CIRPASS 2
Digital Product Passport

RISKS AND MITIGATIONS: A COMPANION TO D4.1 REFERENCE ARCHITECTURE

12/05/2025

Funded by the European Union

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.

RISKS AND MITIGATIONS

A companion to D4.1 COMPANION ARCHITECTURE

Work package	WP Number
Task	T4.1
Due date	15/05/2025
Submission date	12/05/2025
Deliverable lead	TNO
Version	1.0
Authors	David Roefs (TNO), Huib van Nieuwenhuijze (TNO), Kartik Chawla (TNO), Noah Smeets (TNO), Sjoerd Rongen (TNO), Jesper Kuiper (TNO), Rik Rurup (TNO), Mohammed Nacer Lazrak (TNO), Carolynn Bernier (CEA) & many other contributors form the CIRPASS2 consortium
Reviewers	Thijs Klooster (TNO)
Abstract	This document describes risks that can decrease the added value of the DPP system or might harm interest of parties. It proposes mitigations to those risks.
Keywords	System architecture, Digital product passports, ESPR, Risks, Mitigations
Citation	Roefs, D., van Nieuwenhuijze, H., Chawla, K., Smeets, N., Rongen, S., Kuiper, J., Rurup, R., Lazrak, M. N., & Bernier, C. (2025). Risks and mitigations: a companion to D4.1 Reference Architecture. CIRPASS-2 Consortium. https://doi.org/10.5281/zenodo.15389456

Document Revision History

Version	Date	Description of change	List of contributor(s)
0.1	29-04-2025	Creation of the document a derivate form the Reference Architecture document	
1.0	12-05-2025	Finalizing document	

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	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

TABLE OF CONTENTS

GLOSSARY & ABBREVIATIONS

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

'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.

'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).

'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.

[1] ISO 23234:2021

1 INTRODUCTION

The DPP system brings a number of advantages to the European Union. For the advantages of the DPP system to materialize, it is essential the DPP system[2] keeps functioning correctly, also in the face of actors who behave in a non-compliant manner or with malicious intent. This document presents a aggregation of risks that can undermine the DPP system. The document also presents mitigations to make the system more resilient to the effects of those risks. The mitigations have been considered in the design of the DPP architecture. Risks that could not be mitigated are listed in the final section of this document.

1.1 SCOPE OF THE ANALYSIS

The scope of the analysis consists of the technical side of the DPP system, as well as the non-technical side of the DPP system. Both are analyzed because an overlap between the technical and non-technical side exists. Non-technical risks can be solved by technical solutions, and technical risks can be solved by non-technical means. It has been found that many risks of abuse by the system cannot feasibly be mitigated using technical means. Those risks need to be mitigated by non-technical means.

1.2 ACTORS THAT MIGHT BEHAVE WITH MALICIOUS INTENT

Many types of actors will interact with the DPP system. As different actors have different capabilities and interests, the considered actors are listed. The following actors have been considered to be able to behave in a non-compliant or malicious manner which can harm the functioning of the DPP system:

- responsible Economic Operator (rEO)
- Independent Operator (IO)
- Digital Product Passport Service Provider (DPPSP)
- Supply chain actors
- End users
- State actors
- Criminal groups
- Hacktivists
- Insider threats

For the following actors malicious intent is only assumed to come from insider threats (i.e. it is assumed there will be no government body that has as goal to harm the functioning of the DPP system):

- The EC
- Other government bodies

[2] Both the technical as well as the non-technical part

2 RISKS

In this chapter, first a definition of risks is given in Section 2.1. Then, the process of identifying relevant risks is explained in Section 2.2. A list of all identified events that underly risks is presented in Section 2.3.

2.1 DEFINITION

The DPP system is intended to bring more benefits than costs[3]. Some costs of the DPP system are not fixed: those costs might be incurred, but only as an effect of an action[4] that might be performed by an actor when the DPP system is operational. Such a cost that might be incurred by an action is what is meant by a 'risk' in this section.

2.2 IDENTIFYING RISKS

Risks come to exist because a situation can be caused by an action. Therefore actions are aggregated. The first step is to identify all events that can occur. Then, all actions that can cause the event are aggregated. An action is only relevant when an actor is motivated to actually perform the action. In the context of risk, only actions which have a negative effect are considered. Therefore, for every action, two questions need to be answered:

1. what event is caused by the action?
2. what is the motivation of an actor to cause the event?

Different types of actors can be identified which have different motivations and capabilities. A risk is only relevant if an actor has the motivation and the capability to perform the action[5]. For every event, actions have been aggregated. The aggregated events and actions are presented in Section 2.3. Actions are only listed if a motivation could be identified for an actor to perform the action. The motivations are not included to improve the readability of the document.

[3] Benefits and costs are not necessarily monetary, but also include for example social, strategic and environmental gain and loss.
[4] The terms 'action' and 'motivation' should be interpreted broadly: it also includes inaction because an actor is not motivated, as inaction caused by lack of motivation can also cause an event (such as the addition of a part with dangerous substances to a product that is not included in the DPP).
[5] For example, a consumer might be motivated to add a new, expensive, part to the DPP of a product that does not actually have the part, to increase the value of the product. Because an average consumer does not have the technical knowledge to compromise the digital systems of rEO, the risk that such a rEO is compromised by the consumer in order to add the part to the DPP is small. A state actor might have a team of cyber security specialist available who can compromise the systems of a rEO within hours. But the state actor is probably not interested in attacking a rEO to add a part to a product. So even though a motivated actor might exist, and at the same time a capable actor might exist, the risk they will perform the action is still limited as long as no actor is both motivated and capable.

2.3 LIST OF ACTIONS

The list of events below is structured based on events, with relevant actions attached to the events. Events are aligned to the left of the page. Related actions are indented one level below the events. Motivations are left out of the document for readability.

Actions are labeled as being non-technical (👤) or technical (⚙) actions. Non-technical actions are actions caused by malicious usage of the system or by bypassing the system. This kind of action can be performed even when the system is operating exactly as it is meant to[6]. Technical actions are performed by a malicious actor exploiting a technical flaw in the system or the design of the system. This kind of action can be performed only when the system is not operating exactly as it is meant to, for example due to a technical flaw in the design or the implementation of the system. Almost all identified actions cause damage to the goal of the DPP system (e.g. allow actors to retrieve accurate information about a product) while only few actions causing damage to just the system.

Events are categorized based on the life cycle of a DPP: creation, storage, retrieving, updating and deletion.

EVENTS OCCURRING DURING THE CREATION OF THE DPP AND PRODUCT

- A new DPP containing incorrect information is added to the system
    - 1A. 👤 The rEO provides too little information
    - 2A. 👤 The rEO provides too much information
    - 3A. 👤 The rEO provides incorrect information
- An existing DPP is used for a new product
    - 4A. 👤 The rEO reuses one of its own DPP's to put on a product
    - 5A. 👤 The rEO uses a DPP of another rEO to use on a product
- A new DPP for a non-existing product is submitted to the system
    - 6A. 👤⚙ A (fake) rEO submits a DPP with bogus information
    - 7A. ⚙ The rEO submits an excessive amount of DPP's to perform a Denial-of-Service attack
- A new product is made but no DPP is submitted
    - 8A. 👤 The rEO creates a new product, but does not create a new DPP
- A DPP that is being created is intercepted during transfer
    - 9A. ⚙ An actor intercepts the information that is submitted on creation

EVENTS OCCURRING DURING THE STORAGE OF THE DPP AND THE PRODUCT

- A DPP can no longer be retrieved
    - 10A. 👤 The DPP host deletes the information
    - 11A. ⚙ The DPP host stops operating
    - 12A. ⚙ An actor performs a cyber-attack on the DPP host which causes the DPP's to be lost
- The information in a DPP is altered with malicious intent

[6] For example, a malicious state actor identifies a crucial producer in a strategic supply chain by requesting a DPP.

  - 13A 👤 The DPP host alters the information
  - 14A. ⚙ An actor performs a cyber-attack on the DPP host which alters the DPP information
- A product is altered such that it links to a different DPP
  - 15A. 👤 The physical DPP data carrier is modified, replaced or hidden while a new link is attached to the product. The new link points to a different DPP
  - 16A. 👤 The physical DPP data carrier is modified, replaced or hidden while a new link is attached to the product. The new link points to a malicious web page
- Confidential information in a DPP is accessed by unauthorized parties
  - 17A. 👤 The DPP host accesses information it should not access
  - 18A. ⚙ The DPP host is target of a cyber-attack which has the objective to steal the DPP information
  - 19A. 👤 A malicious actor pretends to have a right to see the information
  - 20A. 👤 A malicious actor pays an authorized party to look up and share confidential information

EVENTS OCCURRING DURING THE RETRIEVING THE DPP

- The physical DPP data carrier becomes unreadable or lost
  - 21A. ⚙ An actor with physical access to the product makes the data carrier unusable
  - 22A. 👤 The rEO adds a bad quality data carrier to the product, which becomes unusable over time or because of rough usage
  - 23A. 👤⚙ Someone handling the product destroys the data carrier
- The redirection service is no longer able to resolve the DPP identification
  - 24A. ⚙ The redirection service provider stops providing the redirection service
  - 25A. ⚙ A denial of service attack is performed on the DPP redirection service
- Due to a problem with storing the DPP, the DPP can no longer be retrieved (see category ‘Storage of the DPP and the product’)
- A DPP that is being retrieved is intercepted during transfer
  - 26A. ⚙ An actor intercepts the information
  - 27A. ⚙ An actor intercepts and modifies the information
  - 28A. ⚙ An actor performs a Man-in-the-Middle attack, acting as both a DPP host and a DPP requester
- The retrieval of DPP’s is monitored
  - 29A. ⚙ An actor monitors internet traffic
  - 30A. ⚙ An actor identifies end users that retrieve a DPP
- Actors aggregate public information from DPP’s for malicious purposes
  - 31A. 👤 Actors compile an overview of supply chains dependencies
  - 32A. 👤 Actors compile an overview of properties of products that might be used in sensitive equipment
  - 33A. 👤 Actors use information from DPP dependencies to perform automated spear phishing attacks

- 34A. 👤 Actors compile an overview of strategic products a country can produce to assess the strategic autonomy of the country

EVENTS OCCURRING DURING THE UPDATING OF THE DPP

- A DPP is updated while the product is not updated
  - 35A. 👤 The rEO updates the DPP with incorrect information
  - 36A. 👤 An actor with the right to update the DPP updates the DPP with incorrect information
  - 37A. 👤 An actor with the right to update the DPP updates the DPP so often that loading and viewing the DPP becomes challenging due to the size of the changeset
  - 38A. 👤 An actor pretending to have the right to update the DPP updates the DPP with incorrect information
  - 39A. ⚙ The DPP is updated with incorrect information by an actor that performed a successful cyber-attack on an actor that has the right to update the DPP
- A product is updated while the DPP is not updated
  - 40A. 👤 An IO updates the product but neglects to update the DPP
  - 41A. 👤 An end user alters the product but does not update the DPP
  - 42A. 👤 A malicious third party alters the product but does not update the DPP
- Both a product and its DPP are updated, but the update to the DPP does not accurately reflect what happened to the product
  - 43A. 👤 An IO updates the product but updates the DPP inaccurately
  - 44A. 👤 An end user updates the product but updates the DPP inaccurately
  - 45A. 👤 A malicious third party updates the product but updates the DPP inaccurately

EVENTS OCCURRING DURING THE DELETION OF THE DPP

- The DPP is destroyed, but the product is not destroyed
  - 46A. 👤 A recycler reports the product is destroyed, while it is not. The DPP host destroys the DPP before the lifetime expires
  - 47A. 👤 An end-user reports the product is destroyed, while it is not
  - 48A. 👤 The DPP host destroys the DPP, stating it has been recycled, while the product has not been recycled
  - 49A. 👤 An actor pretending to be a recycler reports the product is destroyed
- A product is destroyed, but its corresponding DPP is not destroyed
  - 50A. 👤 A recycler does not notify the DPP host that the product has been destroyed
  - 51A. 👤 The product is lost (in a fire, flood, etc.), but the owner does not notify the DPP host to destroy the DPP
  - 52A: 👤 the product is brought to a landfill but the DPP is not destroyed

3 MITIGATIONS

This section presents mitigations to the risks in the previous section. Mitigations are measures that can be taken to lower a risk. Some risks can be completely eliminated. Other risks are only lowered, as there might be a risk to a mitigation. For this new risk, another mitigation can be considered.

The risks of Section 2 are repeated, with the risk number that is also used in Chapter 2 in front (R1, R2, etc.). The risk is followed by one or more possible mitigations. As discussed, the mitigations might have their own risks associated with them. If such a such a risk has been identified, it is placed directly after the mitigation. This risks can then be followed by new mitigations if applicable.

All considered mitigations are listed in this section. This includes both mitigations that have been included in the reference architecture, as well as mitigations that have not been included in the reference architecture. It also includes mitigations that are not technical, which cannot be included in the reference architecture.

EVENTS OCCURRING DURING THE CREATION OF THE DPP AND PRODUCT

R1. Risk: The rEO provides too little information

Possible mitigation: A service validates whether all required fields are submitted.

Risk: The rEO submits all fields, but provides too little information in the fields.

Possible mitigation: The rEO is penalized when providing too little information in the fields

2A. Risk: The rEO provides too much information

Possible mitigation: see mitigations of Risk 1A.

Possible mitigation: The API allows to query only a specific section of a DPP, for example only the mandatory information. This allows downloading only the mandatory, even if the DPP has become difficult to download due to its (maliciously inflated) size.

3A. Risk: The rEO provides incorrect information

Possible mitigation: see mitigations of Risk 1A.

Possible mitigation: The rEO is penalized

Risk: The rEO claims it was unclear more information had to be provided

Possible mitigation: The rEO is penalized nonetheless

Risk: The rEO claims information it received from other parties was incorrect

Possible mitigation: The rEO is penalized nonetheless

4A. Risk: The rEO reuses one of its own DPP's to put on a product

Possible mitigation: The rEO is penalized for reusing a DPP

Risk: The rEO takes the risk

5A. Risk: The rEO uses a DPP of another rEO to use on a product

Possible mitigation: The rEO is penalized for reusing a DPP

Risk: The rEO takes the risk

6A. Risk: The rEO submits a DPP with bogus information

Possible mitigation 1: Only authenticated and authorized rEO's can submit a DPP

Possible mitigation 2: rEO's can be (temporary) denied of submitting DPP's

Possible mitigation 3: Submitted DPP's can be altered, removed or (partly) hidden by a trusted administrator

7A. Risk: The rEO submits an excessive amount of DPP in a Denial-of-Service attack

Possible mitigation: A system is in place to limit the number of DPP's submitted by an rEO per day

8A. Risk: The rEO creates a new product, but does not create a new DPP

Possible mitigation 1: The rEO is penalized for not creating a DPP for a new product

EVENTS OCCURRING DURING THE STORAGE OF THE DPP AND THE PRODUCT

10A. Risk: The DPP host deleted the information

Possible mitigation 1: A DPP host cannot be the rEO, who might have an interest in deleting the information

Possible mitigation 2: A backup is kept at a third party, which cannot be altered or removed by the rEO

Risk: The third party is dependent on the rEO, for example because the rEO is the customer, and can be pressured to alter or remove the DPP

Possible mitigation: The other party may not be dependent on the rEO

11A. Risk: The DPP host stopped operating

Possible mitigation: A third party keeps a backup

Risk: After a while the third party also stops operating

Possible mitigation: The third party needs to store a backup by a different party as soon as the rEO stops operating

12A. Risk: An actor performed a cyber-attack on the DPP host which caused the DPP's to be lost

Possible mitigation: A third party keeps a backup

13A. Risk: The DPP host alters the information

Possible mitigation 1: A DPP host cannot be the rEO, who might have an interest in altering the information

Possible mitigation 2: a backup is kept at another party, which cannot be altered or removed (except when a record of the alterations or removals is kept)

Risk: The other party is dependent on the rEO, for example because the rEO is the customer

Possible mitigation: The other party may not be dependent on the rEO

Risk: 14A. An actor performed a cyber-attack on the DPP host which altered the DPP information

Possible mitigation: A third party keeps a backup

Risk: The alteration is performed such that it is not clear the information is incorrect

Possible mitigation: The backup provider verifies the original DPP is still correct on regular intervals

15A. Risk: The physical DPP data carrier is modified, replaced or hidden while a new link is attached to the product. The new link points to a different DPP

Possible mitigation: A backup data carrier is attached to the product

Risk: If the end user can identify the backup data carrier, so can the malicious actor

Possible mitigation 1: The end user checks the purchase agreement to validate the data carrier links to the correct DPP. The original DPP or UID is placed on purchase agreements

Possible mitigation 2: Inspections on national level check product categories that are prone to replacement of the data carrier

Possible mitigation 3: User scans product with DPP application that visually identifies product next to data carrier to perform the check

16A. Risk: The physical DPP data carrier is modified, replaced or hidden while a new link is attached to the product. The new link points to a malicious web page

Possible mitigation 1: Apps that can read the data carrier verify that the data carrier links to a known and valid DPP weblink

Possible mitigation 2: A backup data carrier is attached to the product

Risk: If the end user can identify the backup data carrier, so can the malicious actor

Possible mitigation: Users are made aware of checking whether the data carrier links to the correct site

17A. Risk: The DPP host accesses information it should not access

Possible mitigation 1: The DPP host never stores (and never receives in the first place) information it does not have to access

Possible mitigation 2: The received information is encrypted with a key unknown to the DPP host

18A. Risk: The DPP host is target of a cyber-attack which has the objective to steal the DPP information

Possible mitigation 1: 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

Possible mitigation 2: The DPP host takes cyber security measures that correspond to the sensitivity of DPP information

Risk: This becomes too expensive

19A. Risk: An malicious actor pretends to have right to see the information

Possible mitigation: Only authenticated and authorized parties with the correct roles can access information.

Risk 1: Credentials are stolen/brute forced

Possible mitigation: credentials can be revoked

Risk 2: Parties get authorizations they should not have

20A. Risk: An malicious actor pays an authorized party to look up and share confidential information

Possible mitigation 1: Authorizations are as minimal as possible

Possible mitigation 2: Access to information is logged

Possible mitigation 3: Actors need to proof they need access to confidential information

Possible mitigation 4: Categorization instead of complete information (this product contains >50% or <50% metal)

Possible mitigation 5: Possibly: a party that accesses information needs to provide a reason

Possible mitigation 6: Accessing information for which is no need is penalized

Risk: A party has a valid reason to access information, but also sells it to a malicious actor

EVENTS OCCURRING DURING THE RETRIEVING THE DPP

21A. Risk: An actor with physical access to the product makes the data carrier unusable

Possible mitigation 1: The purchase agreement contains the product id or data carrier that allows for DPP access

Possible mitigation 2: A web portal is created that allows to identify a product using the web portal

22A. Risk: The rEO adds a bad quality data carrier to the product, which becomes unusable over time or because of rough usage

Possible mitigation: Mandatory robustness requirements for the data carrier are set

23A. Risk: Someone handling the product destroys the data carrier

Possible mitigation 1: A product without a DPP is not allowed and the process of giving a product a new data carrier is expensive, making it less attractive to deliberately remove the data carrier

Possible mitigation 2: Mandatory robustness requirements for the data carrier are set

Risk: This only prevents non-intentional destruction of the data carrier

Possible mitigation 1: The purchase agreement contains the product id or data carrier that allows for DPP access

Possible mitigation 2: A web portal is created that allows to identify a product using the web portal

24A. Risk: The redirection service provider stops providing the redirection service

Possible mitigation: The redirection service can be provided by a new party when the default redirection service provider stops providing the redirection service

25A. Risk: A denial of service attack is performed on the DPP identification

Possible mitigation: The redirection service provider takes adequate measures to be able to offer the service also when a DDOS attack is active

26A. Risk: An actor intercepts the information

Possible mitigation: DPP's are send over a properly encrypted connection

27A. Risk: An actor intercepts and modifies the information

Possible mitigation: DPP's are send over a properly encrypted connection

28A. Risk: An actor performs a Man-in-the-Middle attack, acting as both a DPP host and a DPP requester

Possible mitigation: DPP hosts and DPP requesters authenticate each other

29A. Risk: An actor monitors internet traffic

Possible mitigation 1: DPP's are hosted in a more centralized manner

Possible mitigation 2: 'Mixer' or 'proxy' hosts are added to the network, which receive and request multiple DPP' on behalf of different users. This limits, but does not remove the traceability.

30A. Risk: An actor identifies end users when retrieving a DPP (end user tracking)

Possible mitigation: It is mandated that a web page displaying a DPP does not contain JavaScript or trackers to limit end user tracking

Risk: Actors use server side end user tracking mechanisms

Possible mitigation: This is penalized

Risk: Malicious actors (possibly in another jurisdiction) carry on with tracking

31A. Risk: Actors compile an overview of supply chains dependencies

Possible mitigation: A decentralized rate limiting system is implemented (unknown whether this is possible)

Risk: Actors that are determined work around the rate limiting system

32A. Risk: Actors compile an overview of properties of products that are (likely) to be used in sensitive equipment

Possible mitigation: A decentralized monitoring and detection system is implemented (unknown whether this is possible) and actors that seem to be compiling an overview are blocked from the system

33A. Risk: Actors use information from DPP dependencies to perform automated spear phishing attacks

Possible mitigation: product ownership is not placed in a DPP unless consent is given

34A. Risk: Actors compile an overview of strategic products a country can produce to assess the strategic autonomy of the country

Possible mitigation: A decentralized rate limiting system is implemented (unknown whether this is possible)

Risk: Actors that are determined work around the rate limiting system

EVENTS OCCURRING DURING THE UPDATING OF THE DPP

35A. Risk: The rEO updates the DPP with incorrect information

Possible mitigation: The old DPP is retained, and a log is kept of what is updated by the rEO and when. This log is not stored by the rEO

36A. Risk: An actor with the right to update the DPP updates the DPP with incorrect information

Possible mitigation 1: Only authenticated and authorized actors can update a DPP

Possible mitigation 2: The list of authorized actors is kept to a minimum

Possible mitigation 3: Every update is logged (including what, when and possibly why the DPP has been updated)

37A. Risk: An actor with the right to update the DPP updates the DPP so often that loading and viewing the DPP becomes challenging due to the size of the changeset

Possible mitigation: it is possible to request only the latest version of the DPP, without changes

38A. Risk: An actor pretending to have the right to update the DPP updates the DPP with incorrect information

Possible mitigation: Only authenticated and authorized actors can update a DPP

Risk: The actor creates business in the EU, pretends to be a company that would be authorized to update the DPP, and updates the DPP

Possible mitigation: This is penalized

Risk: The actor is from a different jurisdiction

39A. Risk: The DPP is updated with incorrect information by an actor that performed a successful cyber-attack on an actor that has the right to update the DPP

Possible mitigation 1: Actors can review the updates made to DPP's using their own account

Possible mitigation 2: Actors that can update DPP's should take appropriate security measures to prevent their credentials being abused

Possible mitigation 3: An anomaly detection system is implemented that can identify malicious updates to DPP's

40A. Risk: An IO updates the product but neglects to update the DPP

Possible mitigation: This is penalized

41A. Risk: An end user alters the product but does not update the DPP

No suitable mitigation has been identified

42A. Risk: A malicious third party alters the product but does not update the DPP

Possible mitigation: This is penalized

Possible mitigation: Physical security measures prevent this

43A. Risk: An IO updates the product but updates the DPP inaccurately

Possible mitigation: This is penalized

44A. Risk: An end user updates the product but updates the DPP inaccurately

No suitable mitigation has been identified

45A. Risk: A malicious third party updates the product but updates the DPP inaccurately

Possible mitigation 1: This is penalized

Possible mitigation 2: Physical security measures prevent this

EVENTS OCCURRING DURING THE DELETION OF THE DPP

46A. Risk: A recycler reports the product is destroyed, while it is not. The DPP host destroys the DPP

Possible mitigation: This is penalized

47A: Risk: An end-user reports the product is destroyed, while it is not. The DPP host destroys the DPP

Possible mitigation: This is penalized

48A. Risk: The DPP host destroys the DPP, stating it has been recycled, while the product has not been recycled

Possible mitigation: This is penalized

49A. Risk: An actor pretending to be a recycler reports the product is destroyed

Possible mitigation: This is penalized

Risk: As the DPP is destroyed, it is hard to proof wrongdoing

Possible mitigation: The DPP is not actually destroyed, but only a label "destroyed" is added to the DPP when a recycler reports the product as destroyed

50A. Risk: A recycler does not notify the DPP host that the product has been destroyed

Possible mitigation: This is penalized

Risk: It is hard to proof a recycler recycled a product if no trace of the product is left

51A. Risk: The product is lost (in a fire, flood, etc.), but the owner does not notify the DPP host to destroy the DPP

No suitable mitigation has been identified

52A: Risk: The product is brought to a landfill but the DPP is not destroyed

Possible mitigation: Products are marked as deleted after a set time

4 RISKS THAT ARE NOT HANDLED

Some risks are not handled. Risks are not handled because no mitigation exists, or because mitigation is deemed too costly (too costly in terms of money or in burden to the system). If a risk is considered significant but is not mitigated in the reference architecture or otherwise, it is included in the table below.

The table below shows the action that forms the risk that is not mitigated in the second column. In the third column, a description of what the risks means is given.

#	Action	Risk
4A	The rEO reuses one of its own DPP's to put on a product	Products are linked to a DPP that does not accurately describe the product, which diminishes trust in the DPP system and undermines the system
5A	The rEO uses a DPP of another rEO to use on a product	Products are linked to a DPP that does not accurately describe the product, which diminishes trust in the DPP system and undermines the system
10A	The DPP host deleted the information	Parties that rely on the DPP data but who's interest does not align with the interest of the rEO cannot always use the DPP system as an information source for proof, as the rEO can delete the information.
13A	The DPP host alters the information	Parties that rely on the DPP data but who's interest does not align with the interest of the rEO cannot always use the DPP system as an information source for proof, as the rEO can alter the information.
15A	The physical DPP data carrier is modified, replaced or hidden while a new link is attached to the product. The new link points to a different DPP	Products are linked to a DPP that does not accurately describe the product, which diminishes trust in the DPP system and undermines the system
16A	The physical DPP data carrier is modified, replaced or hidden while a new link is attached to the product. The new link points to a malicious web page	End-user devices and systems might become compromised
18A	The DPP host is target of a cyber-attack which has the objective to steal the DPP information	Intellectual property is stolen, diminishing the profitability of the company and possibly undermining the strategic position of the European economy

20A	A malicious actor pays an authorized party to look up and share confidential information	Intellectual property is stolen, diminishing the profitability of the company and possibly undermining the strategic position of the European economy
21A	An actor with physical access to the product makes the data carrier unusable	The added value of the DPP system diminishes
30A	An actor identifies end users when retrieving a DPP	The privacy of end users is violated
31A	Actors compile an overview of supply chains dependencies	Strategic information about production information in the European Union becomes available to (strategic) competitors
33A	Actors use information from DPP dependencies to perform automated spear phishing attacks	Cyber attacks are more effective, causing more damage to end-users. The reputation of the DPP system diminishes.
34A	Actors compile an overview of strategic products a country can produce to assess the strategic autonomy of the country	Strategic information about production information in the European Union becomes available to (strategic) competitors
36A	An actor with the right to update the DPP updates the DPP	Trust in the DPP system diminishes, products are valued wrong or are recycled improperly
41A	An end user alters the product but does not update the DPP	Trust in the DPP system diminishes, products are valued wrong or are recycled improperly
43A	An end user updates the product but updates the DPP inaccurately	Trust in the DPP system diminishes, products are valued wrong or are recycled improperly
44A	An end user updates the product but updates the DPP inaccurately	An end user updates the DPP of a product inaccurately, due to being unqualified or having malicious intent. End users lose their trust in DPP's of second hand products.
50A	A recycler does not notify the DPP host that the product has been destroyed	DPP's that do not correspond to a physical product anymore remain in the system