THE SIMPLEST DPP SYSTEM PROPOSAL – A THOUGHT EXPERIMENT

Publication date	April 2025
Version	1
Contributors	Tanel Tammet (Taltech), Carolynn Bernier (CEA), Huib van Nieuwenhuijze (TNO), Rain Eisler (Taltech), Nikolaos Saklampanakis (Fujitsu)
Abstract	This document presents a proposal for the simplest and lowest cost implementation of the EU DPP System, based only on well-established web technologies and services.
Citation	Tammet, T., Bernier, C., van Nieuwenhuijze, H., Eisler, R., & Saklampanakis, N. (2025). The simplest DPP System Proposal – A thought experiment. CIRPASS-2 Consortium. https://doi.org/10.5281/zenodo.15367063

Document Revision History

Version	Date	Description of change	List of contributor(s)
1.0	May 12, 2025	Final V1	

CIRPASS-2 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	Sweden
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	Hisense Gorenje Europe Poslovne Storitve DOO	HGE	Slovenia
37	Manufacture Francaise Des Pneumatiques MICHELIN	MICHELIN	France
38	COBUILDER AS	COBUILDER	Norway
39	DIN Deutsches Institut Fuer Normung EV	DIN e.V.	Germany
40	VDE Verband Der Elektrotechnik Elektronik Informationstechnik EV	VDE	Germany
41	Energy Web AG	Energy Web AG	Switzerland
42	WORLDLINE France	WORLDLINE FR	France
43	Physikalisch-Technische Bundesanstalt	PTB	Germany
44	Digital Data Chain Consortium GbR	DDCC	Germany
45	ZVEI e. V.	ZVEI e.V.	Germany
46	Association of Service and Computer Dealers International	ASCDI	US
47	Open Blockchain for Asset Disposition Alliance (OBADA)	OBADA	US
48	Green Electronics Council	GEC	US
49	Textile Exchange	TextileExchange	US
50	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

COPYRIGHT NOTICE

ABBREVIATIONS

CPR	Construction Products Regulation
DPP	Digital Product Passport
DPPSP	Digital Product Passport Service Provider
EC	European Commission
ESPR	Eco-design for Sustainable Product Regulation
IAA	Identification, Authentication, Authorization
ID	Identifier
MSA	Market Surveillance Authorities
REO	Responsible Economic Operator
SME	Small-Medium Enterprise
UPI	Unique Product Identifier

DISCLAIMER

The information provided in this presentation is for information purposes only. The CIRPASS-2 consortium partners are not responsible for any damage that could result from making use of this information.

Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union, European Commission, or the European Health and Digital Executive Agency (HADEA). Neither the European Union, the European Commission nor the granting authority can be held responsible for them. Views and opinions expressed are those of the author(s) only and should not be interpreted as reflecting those of CEN/CENELEC JTC 24.

1 OBJECTIVE OF THIS DOCUMENT

The purpose of this document is to stimulate discussion on a "basic" DPP system that has been stripped down to its most fundamental elements and that is:

- easily applicable to extremely **low-cost** products with mandatory 'simplest DPP' requirements
- and focuses on **short-term** DPP deployments for fast adoption of DPPs by industry.

Our objective in presenting this "no frills" proposal for the European DPP system architecture is also to:

- outline the core elements of the DPP architecture in an easily readable short paper,
- facilitate understanding and discussion about the fundamental workings of the EU DPP system,
- support the incremental roll-out of higher-complexity DPP system features, as technology matures and needs arise.

Furthermore, a simple-to-complex incremental roll-out for the DPP system will facilitate successful uptake by industry of the DPP and increase the probability that the European Union will reach its sustainability and circularity goals thanks to the DPP.

Disclaimer: The proposal made in this report may not be applicable to more complex products.

1.1 LIMITING THE COST OF DPP IMPLEMENTATION

This document proposes a design for the EU DPP system based on existing web technologies and web services already well known and used by businesses (responsible economic operators (REOs) and other system stakeholders).

The simplicity of the system ensures its feasibility.

The cost of efforts required to gather the DPP data, before DPP creation, is out of scope of this report.

1.2 LEVERAGING COST VERSUS PERFORMANCE

Because the European DPP system is meant to be highly flexible and future-proof, it should be designed to allow many advanced features and exploit advanced digital technologies, many of which do not exist today. However, because the EU DPP will apply to a wide range of product groups, it is to be expected, and it is highly desirable, that different DPP implementation options will be chosen for different product sectors, all the while ensuring that all implementations remain compliant to the upcoming standards for the DPP system currently under development by CEN/CENELEC JTC-24 .

Because simple, low-cost products (e.g. a rubber ducky) require extremely low-cost DPP implementations, differently from more complex, high-value assets (e.g. a vehicle) which may require more advanced DPP implementations options, in this report we develop a 'bare bones' presentation of the DPP system targeting low-cost products.

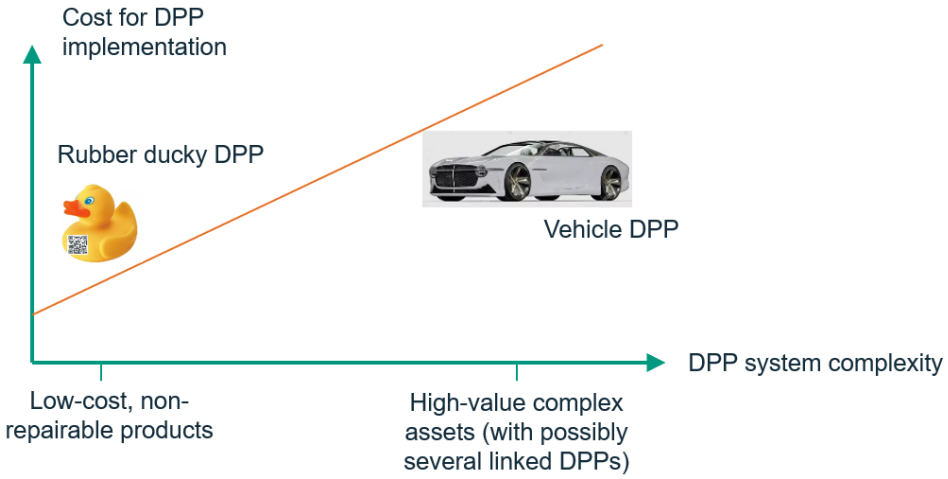

FIGURE 1: DPP SYSTEM IMPLEMENTATION COST/COMPLEXITY TRADE-OFF – FROM LOW-COST PRODUCTS TO HIGH-VALUE ASSETS

1.3 HYPOTHESES FOR THE SIMPLEST DPP IMPLEMENTATION

We assume that the "simplest DPP" has the following features:

- The "simplest DPP" may contain any kind of non-mandatory data in addition to the mandatory data.
- The "simplest DPP" may contain data that is modified or added during the product lifecycle (both mandatory and non-mandatory).
- The "simplest DPP" may contain commercially sensitive data (both mandatory and non-mandatory) requiring either role-based (as defined in ESPR) or identity-based access control.

While many digital technologies exist to provide the advanced functionalities mentioned below, we assume that the "simplest DPP" will not require the following:

- There is no data source authentication. This means that there are no cryptographic mechanisms to validate that the data has been provided by the said data provider, i.e. the economic operator responsible (REO) for DPP creation.
- There is no data integrity check for the 'live' DPP. This means that there is no way to check that the data in the live DPP has not been changed other than by consulting timestamped backups.
- There is no data carrier authentication mechanism.
- The data carrier does not contain control data elements enabling the verification of the authenticity of the data carrier itself nor of the product.
- There are no linked cryptographically verifiable claims to improve trust in specific product claims (e.g. certifications), except using standard Web technology (e.g. HTTPS protocol).
- There is no DPP data timestamping (i.e. no DPP version retrieval) except using timestamped backups.
- There are no identifier authentication mechanisms.

In accordance with the requirements from the Standardisation Request Annex 2, Part A, section 2.1 which states "(j) data authentication, reliability and integrity shall be ensured;", the proposal outlined below ensures:

-**data authentication** through the authentication of economic operators when registering their DPPs in the EU Registry;

-**reliability** through mandatory requirements for DPP hosting infrastructure;

-**integrity** using time-stamped backups.

1.4 ASSUMPTIONS CONCERNING THE UNIQUE PRODUCT IDENTIFIER

Actual supported standards for unique product identifiers for the EU DPP will be defined by standardisation. This report does not attempt to give recommendations for the form of product identifiers. Requirements for product identifiers have already been discussed at length in a previous report[1] which introduced the assumption that "interoperability relies on product Identifiers that must either be in the form of a web URI or have a formal, specified and known transform into a web URI." In this document, we assume that the web URI is a web URL.

Conceptually, a product identifier may be either unique for every separate item, batch or model[2]. The behaviour of the DPP system architecture described below does not assume that the form of the product identifier indicates whether it stands for a unique item, a batch of products or a product model. This is a matter of the DPP unique product identifier (UPI) encoding and/or subsidiary architecture.

1.5 ASSUMPTIONS CONCERNING THE DPP WEB DOCUMENT

We assume that the DPP is a JSON web document that may be embedded in an HTML document (Figure 2).

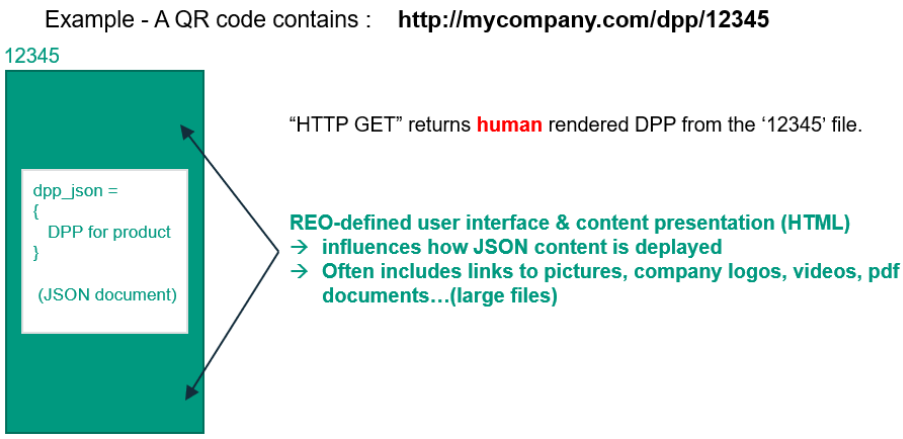

FIGURE 2: THE DPP WEB DOCUMENT EMBEDDED INTO AN HTML FILE.

1.5.1 RETRIEVAL OF HUMAN-RENDERED DPP

[1] Archer, P., Poggiali, F., & Olsson, S. (2024). Identification Schemes (1.3). CIRPASS Consortium. https://doi.org/10.5281/zenodo.15274537

[2] Annex 2 Part B. section 1.4 of the Standardisation Request states: "The unique product identifier shall always allow the possibility to include the three different granularity levels, i.e. model, batch, or item."

If, for example, a QR code contains the following URL http://mycompany.com/dpp/12345, an HTTP GET request to this URL performed by a Web browser would retrieve the HTML file 12345. This HTML file includes encoded instructions for DPP content presentation (e.g. Web browsers on mobile devices require specific presentations) and will likely include links to pictures, company logos, videos, pdf documents, etc. which, because they represent large amounts of data, should be limited in the mandatory DPP information requirements. A specific variable ('dpp_json' in the example) is used to identify the DPP Web document in the HTML document.

We assume that human-rendering of the mandatory DPP backup (the JSON Web document without its HTML wrapper) will be performed by the EU Web Portal.

1.5.2 RETRIEVAL OF THE DPP BY MACHINES

The following options are possible.

Option 1: The application makes an HTTP GET request to (e.g.) http://mycompany.com/dpp/12345?format=json.
This retrieves the 12345.json document directly or the html file rewrites itself (e.g. using techniques like rerouting by the web server, some Javascript code, etc) to provide the the json format directly. Optionally, rather than the "?" query parameter, the request could be made using an HTTP header (like the 'Accept' HTTP header)[3].

Option 2: The application makes an HTTP GET request to http://mycompany.com/dpp/12345. The JSON Web document DPP is extracted from the HTML file by the requesting application, using the (e.g.) dpp_json variable.

2 COMPONENTS OF THE BASIC DPP SYSTEM ARCHITECTURE

The basic architecture contains four systems, several of which may have several independent implementations:

- EU Registry for accepting and storing the live and backup URLs for each unique product identifier (in addition to the other information required by ESPR Article 13).
- Decentralized DPP data repositories for hosting DPP data by REOs or their appointed DPP service provider. The actual storage of DPP-related web documents is not considered a part of the basic architecture. Each publisher of DPP data can and should use their own preferred way to publish these web documents: either in their own servers or using cloud services or any other third-party web hosting companies.
- Decentralized DPP backups for backing up the DPP web documents.
- EU Web Portal for searching and presenting DPP information from the beforementioned systems.

The EU registry and the EU Web portal have an official, guaranteed and supported EU implementation. The two related systems, repositories and backups, have a possibly unlimited number of third-party implementations, optionally providing additional services.

The proposed EU DPP system as a whole can be integrated into a world-wide system of different DPP formats and architectures via connecting different DPP systems with the proposed DPP repositories,

[3] This approach allows the recipient to request other presentations, such as application/vc+jwt, if these become available in the future.

backups and other parts of the infrastructure allowing foreign DPP systems to easily access data from the EU DPP system. Inevitably, the connectors have to translate between different DPP data encodings.

2.1 EU REGISTRY

For each unique product identifier, the EU Registry accepts and stores the live and backup URLs which link to the relevant DPP web document (in addition to the other information required by ESPR Article 13). The EU registry is fundamentally a key-value database. Each product identifier will have exactly one corresponding entry in the database.

The information in the EU Registry is not publicly available. It can only be accessed by other EU-controlled systems (e.g. the EU Web Portal).

The organisation creating a DPP and associating it with a product identifier must submit this information to the EU Registry. The EU Registry accepts information only from previously registered, known organisations.

Assuming token-based authentication, each such organisation will be assigned a unique token for authentication. The EU DPP registry will maintain the database of registered organisations and their tokens.

Registering a DPP in the EU Registry might be performed either by:

- Using an API URL like https://eudppregistry.eu/submit?id=XXXX&url=YYYY&token=ZZZZ[4]
- Using a web page with corresponding three fields and a submit button.

An organisation which has registered a DPP in the EU Registry can later submit different information for the same unique product identifier, but receives distinct unique registration identifiers (as defined in ESPR Article 13) for each submission. This allows organisations to modify the active and backup web links if necessary.

The EU Registry should enable the registration of organizations allowed to register DPPs on behalf of other organisations and also the transferring of rights to re-submit information concerning pre-registered products. For this reason, it is necessary to keep the information about the organization making the registration and the economic operator legally responsible for placing the product on the market.

Thus the information stored in the EU should possibly also include these organisations identifiers and the submission data and time.

2.2 DPP DATA STORAGE (DECENTRALIZED DPP DATA REPOSITORIES)

We assume that the DPP is a JSON or XML web document that may be embedded in an HTML document accessed using standard web protocols (http or https). Information defined as publicly accessible should not require the reader to authenticate.

A DPP web document must be static in the sense that it contains all the information necessary for backup in case the original web server no longer functions. However, the content of the DPP web document can be

[4] This could be implemented as a REST API. By providing an 'HTTP POST' endpoint both the token and the DPP data can be put in the request body for confidentiality. The unique registration ID can be part of the response to the economic operator. A POST request is a very commonly used HTTP method, limiting complexity for implementers.

changed anytime to enable the presence of dynamic information in the DPP. Checks of changes to DPP data must be done by consulting timestamped backups. Note that 'static' should be interpreted as 'conceptually static', as many implementations will generate the live DPP web document on the fly. For example, because item-level DPPs contain almost identical data for each item, these DPPs can be composed and produced in real-time with a program using a database, as is commonly done in Web tech. This means that there is no need to store pre-built DPP data files on the servers publishing the live DPP.

In case additional parameters such as specialized visualization requests https://mycompany.com/products/13437?usage=materials are implemented, the implementation has to be done on the client-side using Javascript, and not as a server-side implementation, otherwise the adequate backing up of a DPP web document becomes impossible.

A DPP web document may contain, in addition to the public mandatory information requirements, additional information such as:

- Additional non-mandatory information, such as certifications and links to repair videos etc.
- Non-public sensitive information (both mandatory and non-mandatory) available only to selected/restricted third parties.

Considering these kinds of information we propose the following way to encode them:

- **Non-mandatory data**. Presented either in the HTML page in which the web document containing the mandatory DPP data is embedded, or as additional data fields in the DPP web document or as pages pointed to by URLs also included in the DPP web document.
- **Non-public (restricted) commercially sensitive information.** Whether this information is mandatory or not, an extremely simple implementation to enable this consists in presenting this information only as separate web documents pointed to by URLs in the DPP encoding. The access to these separate documents is regulated and implemented by the publisher of this information. Several (short-term) options are possible for the setting of access restrictions by the publisher of this information. These options should be considered « short-term » solutions and do not consider more advanced options that will become available once the eIDAS 2.0 Regulation becomes widely implemented along with means for assigning role-based verifiable credentials by trusted authorities. The European Commission should provide clear guidelines on the interim solution and ensure that a grace period is defined in which both systems are compliant and acceptable, to ensure that migration can take place without disrupting businesses, especially SMEs.
    - Option 1: Each organization hosting sensitive information delivers static API keys individually to all stakeholders who have a right to access the sensitive information.
    - Option 2: Each organization hosting sensitive information provides JWT tokens individually to all stakeholders who have a right to access the sensitive information. This option lowers the risk of token capture and impersonation with respect to option 1, if these tokens have limited life span and can be refreshed.
    - Option 3: To facilitate access by public officials to mandatory sensitive data, a specific IP address is reserved for permissioned access. Private sector stakeholders must still use the previous options.
    - Option 4: To facilitate access by public officials to mandatory sensitive data, TLS certificates are exchanged to implement mutual TLS. Private sector stakeholders must still use the previous options. This approach lowers the risk of IP spoofing (option 3).
    - Option 5: To facilitate access to mandatory sensitive data to any stakeholder with legitimate interest (including public officials), the EC operates an identity provider delivering access tokens.

2.3 DECENTRALISED DPP BACKUPS

A DPP backup is a system that regularly stores the DPP web document. For example, every day/week/month, and stores the changes (differences) of the DPP. This way it is be possible to see whether/when/how the published DPP has been changed since the moment of registration in the EU Registry.

The DPP backup systems are used by the EU Web Portal to obtain information for product identifiers for which the original DPP URL is no longer accessible.

Furthermore, to enable "archiving" (defined by the Standardisation Request as the ability for authorities to investigate historical data of a DPP), DPP backups must also store timestamped hashes of mandatory DPP web documents, for the cases when the mandatory content of the DPP web document is modified and there is interest by public authorities to see the contents of the older versions. This means that the verification by public authorities of a given DPP's validity (irrespective of the validity of the DPP's information content itself, i.e. regarding the truth or falseness of the provided information) would imply the following, easily automatable, steps: 1 - retrieving the latest version of the mandatory DPP document from the backup, 2 - retrieving the mandatory content of the live DPP, 3 - running automatic validation checks on both versions.

A DPP backup system may be tasked to store only the DPP mandatory data, the structured parts of the non-mandatory data, the whole DPP HTML page with possible unstructured non-mandatory data, or possibly also the publicly available optional data on separate web pages (for example, user manual pdfs) pointed to from the DPP via URLs. A backup system storing sensitive mandatory data will have to apply the same access control mechanisms as the live DPP storage to enable access to restricted information on web pages requiring authentication.

2.4 EU WEB PORTAL

The EU Web Portal[5] is used for searching and displaying model-level information associated with the product identifier or URL. In particular, if the URL of the live DPP does not respond, the Web Portal can retrieve the data from the mandatory backup (thanks to the link to the backup retrieved from the EU Registry). This portal is publicly available and can be used both by human users with various interests or by fully automated systems of various kinds. A user will either:

- Open a portal URL like https://eudppportal.eu?uid=XXXX&format=JSON. Alternatively, an HTTP Accept header could be used to define the desired format.
- Open a portal web page, with a search engine-like search field for the unique product identifier or URL and a "search" button.

The portal formats information found according to the value of the "usage" field: the result could be raw JSON, a human-readable web page, etc. It is assumed that the EU Web Portal will be able to provide human rendered displays of backed-up DPP web documents that do not have HTML wrappers.

The default URL, without a 'format=' parameter should display the human-readable DPP.

[5] An extensive discussion of the requirements and implementation options for the EU Web Portal is provided in CIRPASS-2 Consortium. (2025). Options for EU Web Portal Search (DPP System). https://doi.org/10.5281/zenodo.14975070

3 SUBSIDIARY COMPONENTS

3.1 ASSOCIATED INFORMATION REGISTRIES

There are two types of associated information registries:

The first type is needed to find the DPP URLs for product IDs which are not URLs themselves. Such a service is necessary when a data carrier cannot store a URL (e.g. an RFID chip). These types of services will likely be proposed by certain industry associations and will be known in the partner industrial ecosystem.

The second type is needed to store optional links to additional non-mandatory information about a product from third parties. Such a registry accepts “product identifier” or “DPP URL” and “additional information web URL” pairs typically added by third parties, such as consumer protection organisations. Such registries will be found using standard web indexing technology. Publishing these additional web documents is the responsibility of the submitter of the information to the associated information registry.

The information pointed to by these optional links is also stored as web documents, which may potentially carry structured JSON, human-readable html, images, pdf or any other kind of information. The web documents with associated information may be either publicly available or restricted by their publisher (for example, requiring authentication).

Some of the DPP associated information registries may use a policy of pre-registering organisations with a right to submit and provide an associated token. Some may prefer to allow unregistered organisations to submit as well.

The associated information registries might be used by associated portals to search for additional information for a given product identifier.

3.2 PRODUCING AND PUBLISHING A DPP: A VIEW FROM A COMPANY

In practice, a highly critical question is how companies actually produce a DPP, associate it with a product and notify the EU registry. By a “*company*” we mean the organization placing the product on the EU market, i.e. the Responsible Economic Operator (REO), who has to form and publish a DPP.

From the company viewpoint, all of this will be conducted with the help of a mix of tools viewed by the company as *DPP software*.

In a typical case, the company will already operate with product identifiers and will have an information system for managing product information (a PIM). In that case it would be expected that the DPP can be produced automatically from the information in PIM and then associated with the product identifier.

There could also exist a number of third-party DPP service providers, providing services such as converting product information management system (PIM) information to the DPP format or using AI to convert human text into the DPP format or additionally offering DPP web page hosting.

It is likely that a number of specialized companies will start offering DPP *software as a service* on behalf of the REO. Such services will likely:

- Provide the necessary APIs to automatically form the DPP data structure from multiple data sources.
- Publish the DPP data structure as a suitable web page.
- Validate the correctness of the mandatory DPP data structure.
- Register the required information in the central EU DPP registry.

- Optionally publish non-mandatory additional data.

We note that the methods of producing the DPP data structure from the data available from PIM will vary. In some cases it can be produced via traditional, structured software methods. In other cases, it may need using AI technologies to, e.g., automatically distill relevant data from possible textual information in PIM. It is highly likely that in some cases human oversight and a human/software/AI dialogue will be involved in producing a DPP from a PIM.

3.3 VOCABULARY HUB AND VALIDATION CHECK

A vocabulary hub providing schemas and semantic information for specific regulated DPPs would be a very convenient component.

The EU public authorities and the Member State market surveillance authorities will likely be endowed with means to verify the validity of the DPP, a function that could be part of the EU registry. A vocabulary hub providing schemas and allowing validation would support this functionality and could be provided not just to authorities but also as a service to economic operators.