPP system and provides a direction for the development of the system until such a delegated act may become available.

Access control in the DPP system

Different actors in the circular economy have different requirements regarding access to a DPP. These access rights concern both the data which is available to an actor and the permissions available. Some examples which have been discussed in the consortium meetings are:

- A subset, possibly aggregated, of data about the chemical composition of materials, which is a commercial secret of the producer, is crucially important for recyclers and must be made available to them but not to other parties (particularly competitors of the producer);
- The right to modify DPP data (instead of *appending* data without modifying the original data) is granted to the rEO, but *could* be granted to a limited set of certified repairers, thereby necessitating a robust access control mechanism[35].

Several requirements for access control have been considered:

Criteria

Sufficient for compliance

Delegated acts for specific product categories may prescribe certain access controls for the DPPs in the act. The access control mechanism of the DPP system should support these requirements.

Assigned by the rEO

Although a delegated act for a product category may specify access controls, it is expected that the rEO's, either individually or based on sector-specific agreements, add voluntary data to a DPP to support additional uses of the DPP. This voluntary data may be of a nature which requires limiting access to it. An rEO should therefore be able to assign access rights to specific data points in a DPP as long the legal requirements remain met.

Generic across countries and products

Conformity across the EU is necessary, in order to prevent the emergence of incompatible DPP systems between countries. Additionally, as products are interrelated along supply/value networks, interoperability across all product categories is a necessity and guarantees trust regardless of the EU country of the stakeholder requesting access. The requirement for interoperability in the ESPR would require the development of interoperability mechanisms, by designing for a interoperable solution from the start we avoid this additional effort.

Exchangeable across organizations

Since the availability of a backup for DPPs is mandatory, the service providers hosting such a backup must be able to manage access to the data in a backup just as the original rEO does for the DPP, at least for the mandatory DPP data. The combination of requirements for access controls for a DPP and for the existence of a backup requires that managing access restrictions for a specific DPP must be transferable to another company (at least after the rEO goes out of business

[35] Modifying the data in a DPP is undesirable, as it creates many opportunities for fraud. We strongly recommend to not allow this, and to require both the original DPP and every update (stored as a separate appendix to the DPP) to be signed by the relevant organization

since the backup copy can be assumed to be synced, including the access rights, as long as the rEO is operational).

This requirement leaves some room for discussion, as all legally mandated access controls must be transferable, but there is no legal guidance regarding access restrictions for voluntary data added by an rEO.

Flexible across use cases

An actor may have different roles in different situations. If, for instance, a role 'repairer' is defined, an organization may be proficient at repair in one product category but not at all in another product category. Furthermore, accreditation for a certain role can be limited to a specific period of time, after which recertification is required. Of course an actor may perform multiple roles, requiring the possibility for the presentations of multiple credentials for roles.

Risk of illegal competition

The risks for business discrimination, unfair competition and monopolistic behaviour should be minimized.

Time-limited

An organization may not perform a role indefinitely, for multiple product types a time-limited certification may be required in order to be recognized as qualified for a role. A role could therefore have a limited validity and a verification mechanism for the continuing validity of the role assignment should exist.

Easy to implement

Keeping the DPP system accessible to all organizations, including SME's, requires the solution to be based on commonly used techniques. Although advanced methods for access control are being developed, adopting these will create a barrier for entry for smaller parties.

Extensible

If an rEO wishes to add specific additional access rights to a DPP (i.e. not conflicting with the legal requirements) this should be possible. All mandatory access rights must be maintained, but adding specific categories of parties with additional rights (e.g. 'my preferred suppliers' or 'repairers certified by me') must be possible. Whether these extended access controls are transferable to other companies, such as backup providers, is out of scope of this document and could be a contractual agreement between organizations.

Tool support

Related to the requirement for easy implementation, access control should be based on well-supported mechanisms. Using these mechanisms allows quick and easy implementation by organizations.

Assigning access rights types

Based on the requirements above, it is clear that a mechanism to assign access rights to specific parties is required. Some options have been considered:

- Individual parties: An rEO determines, based on proprietary criteria, which parties have certain access rights;

- rEO-specific roles: An rEO defines roles and their access rights, and assigns roles to parties based on proprietary criteria;
- EU-defined roles: The EU defines, or delegates the definition, of roles for parties, rEO's grant access rights to roles;
- Extensible EU-defined roles: The EU defines generic roles, individual countries, sectors, industries or even rEO's can base specific roles on these generic roles to allow fine-grained distinctions.

Analyzing the fit to the requirements for these options provides the following table ('Easy to implement' and 'Time-limited' are not differentiating factors for these options, but are relevant for the technical implementation):

	Compliance	Assignment	Generic	Exchangeable	Flexible	Risky	Easy	Extensible
Individual parties	--	++	--	--	+	++	+-	+-
rEO-specific roles	-	++	-	-	+	++	+-	++
EU-defined roles	++	++	++	++	+	+-	+-	-
Extensible EU-defined roles	++	++	++	++	++	-	+-	++

Based on the table above, 'extensible EU-defined roles' is proposed as the mechanism for defining roles. Although a risk that needs to be considered is that this might hinder interoperability, e.g. specific roles that disproportionately favor specific parties.

UPDATES AND AUTHENTICITY

Context

Controlling access to the data in a DPP is mandated in the ESPR (in articles 9, 10 and 11). Access control is particularly important for updates to a DPP, as article 9.1 states that "The data in the digital product passport shall be accurate, complete and up to date". Depending on the Delegated Acts, the economic operator putting a product on the market may be responsible for providing accurate data during the lifetime of the project, in which case updates must be tightly controlled. As we expect that lifetime accuracy of DPP's will become the norm as the economy becomes more circular, the DPP system must be prepared to support this control mechanism.

Based on the articles mentioned above a clarification of 'update to a DPP' is required. Allowing changes to the data in the original DPP provides many opportunities for fraud. A DPP must

therefore be immutable: once it has been created, no updates may be performed. Any changes to the product must be provided as *additions* to the DPP, by considering the original DPP and all additions an "accurate, complete and up to date" DPP can be (re)created. Keeping the DPP system as open and accessible as possible is an explicit goal of the architecture, based on the requirements in the ESPR. Accessibility facilitates a dynamic and innovative ecosystem of organizations surrounding DPP's. While openness and accessibility reduce undesired control of markets and data by specific parties, they can also create possibilities for abuse. To maximize opportunities without introducing excessive risks for rEO's and consumers, a careful balance must be struck between openness / accessibility and access control. This is particularly relevant when considering updates to DPP's.

In the relevant regulations the role of 'independent operators' is clearly mentioned. An open and innovative marketplace must allow room for independent companies providing support, repairs and modifications for products, all of which may result in updates to the DPP of a product. This implies that the right to update a DPP cannot be limited to the rEO.

Two aspects of updates must be considered: where is the data stored and how a consumer can assess the reliability of the available data.

Data storage

The rEO stores all DPP data

As the rEO is responsible for making a DPP available for a product, it is very convenient if the rEO additionally stores all updated data. This reduces dependencies between parties, some of which may have a limited lifetime, and makes both access and backups very simple.

Disadvantages of this solution are that an rEO is responsible for the storage and backup of data without being able to predict the size and number of updates, for the expected lifetime of a product. This will result in additional costs for the rEO and may provide risks for security and availability.

DPP data is completely decentralized

Leaving all data regarding updates or modifications of a product in the IT system of the repairer facilitates a decentralized system. If there is no requirement for the economic operator to be aware of the additional data, the burden for the rEO is minimized. The complexity of the DPP system as a whole is increased sharply, since a mechanism to find all updates related to a specific product must be introduced, while the reliability of data in a DPP is reduced and possibilities for abuse are far greater.

The rEO provides access to updates

Allowing repairers and other parties providing updates to a DPP to store data wherever convenient, including at the rEO, and requiring them to provide a digitally signed set of the updated data and the storage location of the data to the rEO mitigates most disadvantages from the other storage solutions. The rEO can now either use the link to the storage location to provide access to the updated data, or store a copy of the data.

This option does introduce a risk for economic operators, as they must provide access to their IT systems to *everyone*.

Veracity of updates

The responsible EO is fully responsible

As the EO is responsible for providing the DPP, leaving full control of all DPP data with the EO allows the EO to fulfil this responsibility. A large disadvantage of leaving full control of all DPP data to the EO is that this effectively creates a monopoly regarding the DPP for a product. Although independent parties can no longer abuse or manipulate the system, a monopoly creates possibilities for abuse by the EO.

The supplier of the update is responsible

If independent organizations can update the data in a DPP without any influence from the responsible EO, this presents a challenge for the EO. As the EO is responsible for providing the DPP, but they no longer have control over the contents, they cannot reliably bear this responsibility. The possibilities for abuse are very great, with bad actors being able to commit fraud, influence the market for a product or product category, and even extort EO's by threatening the integrity of their DPP's.

Responsible EO is responsible for access and provides meta data

Limiting access to certain roles prohibits end users from updating information, and allows for a measure of control avoiding the most easy abuse

If the EO can provide metadata for each update, this allows a judgement of the veracity and reliability of the update. One can think about a 'reliability' score for each update, in which official (brand) certification or the method of supplying repair data (from a professional computer system or hand-written) may be considered indications.

Requiring all updates to be electronically signed and thereby verifiably linked to a specific party reduces the possibilities for abuse and allows bad actors to be identified. Some possibilities for abuse still exist, both by the rEO and by the independent operators providing updates.

Party	Abuse	Mitigation explanation	Mitigating measure
IO	Provide an update with incorrect information	The IO can provide an incorrect update, but cannot deny having done so[36]	Electronic signing
IO	Provide an update to the DPP without updating the product*	The IO can provide an update without updating the product, but cannot deny having done so*	Electronic signing
IO	Claim to have sent an update to the rEO without having sent an update to the rEO	(no mitigation)	-
IO	Update the physical product but not the DPP	(no mitigation)	-

[36] This is only possible if the rEO permanently stores the update (including its signature)

rEO	Deny having received an update	(no mitigation)	-
rEO	Display incorrect information about the update to the DPP requester	(no mitigation)	-
rEO	Display a fake, never supplied update to the DPP requester	(no mitigation)	-
rEO	Claim to have received information in an update that has not actually been provided	The rEO cannot provide a valid signature corresponding to the update	Electronic signing
rEO	Claim to have received an update that has not actually been provided	The rEO cannot provide a valid signature corresponding to the update	Electronic signing

Criteria

Difficulty of abuse

This criterium may need to be split up to distinguish abuse by the rEO and abuse by independent operators.

The scale of this criterium is based on the number of parties required to cooperate in order to abuse the system: if a single party can provide undetectable fraudulent data, this is a low score, if more parties are required the score increases

Technical complexity

Requiring more technical know-how lowers the score for this criterium. Digitally signing an update is more complex than providing plain data. The complexity of the system as a whole is also considered for this criterium: a fully decentralized system without an easy way to link data requires additional components like search engines and portals, increasing the complexity and causing a lower score.

Decentralization

Since the DPP system must be a decentralized system, more centralization results in a lower score.

	Difficulty of abuse	Technical complexity	Decentralization	

EO stores all data	--	+	--	
Completely decentralized	--	-	++	
EO provides access	+-	+-	-	
EO responsible	--	-	NA	
Updater responsible	--	-	NA	
EO provides metadata	+-	+	NA	

Based on the table above we recommend that the rEO stores all updates and (optionally) provides metadata about the provenance and trustworthiness of each update. This decreases the decentralized aspect of the DPP system, but provides more complete and trustworthy DPPs.

EXCHANGE FORMAT

Context

Since the DPP system is concerned with digital product passports, the exchange format for these is an important factor. The implication of recommending an exchange format is that it is a requirement for all CIRPASS2 pilots to make the mandatory DPP data available, at least, in the chosen format. The reason for this is that agreement on a format in which the data is exchanged benefits semantic interoperability.

Exchanging digital product passports

There are several standardized exchange formats suitable as format for a DPP. Based on the user stories, the derived requirements and inputs from the CIRPASS project and several stakeholders are used for an analysis to justify a suitable choice.

A guiding principle for the architecture of the DPP system is that the barrier for entry should be as low as possible. The introduction of the DPP will have a large impact on businesses, the vast majority of which are SME's. Formats increasing the barriers for entry to the system are therefore not preferred.

Criteria

The following requirements have been considered for this choice. All requirements are considered to be important, but we deem 'adoptability' to be essential for the success of the DPP system.

We note that it is still possible for proprietary DPP software systems to use other formats internally, but for the common DPPs a communal format representation is advised, that would be served e.g. via an export converter, at discretion by the DPP solution provider.

Maximal (semantic) interoperability

The DPP system operates across sectors and industries. The regulations clearly state that DPP's must be interoperable across these different domains. Interoperability concerns several levels (see the EU Interoperability framework). Technical interoperability is not very hard to achieve, but semantic interoperability, in which the meaning of the data being exchanged is preserved, is harder. This concern is a clear driver for an exchange format which specifies not just technical aspects but also semantics.

Ubiquity of the format

Selecting a commonly used and easily adopted format will help all companies in the adoption of the DPP without excessive costs. Even for SME's which delegate (part of) their responsibilities to service providers, using commonly used techniques will be advantageous.

A commonly used format provides access to many different IT suppliers, making it easy to fit existing systems in the DPP system. Furthermore, it will ensure a broad presence of developing competencies/skills on the market, which in turn will reduce costs, ensure a large presence of suppliers, lower the risk of errors and ensure a sustainable development path (the maintenance of the format is ensured over the time).

Compatibility

This aspect is concerned with the ease with which the format can be transformed into other formats. The easier it is to convert a DPP from the recommended format to other formats, while maintaining as much technical and semantical information as possible, the easier the format can be integrated with the existing systems in organizations.

Extensibility

Legal requirements for DPPs are specified in delegated acts and are not expected to change rapidly and often. If the DPP system is as successful as expected, new and unforeseen uses for DPP's will quickly evolve in the market, and some of these will require extending the legally specified parts of the DPP with voluntary data to enable new services and business models. The exchange format for a DPP should therefore be easily extendable with voluntary data without compromising the compliance to legal requirements.

Tool support

Formats which are very well supported by tools used by companies and developers are easier to implement, giving them a large advantage over other formats. This impacts the initial development, monitoring of systems, and analytics.

	Semantics	Ubiquity	Compatibility	Extensibility	Tool support
JSON	-	++	+	++	++
RDF / Turtle	++	-	+-	++	-
JSON-LD	++	+-	++	++	+

XML	+-	+	+	+	++
Custom format	+	-	-	+	+

Based on the table above, the JSON-LD exchange format is recommended. Given the importance of semantic interoperability in the DPP system this format has a slight edge over JSON.

JSON-LD allows for complete serialization of RDF graphs, which means that it inherits all of RDF's semantic robustness. It also inherits all of JSON's tooling support, since it uses regular JSON syntax – though special tooling is of course required when trying to use its linked data or RDF features. Most importantly, the barrier of entry with using JSON-LD is quite low, since at its most basic form a JSON-LD message is nothing more than a JSON message with a handful of additional fields connecting it to the world of linked data.