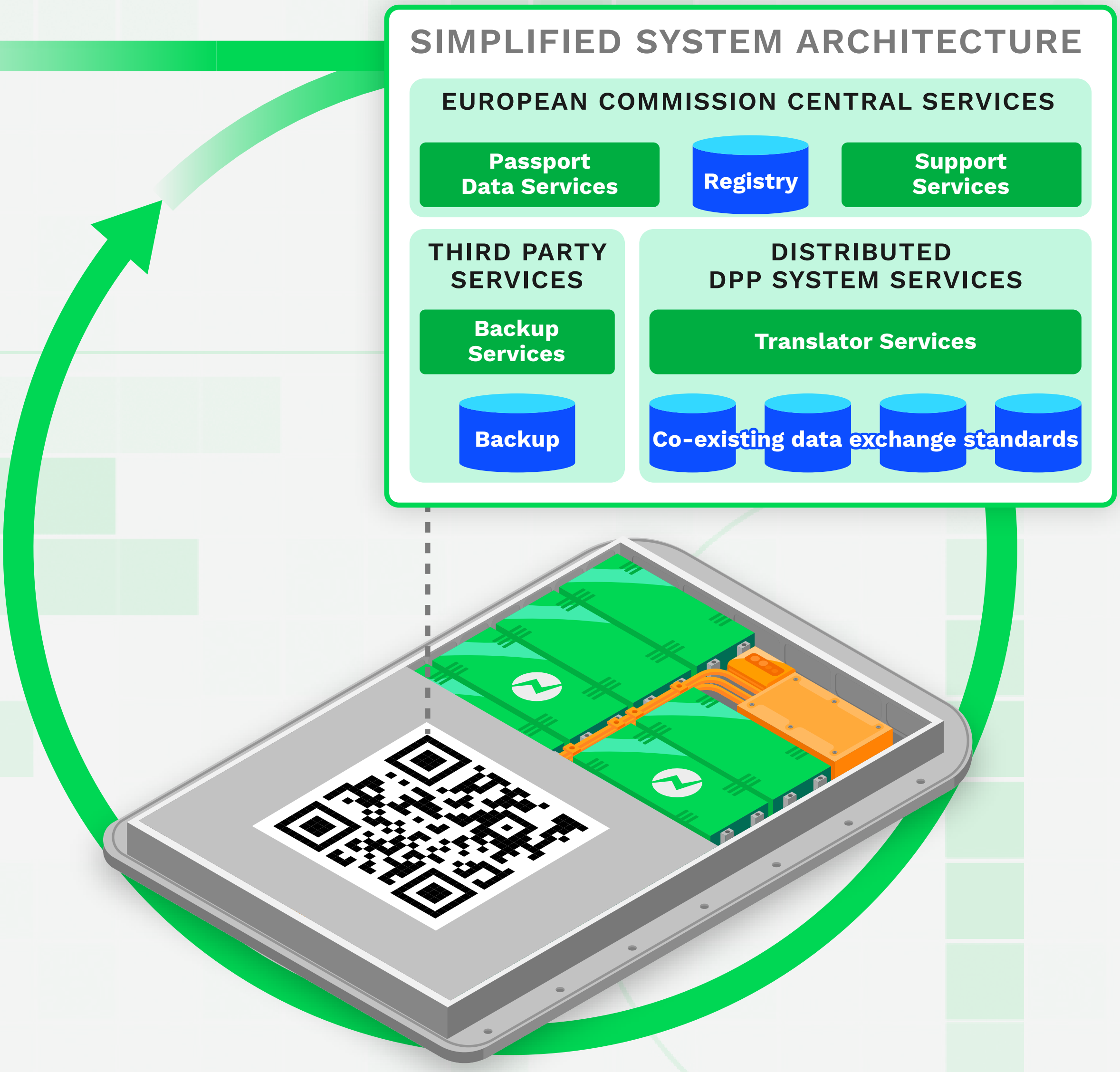
Battery Pass


SIMPLIFIED SYSTEM ARCHITECTURE
EUROPEAN COMMISSION CENTRAL SERVICES
Passport Data Services
Registry
Support Services
THIRD PARTY SERVICES
Backup Services
Backup
DISTRIBUTED DPP SYSTEM SERVICES
Translator Services
Co-existing data exchange standards

Battery Passport Technical Guidance

Technical challenges,
standards and recommondations
for a battery passport system

Version 1.0 / March 2024

Supported by:
Federal Ministry
for Economic Affairs
and Climate Action

on the basis of a decision
by the German Bundestag

The Battery Pass consortium

CONSORTIUM LEAD

SYSTEMIQ

CONSORTIUM PARTNERS

acatech

BASF We create chemistry

BMW GROUP

Circulor

FIWARE FOUNDATION

Fraunhofer IPK

TWAICE

umicore

VDE RENEWABLES

*under subcontract

ASSOCIATED PARTNERS

GLOBAL BATTERY ALLIANCE

GS1 in Europe

RWE

SAP

Co-funded by the German Federal Ministry for Economic Affairs and Climate Action (BMWK), the Battery Pass consortium project aims to advance the implementation of the battery passport based on requirements of the EU Battery Regulation and beyond. Led by system change company Systemiq GmbH, the consortium comprises eleven partners and a broad network of associated and supporting organisations to draft content and technical standards for a digital battery passport, demonstrate them in a pilot application and assess its potential value.

DISCLAIMER

This document (the “Document”) is for informational purposes only and is being made available to you by the Battery Pass consortium.

This document is published by the Battery Pass consortium and contains information that has been or may have been provided by a number of sources. The findings, interpretations and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by the Battery Pass consortium. The Battery Pass consortium partners (the partners as set out on the following page of this Document) endorse the overall project approach and findings and the Battery Pass consortium has made efforts to accurately capture stakeholder positions set out by organisations (including supporting partners and further experts), although the results may not necessarily represent the views of all individuals or the organisations they represent. The Battery Pass consortium has not separately verified the information provided from outside sources and cannot take responsibility if any of these statements misrepresent a stakeholder position or if positions evolve over time.

To the extent permitted by law, nothing contained herein shall constitute any representation or warranty and no responsibility or liability is accepted by the Battery Pass consortium as to the accuracy or completeness of any information supplied herein. Recipients of this Document are advised to perform independent verification of information and conduct their own analysis in relation to any of the material set out.

The statements contained herein are made as at the date of the Document. The Battery Pass consortium or any member, employee, counsel, offer, director, representative, agent or affiliate of the Battery Pass consortium does not have any obligation to update or otherwise revise any statements reflecting circumstances arising after the date of this Document.

This Document shall not be treated as tax, regulatory, accounting, legal, investment or any other advice in relation to the recipient of this information and this information should not and cannot be relied upon as such.

If you are in any doubt about the potential purpose to which this communication relates you should consult an authorised person who specialises in advising on business to which it relates.

Table of contents

Preface

Batteries are a pivotal element for sustainable and climate-neutral transport and the energy transition in general. They power electric cars, trucks and other means of transport and they can store the energy intermittently supplied from renewable sources. We cannot decarbonise our societies without batteries. In this context, the German Federal Ministry for Economic Affairs and Climate Action (BMWK) is pursuing two goals:

Firstly, to secure the supply of batteries for Europe in a fast-growing global market. To this end, the entire value chain is taken into account. This entails the localisation of the major part of this value chain (upstream including materials refining in Europe), based on European knowhow including the corresponding machinery. As regards the needed raw materials, we in parallel support the ramp-up of domestic mining in Europe, the establishment of large-scale recycling as well as sourcing the indispensable raw material imports from like-minded countries in a sustainable manner.

Secondly, to ensure that the batteries offered on the EU market comply with the highest – that means world-leading – standards with respect to climate footprint, social and environmental sustainability. This is necessary to comply with our European values. It is further needed to make use of the full decarbonisation potential of battery-powered applications, but there is also an industrial policy angle to it: We strive to establish a European battery industry that is leading globally in terms of environmental and social standards.

To verifiably and credibly ensure that batteries comply with these standards (carbon and environmental footprint, social responsibility, repairability, recyclability, etc.), which now have a regulatory foundation in the EU Battery Regulation, we need a transparency instrument. The battery passport shall deliver just that – a digital record that documents all conditions under which a battery has been produced, logs its relevant usage history and delivers crucial information for repair, reuse and recycling. The battery passport is a striking embodiment of the (digital and green) “twin transition”: it utilises the digital world to facilitate the decarbonisation of the real world. And it rightfully is a key pilot application of digital product passports in general, to be rolled out in other sectors in the future, thus increasing its significance.

The “Battery Pass” project, joining partners from industry and academia along the value chain and funded by BMWK with €8.2 million, develops standards for a battery passport and implements those in a demonstrator. It is the first large-scale project tackling a pilot implementation of the battery passport comprising all key elements – technical and content standards as well as software implementation and impact evaluation. The project intends to deliver a workable exhibit of how a real-world battery passport will look and work. Its output will focus on the requirements of the EU Battery Regulation but have in mind also the interoperability with other markets.

The document presented here is a major milestone in the 3-year journey of the Battery Pass project. It provides businesses and other actors of the battery value chain with a first comprehensive picture of the technical requirements of the upcoming battery passport in Europe and beyond. It is thus an important contribution towards the EU process, detailing the operative elements of the passport mandated in the EU Battery Regulation, as well as towards a smooth and quick implementation of the passport in business reality.

Dr Tim Schulze, Policy Officer, Unit IV A 6, Federal Ministry for Economic Affairs and Climate Action (BMWK)

Acknowledgements

All sorted alphabetically by organisations and individuals.

Authors of this document coordinated by Fraunhofer IPK:

- Niko D'Agostino, Circulor GmbH
- Gernot Böge, FIWARE Foundation e.V.
- Coenraad van Deventer, Circulor GmbH
- Jason Fox, FIWARE Foundation e.V.
- Patrick Gering, Fraunhofer IPK
- Prof. Dr-Ing. Thomas Knothe, Fraunhofer IPK

Consortium partner working group members (excl. the authors):

- Anna Sophia Braunfels, Systemiq GmbH
- Dr. Torsten Freund, BASF SE
- Dr. Sven Jantzen, Umicore AG & Co KG
- Dr. Lisa Risch, acatech – National Academy of Science and Engineering e.V
- Stephanie Schenk, Systemiq GmbH
- Dr. Johannes Simböck, acatech – National Academy of Science and Engineering e.V
- Tilmann Vahle, Systemiq GmbH
- Patrick Zank, VDE Renewables GmbH

Advisory Council:

- Christian Eckert, ZVEI e.V.
- Dr. Jens Gayko, VDE e.V.
- Thomas Götz, Wuppertal Institut für Klima, Umwelt, Energie gGmbH
- Benjamin Helfritz, DIN e.V.
- Lars Johanssen, BMUV / GIZ GmbH
- Dr. Michael Krausa, KLiB e.V.
- Julia Poliscanova, European Federation for Transport & Environment AISBL
- Ernst Stöckl-Pukall, BMWK
- Ilka van Dalwigk, European Battery Alliance (EBA) / EIT InnoEnergy SE

Design and editorial:

- Design: Antje Kelly, FIWARE Foundation e.V.
- Proofread: Cassandra Rigg

List of abbreviations

Abbreviation	Definition
API	Application Programming Interface
BMS	Battery Management System
BOM	Bill of Materials
CEF	Connecting Europe Facility
CEID	Circular Economy Initiative Germany
CF	Carbon Footprint
CLP Regulation	Classification, labelling and packaging Regulation
CFF	Circular Footprint Formula
CoC	Chain of Custody
CSRD	EU Corporate Sustainability Reporting Directive
DG CONNECT	Directorate-General for International Partnerships by the European Commission
DG GROW	Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs by the European Commission
DG TAXUD	Directorate-General for Taxation and Customs Union by the European Commission
DID	Digital Identifier
DPP	Digital Product Passport
DSBA	Data Space Business Alliance
DSSC	Data Space Support Center
ECHA	European Chemicals Agency
EC Number	European Community number (unique seven-digit identifier for enzymes)
EES	Electronic Exchange System
EOL	End-of-life
ESPR	Ecodesign for Sustainable Products Regulation
ETSI	European Telecommunications Standards Institute
EU CSDDD	EU Corporate Sustainability Due Diligence Directive

EU	European Union
EV	Electric Vehicle
GBA	Global Battery Alliance
GerSCA	German Supply Chain Due Diligence Act
GHG	Greenhouse gases
ICT	Information and Communication Technology
IEC	International Electrochemical Commission
IMDS	International Material Data System
JSON	JavaScript Object Notation
JSON-LD	JavaScript Object Notation for Linked Data
JTC	Joint Technical Committee
LMT	Light Means of Transport
OECD	Organisation for Economic Co-operation and Development
PEF	Product Environmental Footprint
PEFCR	Product Environmental Footprint Category Rules
SBESS	Stationary battery energy storage system
SoH	State of Health
SoC	State of Charge
SRAHG	Standardisation Request Ad-hoc group
SReq	Standardisation Request
VDA	Verband der Automobilindustrie (German Association of the Automotive Industry)
VC	Verifiable Credential
VP	Verifiable Presentation

List of figures

List of tables

Terminology

The Battery Pass Technical Guidance uses different terms to differentiate between regulatory requirements, recommendations, and permissible or allowable options:

Table 1 Terminology

Term	Expressed intention
Shall (not)	Requirement as per the Battery Regulation or other relevant legislation
Should (not)	Recommendation made by the Battery Pass consortium
May (not)	Option that is permissible
Mandatory	Requirement as per EU Battery Regulation or other relevant legislation (see “shall”)
Voluntary	Recommendation made by the Battery Pass consortium (see “should”)

1 Introduction

This document represents a comprehensive technical guidance of the Battery Pass consortium on how the battery passport system can look fand which required technical standards it should support. This document is intended as a foundation for other organisations to build on the results.

1.1 Context – European regulations implementing the Green Deal

The European Green Deal, initiated in 2019, is a response to the well-known climate and environmental challenges. It outlines a new growth strategy that aims to transform the EU into a fair and prosperous society, characterised by a modern, resource-efficient, and competitive economy. The goal is to achieve net-zero emissions of greenhouse gases by 2050 and decouple economic growth from resource consumption [1].

In March 2022, the EU launched the Sustainable Products Initiative (SPI), which included the Proposal for the Ecodesign for Sustainable Products Regulation (ESPR). This regulation provides a comprehensive policy framework for the widespread introduction of digital product passports across various product categories as facilitators for the transition to a circular economy (CE). Additional regulations exist, which encompass elements of traceability, chain of custody, and data sharing requirements. These regulations are all part of the European Union's Digital Transition and Data Spaces plans, designed to harmonise and standardise access to data.

In addition to other sector-specific regulatory activities (e.g. the Construction Products Regulation), the new EU Battery Regulation 2023/1542 is ground-breaking as it is the first product legislation that covers the entire product life cycle. Its comprehensive requirements include transparency on carbon footprint, including performance classes and maximum threshold values, metal-specific recycling rates, recycled content quotas, corporate supply chain due diligence obligations, minimum requirements for durability and performance, as well as the introduction of a digital battery passport – the first digital product passport (DPP) at the European level.

With the introduction of a digital battery passport, the European Commission aims to support the sustainable and circular management of batteries by requesting comprehensive data along the entire battery value chain to be documented and exchanged through a digital infrastructure. As the first in a series of sector-specific DPPs due to be introduced in the coming years, the battery passport can be seen as the pilot implementation of the entire technical DPP system. Therefore, the implementation must consider the technological applicability for the whole DPP ecosystem, including areas such as construction, textiles, and furniture, in addition to batteries.

The digital battery passport is detailed in *Chapter IX* of the EU Battery Regulation and will be mandatory for batteries in light means of transport (LMT), industrial batteries with a capacity above 2 kWh, and electric vehicle batteries placed or put into service on the EU market. It will be required from 18 February 2027 onwards, which is 42 months after the regulation entered into force on 17 August 2023 [2].

In parallel to the negotiation of the ESPR and Battery Regulation, the European Commission initiated the process to establish harmonised standards required for setting up, operating and, maintaining the DPP system from a technical perspective. Therefore, in May 2023, the first draft of a standardisation request (SReq) for the DPP system was sent to the European Standardisation Organisations CEN, CENELEC and ETSI as a basis for consultation and feedback. The SReq aims to underpin the regulatory specifications of the ESPR and the Battery Regulation.

In December 2023, the CEN-CENELEC Joint Technical Committee JTC 24 was established to develop the standards as required by the draft SReq, even though the proposal of the ESPR as well as the SReq have not been finalised. This decision was made because the timing requirements set forth in the Battery Regulation demand the availability of an operational DPP system for batteries by 18 February 2027. As a result, there is a strict deadline for the availability of technical standards on DPP by 31 December 2025. This would provide stakeholders in the battery industry just under 14 months for the implementation, testing and launch of their DPP system.

Due to the circumstances outlined above, the context of the technical standards is derived from the three sources of European regulation: the ESPR, the Battery Regulation and the current draft of the SReq on the DPP system. Furthermore, the very tight time constraints necessitate careful consideration when commencing operations of the DPP system for batteries, potentially with limited capabilities to meet the legal requirements.

1.2 Battery Pass Project

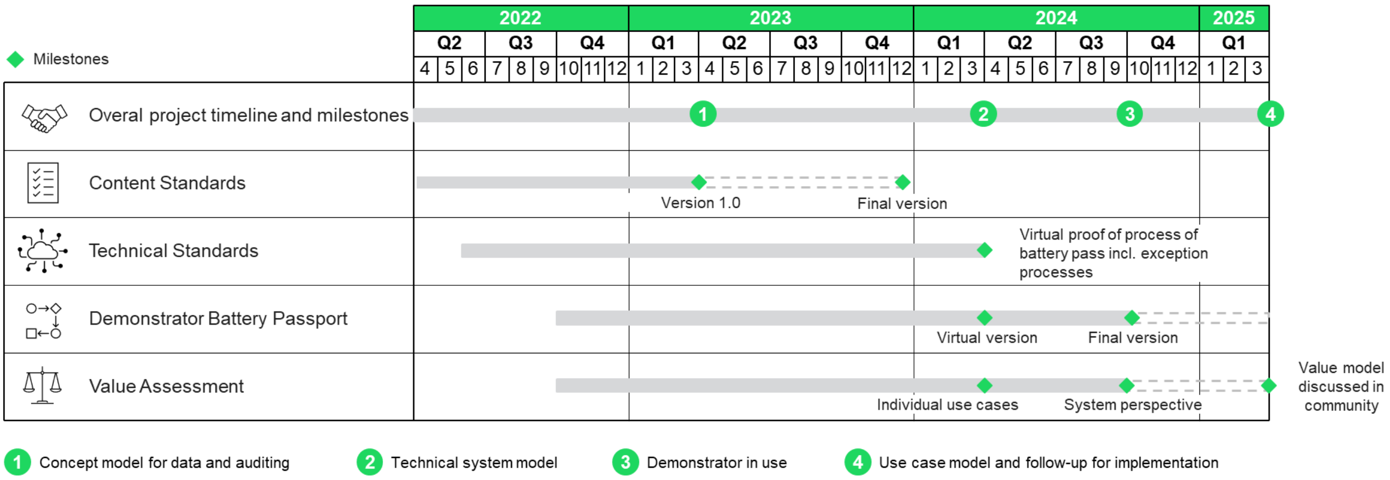
The Battery Pass Project, launched in April 2022, is developing a comprehensive view on the entire battery passport concept from content, technical and impact perspective. The core partners are acatech – National Academy of Science and Engineering, AUDI AG, BASF SE, BMW AG, Circulor GmbH, FIWARE Foundation e.V., Fraunhofer IPK, SYSTEMIQ GmbH, TWAICE Technologies GmbH, Umicore AG & Co KG, and VDE Renewables GmbH (under subcontract). The core partners are supported by numerous associated partners and supporting partners, most notably the Global Battery Alliance (GBA), GS1, Kompetenznetzwerk Lithium-Ionen-Batterien e.V. (KLiB), Mercedes Benz AG, RWE Generation SE and SAP SE and Siemens.

Over the course of the project, the consortium will develop a detailed content specification for the battery passport, necessary standards for complete and executable technical system and data infrastructure, a software and physical demonstrator, and qualitatively as well as quantitatively assess the passport's value for business, society, and environment alike (see Figure 1 and Figure 2).

Figure 1: Overview on Battery Pass consortium work packages and leading organisations

Work packages		Sub-topics
WP1	Project Coordination and Stakeholder Engagement	a) Consortium coordination b) Content governance for quality and coherence c) EU alignment and global compatibility d) External communication for results dissemination e) Scaling up and making results permanent
WP2	Content Standards	a) Carbon footprint b) Supply chain due diligence c) Circularity and resource efficiency d) Performance and durability e) Responsibility and liability f) Auditability
WP3	Technical Standards	a) Reference models for data collection along battery life cycle b) Contextualisation regarding EU and global data spaces c) Process and access logics based on the reference models
WP4	Demonstrator	a) Data infrastructure b) Data storage and process execution c) Integration with Catena-X/ EES/ Gaia-X d) Demonstration
WP5	Value Assessment	a) Benefit modelling of individual use cases b) Benefit modelling of the battery pass overall

Figure 2: Overview on Battery Pass consortium three-year timeline including major milestones

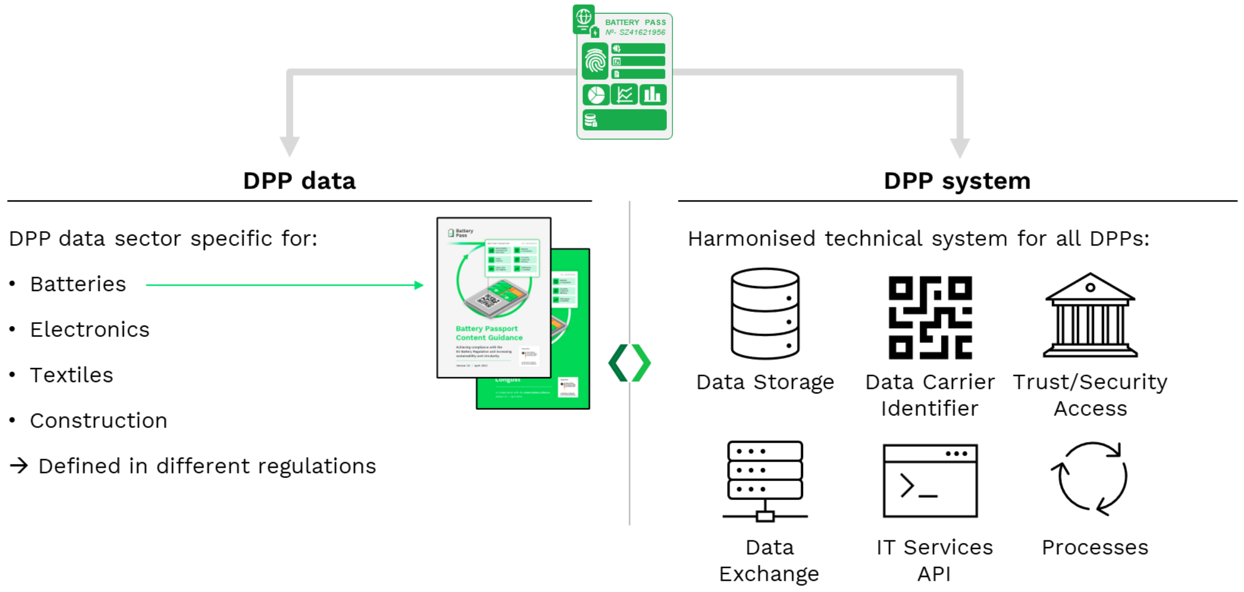


As defined in the SReq[1], based on the current version of the ESPR, the term “product passport” refers to a set of product-specific data that includes the information outlined in the applicable delegated act adopted in accordance to *Article 4* of COM(2022) 142 [3] final or specified in *Article 77* of Regulation (EU) 2023/1542. This data is accessible electronically through a data carrier [4]. According to this definition a digital product passport consists of two components: the DPP data and the DPP system. While the DPP data for batteries is specifically related to batteries

[1] Standardization requests are a mechanism for developing technical standards that can be closely tied to EU regulations and directives

within the scope of the Battery Regulation, the DPP system has to be designed to be applicable across different sectors (Figure 3).

Figure 3: The DPP consist of sector-specific DPP data and the interoperable DPP system



The DPP data is covered by the Content Guidance of the Battery Pass Project, which was launched in April 2023 and updated in December 2023. This document provides a comprehensive definition of the required data points, methodologies for data collection and calculation rules, as well as the long list of all mandatory data attributes as stipulated by the aforementioned regulations. Furthermore, the Content Guidance contributes to the standardisation efforts aimed at developing harmonised European Norms (hEN) for battery data.

This document addresses the DPP system specification, aiming to support the implementation of the regulations, mentioned above, to achieve the goals outlined in the Green Deal.

1.3 Aim, scope and targeted audience of this document

Aim

The primary objective of this document is to offer *a comprehensive overview of the technical standards that* should *be implemented in order to* support the development of a reliable and seamlessly interoperable battery passport system. It aims to assist *the key stakeholders of the battery passport* system, including economic operators, data providers across the value chain, regulatory authorities (especially market surveillance and customs), government agencies (for assessing the impact of policy decisions) and, last but not least, data consumers (e.g. recycling companies). Furthermore, this document is intended to *be valuable for the standardisation processes* related to DPP, both as required by European Regulations and within the global context.

What can readers expect to gain from this document?

Comprehensive overview of technical standards: The document will provide an overview of the scope of the technical passport system, encompassing value chains, necessary technical specifications to enable interoperability, data flows, and responsibilities. This includes the interface between the passport data as defined in the Content Guidance and the technical passport system. Employing a comprehensive framework, it will offer a complete set of technical standard categories to facilitate the assignment of existing and forthcoming standards. In conjunction with external work on DPP, suitable technical standards will be identified and presented. By defining the correct scope, the framework for technical standards and the standards themselves, the document will contribute to clarifying the procedural and organisational complexity mentioned in chapter 0.

Support of the main stakeholders: The document will address the key technical elements required for the implementation and utilisation of the battery passport and its data. Depending on their roles, stakeholders will be able to identify the necessary business processes, technical responsibilities, technical standard categories as well as potential candidates for standards. These are essential for participation in the battery ecosystem. Furthermore, the technical requirements will serve as a validation foundation to plan the technical passport infrastructure, services and processes, tailored to individual stakeholder groups.

Support of standardisation process: Given the complex situation discussed in chapter 1.2 and 1.3, this document will contribute to the upcoming standardisation efforts in developing harmonised European Norms (hEN) for the DPP system in the JTC24. This will be achieved by providing a guideline with principles and criteria to assist the standardisation process. The document will identify gaps, overlaps, assess the maturity and readiness of the existing standard landscape, and identify ready-to-use standards and major interoperability issues. Based on this analysis, it will offer an in-depth understanding of the most critical interoperability challenges and propose approaches to address these contingencies while adhering to the principles of creating open standards, as mentioned earlier.

Scope

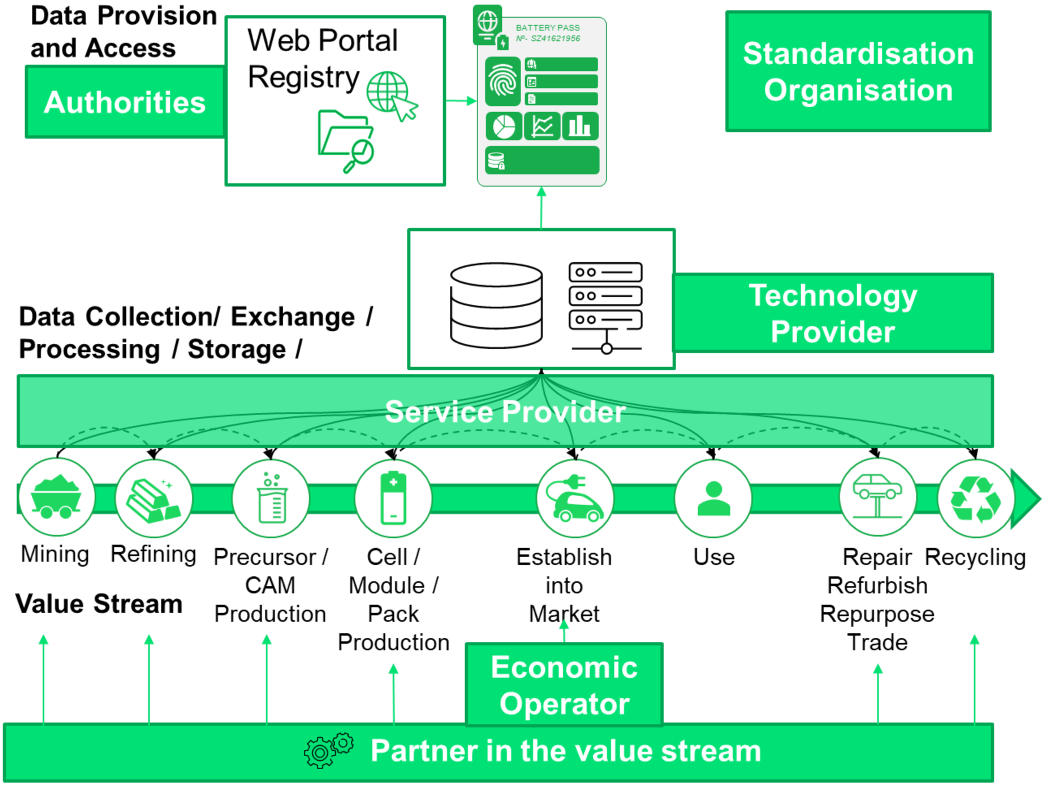
In this document, we address an interoperable system architecture for the DPP system, necessary to support the user stories of the battery passport operation and to enable the required management procedures around operations. Furthermore, the major architectural elements and their functions for executing the user stories are specified. An analysis of existing standards, reflecting their capabilities for reliable and future-oriented fulfilment of functional requirements will lead to a comprehensive map of existing and required technical standards for the entire DPP system. This document will be grounded in the specific standards outlined in the SReq, which aims to develop hEN for defining the DPP system, as required by the Eco-ESPR and the Battery Regulation.

Target audiences

The value chain of a battery defines the initial scope of the organisations affected by the battery passport (see Figure 4). Major upstream processes, such as mining and refining, as well as cell and module production, are carried out by dedicated supplier roles. Suppliers are required to provide data, such as greenhouse gas emissions of their parts and materials, or certificates. The economic operator placing a battery on the market is responsible for collecting and processing this battery passport information.

Other organisations are involved around the value stream. These include technology and service providers supporting the economic operator, as well as authorities that might need to use aggregated data, such as customs and market surveillance. Technology providers are responsible for reliable and functional technical components, such as data storage systems or application programming interfaces (APIs) for data exchange. DPP service providers are responsible for the operations of the DPP system, either overseeing an economic operator, setting up and maintaining the DPP system infrastructure, providing and updating DPP data and policies, or handling DPP system components that need to be managed by the European Commission, such as the EC User web portal and the Registry.

Figure 4: The EV battery value stream and the related targeted audience


Data Provision and Access
Authorities
Web Portal
Registry
BATTERY PASS
Nº- SZ41621956
Standardisation Organisation
Data Collection/ Exchange / Processing / Storage /
Technology Provider
Service Provider
Mining
Refining
Precursor / CAM Production
Cell / Module / Pack Production
Establish into Market
Use
Repair Refurbish Repurpose Trade
Recycling
Value Stream
Economic Operator
Partner in the value stream

Furthermore, *standardisation organisations and individuals* involved in standardisation activities are addressed by this document.

Table 2: Targeted audience

Targeted Audiences	What can be found in the document
Responsible economic operator (EO)	- User stories to be implemented - Specification of the DPP system architecture and its elements - Consideration of alternative technologies for implementation
Supplier and partner in the value stream	- Interface specifications that may be useful for seamless interoperability
Technology provider	- Same as economic operators - Interoperability challenges and specifications
Authorities	- User stories related to interactions with authorities to be implemented - Specification of the DPP system architecture and its elements, with a special focus on elements under the responsibility of authorities
Digital product passport service provider	- Same as economic operators - Interoperability challenges and specifications
Standardisation organisation	- DPP system architecture - Interoperability challenges and recommendations

2 The technical battery passport system in a nutshell

The Digital Product Passport (DPP) will become a reality no later than February 18, 2027, when every new electric vehicle battery, light means of transport battery, and industrial battery above 2 kWh will require the operation of such a system. The digital battery passport will serve as a pilot for DPPs and will be relevant for most industrial sectors in the coming years. Unlike many other regulations, the technical infrastructure, procedures, and the business and economic environment must be established as prerequisites for the digital operation of DPPs.

2.1 Major business and technological challenges for the DPP system

Establishing standards is never easy, due to specific business interests, the need to consider and integrate existing applications, and anticipate future developments. In the case of DPP, the following major business and technological challenges make the development of standards for the setup of the DPP system an extraordinarily complex task.

Complete interoperability: Various stakeholders, including consumers, business partners from different sectors and authorities must be able to access and maybe even exchange distributed and potentially highly sensitive data in a secure and reliable manner. This necessitates a full spectrum of interoperability aspects encompassing technical, organisational, and semantic interoperability, in compliance with various sector-specific regulations and conditions. Therefore, there is a need for a comprehensive and formal system specification for highly automated procedures, which should cover the necessary technical, organisational, and semantic elements. This specification should aim to be as inclusive as possible, allowing for the integration of various existing technical systems to minimise changes and operational costs.

Complex legal and business environment: From a legal perspective, fulfilling requirements stemming from various regulations across different sectors and legislative periods is a complex challenge. The battery passport system, in particular, is subject to compliance with two different regulations: the ESPR with its corresponding standardisation request for the DPP system, and the Battery Regulation, which share some conflicting requirements. Additionally, future regulations, such as the End-of-Life Vehicles (ELV) Regulation, and global regulations from regions like Asia and the US, may also impact the system design. Given the expected technological advancements in batteries, the emergence of new business models, and the significant market influence, the technical standards for the DPP system must be designed to accommodate future developments.

Tight timeline constraints for elaborating standards: Harmonised European Norms (hEN) will be developed to fulfil the SReq, based on ESPR and the Battery Regulation. In the field of data access and exchange regarding products and organisations, there are numerous partially overlapping and even contradicting standards. However, some standards are still missing. Given the traditional standardisation methods and the associated time constraints, meeting the December 31, 2025 deadline presents a significant challenge. Therefore, we must adopt innovative approaches to streamline the standardisation process. In addition, also government and industry sectors must employ innovative approaches to implement standards effectively.

2.2 The fundamental parts of the technical guidance

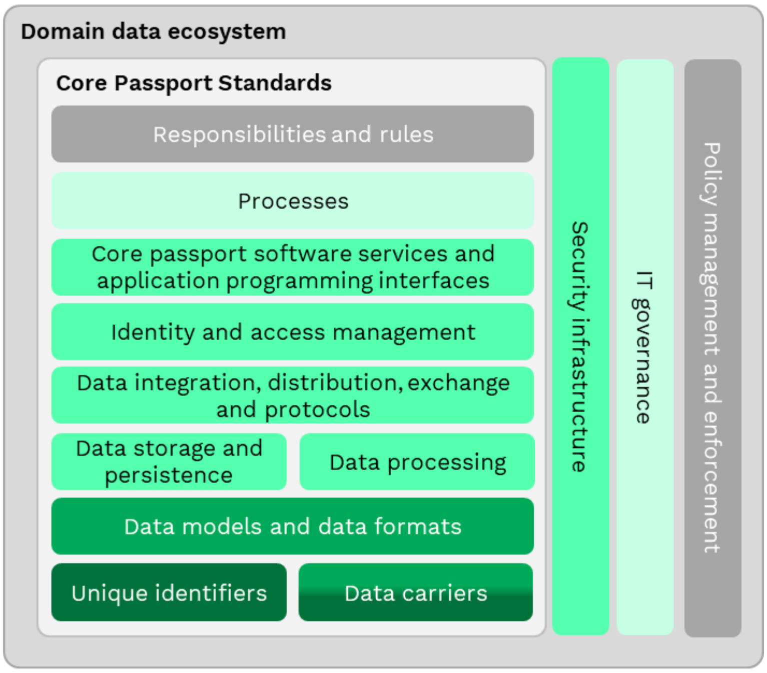
As background to the aforementioned challenges, the specification proposal for the technical standards of the DPP system comprises four fundamental parts:

1) The **Technical Standard Stack** for a comprehensive operational system based on existing frameworks to provide a complete and modular perspective on the standards that need to be established and harmonised.
2) **System architecture** with interconnected components fulfilling the standards derived from the Technical Standard Stack to enable automated data provisioning, exchange, and access processes.
3) **Interoperability challenge description** is a proposal aimed at facilitating the seamless integration of various technologies already in use in the market while ensuring that the DPP system remains as open as possible to accommodate global and future developments.
4) **Guideline to assist the industrial stakeholders** in preparing for their responsibilities within the specified time frame.

2.3 Introduction to the Technical Standard Stack

The Technical Standard Stack (see Figure 5) consists of essential technical standard building blocks that need to be integrated. These include IT infrastructure, (distributed) software functions, management systems, and governance systems. These components collectively lay the groundwork for achieving a range of critical objectives, with a primary focus on facilitating safe, secure, and cost-effective passport operations.

Figure 5: Technical Standard Stack

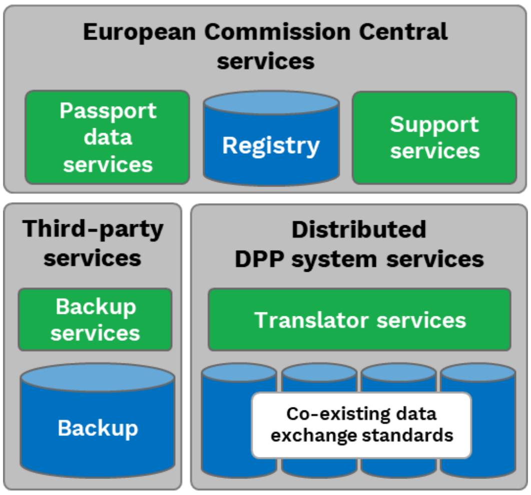

Domain data ecosystem
Core Passport Standards
Responsibilities and rules
Processes
Core passport software services and application programming interfaces
Identity and access management
Data integration, distribution, exchange and protocols
Data storage and persistence
Data processing
Data models and data formats
Unique identifiers
Data carriers
Security infrastructure
IT governance
Policy management and enforcement

These technical components are divided into parts from the perspectives of data, services and processes as defined by the Enterprise Interoperability Framework in ISO 11354. See chapter 4 for a detailed description.

2.4 System architecture

The recommended principal system architecture (Figure 5) is divided in the three major service-oriented components: the EC Central services, the distributed DPP system services and the third-party services. The EC Central services are under the responsibility of the European Commission and the distributed DPP system services must be established and operated by the economic operator or by a service provider in charge. The third-party services must be established, mandatorily by a certified independent third-party product passport service provider. This is a mandate according to the current ESPR Regulation, specifically for the data backup service. Additional third-party services might be necessitated by other regulations. The distributed DPP system services require translator services providing functionalities that handle the conversion of data across various formats or standards in the distributed system ensuring the co-existence of different data exchange standards.

Figure 6 Principal system architecture



2.5 Interoperability challenges

The following summarises the primary challenges in developing the battery passport system, emphasising the need for attention and focus from all stakeholders. Key areas include:

1) **Application of different data carriers:** The choice between QR codes, as specified by the Battery Regulation, and alternative smart labels like RFID or NFC tags. The challenge lies in the QR code's static nature versus the evolving data of digital product passports. Solutions such as dynamic linking mechanisms need to be explored to ensure QR codes can direct users to up-to-date DPP information.
2) **Unique identifiers:** Establishing unique identifiers (UIDs) is essential for the battery ecosystem, requiring the accommodation of diverse identifiers used by economic operators. The goal is to avoid unnecessary duplication and potential ID collisions.
3) **Routing to different distributed DPP systems:** A flexible routing mechanism within a decentralised data system is crucial to ensure access to the correct and current economic operator data repository, especially when responsibilities shift or operators cease to exist.

4) **Application of different data management technologies:** Achieving full cross-sectoral interoperability poses a significant challenge. A federated approach to standardised data exchange is recommended, allowing for diversity in standards across different industries while maintaining interoperability.
5) **Secure and reliable supply chain data acquisition and exchange:** Supply chain transparency systems are vital for tracing the flow of products, materials, and information. Standardisation in data, communication, and identifiers is necessary to integrate upstream value chain data with the battery passport effectively.
6) **Seamless and secure provision of access to different stakeholder groups with sector-specific policies and rules:** Implementing secure and reliable access control mechanisms, integrated with sector-specific policies and rules, is imperative. This includes ensuring data protection and sovereignty to maintain trust in the decentralised data system.
7) **Cross-domain interoperability:** Interoperability across different data spaces requires harmonising data formats, standards, and governance models. Collaboration among stakeholders is essential to address the diverse challenges of data integration across domains.
8) **Connectivity for dynamic data acquisition:** Ensuring the battery passport's information remains accurate and up-to-date is challenging, especially with potential connectivity issues. Regulatory mandates for dynamic data provision need to be considered to mitigate risks associated with data gaps.
9) **Alignment global DPP initiatives:** The global importance of batteries necessitates common content and technical standards for DPPs. Initiating a joint work program under ISO Level for interoperability and collaborating with international standards institutions is suggested.

2.6 Guideline for supporting the industrial stakeholder

Below there are major guiding proposals provided for industrial companies affected by the DPP regulations and specifically by battery passport issues (this is not only related to economic operators but also to other companies involved in the physical and information value chain):

- **Decide on the business model and technical strategy for “make-or-buy”.** A business and technical due diligence of existing data and infrastructure can serve as a solid foundation for this decision. The technical guidance can be used as a checklist for implementing technical specifications, requirements, and provides useful hints.
- **Decide whether to join or expand into one or more data spaces.** Data spaces enable efficient, secure, and standardised data sharing and transactions within an ecosystem by providing a technical infrastructure based on a governance framework. In the context of the digital product passport across different sectors, data sharing is one of the most crucial aspects. It impacts key business concerns such as your business models, protection of intellectual property, trade secrets, and even technical and business operational processes. Therefore, businesses must establish or maintain their business, organisational, and technological capabilities simultaneously.
- Even though the standardisation of technical aspects may take until the end of 2025, **companies should actively follow and contribute to the standardisation process**. This is especially important for economic operators since the adoption of already applied technologies and procedures should be implemented as simply and cost-effectively as possible.

Later in the document, guidance is provided for organisations involved in standardisation, government entities, and IT service providers.

3 Methodology Framework

The purpose of this chapter is to provide a suitable and comprehensive technical framework for the digital product passport system. It begins with an introduction to the requirements defined in the current SReq for a DPP system based on ESPR and the Battery Regulation. A comprehensive examination of the use cases of the battery passport system will shed light on the application of the components of the DPP system throughout the passport's life cycle.

For analytical purposes, two interoperability frameworks (the Enterprise Interoperability Framework and the European Interoperability Framework) are introduced to offer perspectives on completeness and systematics. Furthermore, in today's context, interoperability is closely linked to the concept and ecosystem of data spaces. Essential aspects of data spaces in the context of DPP will be presented to facilitate the creation of a comprehensive system specification.

3.1 Base – standardisation request on the DPP system

3.1.1 Introduction into the standardisation request

As mentioned in the introduction, the standardisation request (SReq) serves as the baseline for the development of the technical guidance. This decision is based solely on the relevance and impact of the regulation and standardisation, particularly in the context of circularity in general and specifically for the digital product passport (DPP). The current SReq clearly states: "Products may only be placed on the market or put into service if a digital product passport ('product passport') is available in accordance with delegated acts to be adopted under the future Regulation." Additionally, the SReq outlines the objectives, scope, and fundamental requirements for the DPP System.

The following are the eight modules of standards that must be developed by CEN, CENELEC, and ETSI, as outlined in the SReq:

- **Module 1 - Unique identifiers:** This module ensures that each identifier is unique, meaning that the same identifier cannot be assigned to different products, different economic operators, or different facilities. The identifiers should cover all levels of granularity as mentioned in the ESPR (Item, Batch, Model).
- **Module 2 - Data carriers and links between physical product and digital representation:** The module requires the definition of common rules for how to construct the automatic identification and data capture (AIDC) media to be used as data carrier linked to the product passport. The data carrier should act as a reference to both, the public and the restricted DPP data and should also include control data elements for the verification of authenticity of the data carrier and the product itself. Offline capability for data provision may also be included.
- **Module 3 - Access rights management, information system security, and business confidentiality:** This module ensures that organisations, individuals, machines, and services have recognised identities. It provides access control measures to regulate access to restricted product information. Additionally, rules for ensuring IT security, cybersecurity, data protection, and the transfer of responsibilities, access rights, and data from one economic operator to another must be defined.

- **Module 4 - Interoperability (technical, semantic, organisational):** The standards should provide a solution for the semantic description of a product, using a common information model and metadata models and formats for representation and exchange.
- **Module 5 - Data processing, data exchange protocols and data formats:** These standards must establish protocols and rules for exchanging data between partners, as well as processes for introducing, modifying, and updating information in the passport.
- **Module 6 - Data storage, archiving, and data persistence:** These standards define rules for decentralised data storage, archiving, and data persistence. The archiving service securely stores historical passport data, preserving a comprehensive record of past information.
- **Module 7 - Data authentication, reliability, integrity:** This module should define open and interoperable methods between automated identification services and data carriers to read data, verify data originality, and ensure data integrity in offline and online use cases.
- **Module 8 - Application programming interfaces (APIs) for the DPP life cycle management and searchability:** APIs must be established to automate the management of digital product passport data throughout its life cycle and to facilitate remote queries from the digital product passport registry or applications from national authorities.

Additionally, the SReq defines interoperability requirements with a focus on interoperability across various technical systems, platforms, products, industry sectors, and regulations. The aim is to ensure independence from any technology and service provider and to avoid monopolies, allowing for technological progress and cost-effective DPP system implementations and operations.

The SReq defines the scope of interoperability across different technical systems and platforms, including data storage and management, unique identifiers already in use in the market, and data carriers. These provisions should enable the safeguarding of investments made by companies and entire ecosystems.

Interoperability across products, industry sectors, and regulations addresses two complementary aspects. Firstly, there is a single technical system specification for DPPs intended to encompass all regulated industry sectors. To achieve this, the DPP system must be adaptable to cover sector-specific passport data models and rules for the management of information and access rights. Secondly, the interconnection of passports from different sectors, such as those of a car and a battery contained in a car, needs to be established.

Crucially, the entire ecosystem requires independence from specific technologies. Due to the significance of the DPP system, it aims to prevent monopolies, allowing for technological progress, and ultimately ensuring cost-effective DPP system implementations and operations.

3.1.2 Identified major technical components of the DPP system

In the following Table 3 the technical components of the DPP system are listed according to the requirements of ESPR, Battery Regulation and standardisation request on DPP system.

Table 3: DPP system components as required by SReq, ESPR and Battery Regulation

DPP – System Components as defined in the SReq	Type of Component	Reference to SReq, ESPR, Battery Regulation
Unique identifier for product, economic operator, facilities and DPP unique identifier	Alphanumerical Code	Module 1 of SReq, ESPR version Post-meeting Version of Technical Meeting on December 15, 2023, Article 11(4a)
Data carrier	Medium holds the unique identifier with link	Module 2 of SReq, ESPR version Post-meeting Version of Technical Meeting on December 15, 2023, e.g. Article 11(4a)
Registry	Database	ESPR version Post-meeting Version of Technical Meeting on December 15, 2023, Recital 34
EC User web portal	Software	ESPR version Post-meeting Version of Technical Meeting on December 15, 2023, Recital 34a
Individual distributed data repository	Database	ESPR version Post-meeting Version of Technical Meeting on December 15, 2023, Recital 103a, Module 3 of SReq
API for CRUD of data	Software	Module 8 of SReq
System for access rights management	Software	Module 3 of SReq
Verification of authentication	Method	Module 7 of SReq
Verification of DPP conformance	Method and software	Module 7 of SReq
Data verification of data integrity and originality	Method and software	Module 7 of SReq
Logging and monitoring	Method and software	Module 7 of SReq
Querying of passport data	Method and software	ESPR version Post-meeting Version of Technical Meeting on December 15, 2023, Article 9(1), Module 8 of SReq
Back-up service	Software	Module 6 of SReq
Data modelling	Method	Module 5 of SReq

3.1.3 Process scope and user stories

Based on the definitions provided in the SReq and through joint discussions with the CIRPASS project, the table below outlines the user stories that must be covered by the technical DPP system. The user stories are defined by a user story group (e.g. passport management cases for economic operators), a general business use case (place a battery on the market), examples of technical procedures (e.g. equipment manufacturer creates a unique identifier), and the relevance for the mentioned major technical components of the DPP systems as defined above in Table 3 and the process scope as indicated in Figure 4.

Table 4 User story overview

User stories	Example / Partial Case	Affected Technical components	Process Context as defined in Figure 4
Passport management for economic operators			
Place a battery on the market	Equipment manufacturer creates a unique identifier and other mandatory battery-related attributes	• Unique identifier • Data carrier • Registry • Individual data repository • API for CRUD of data • Access rights management • Verification of authentication	Prepare for selling the battery
Transfer the responsibility from one economic operator to another	Inform former economic operator when a new passport for a refurbished battery is created by the new operator		Refurbish process
Delete the battery from the market	Change status of battery Update data for created recycled content Set organisation identifier for recycling organisation		Recycling
Passport data operation			
Updating passport data	Update a set of or individual data points	• Individual data repository • API for CRUD of data • Access rights management • Verification of authentication	Use
Request data from a certain passport	Check credentials of requester Check validity of requested UID of battery Send request to registry Send request to data source (website)		Market placement (re-) use Repair, Repurpose Recycle Buy a battery
Backup passport data	Send passport data to the data base of the external battery passport system service provider		Use
Monitoring and analyses cases			
Market surveillance check	Check: Batteries, where faulty certification issuer had provided certificates for supply chain due diligence Search for passports	• Unique identifier • Data carrier • Registry • Individual data repository • API for CRUD of data • Access rights management • Verification of authentication • Querying of passport data	Use
Impact analysis cases	Data aggregation: e.g. average percentage of recycled material for NMC batteries in use Queries across the entire passport data sets coming from all products		Use
Eco-system validation	Plausibility check: Percentage of certified critical raw material for		Use

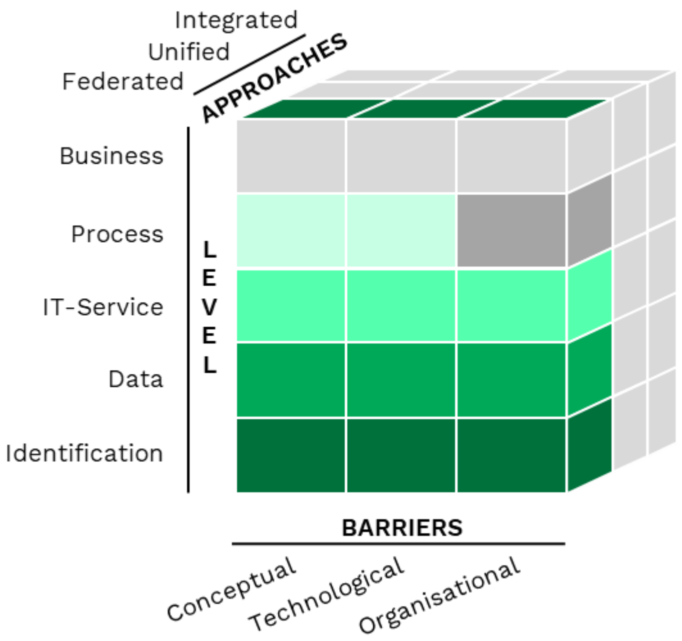
User stories	Example / Partial Case	Affected Technical components	Process Context as defined in Figure 4
	each battery against total produced certified critical material.		
Establish and manage the organisation and technical passport system			
Create and update technical standards	Introduce additional accepted IT governance standard	• Access rights management • Verification of authentication	Monitoring measures
Create and update data model	Add a new parameter into the mandatory battery passport. Update validation rules (e.g. the accepted range of recycled content)	• Registry • Individual data repository • API for CRUD of data • Data modelling	Monitoring/ measures Issue battery passport
Establish and operate registry services	Setup a registry Monitor registry services	• Registry	Registry
Onboard and govern service provider	Check organisation Check certification Provide accreditation	• Access rights management • Verification of authentication • Querying of passport data	Accreditation

3.2 Used concepts from interoperability frameworks and data spaces

3.2.1 Enterprise interoperability framework

The enterprise interoperability framework as defined in ISO 11354-1:2011 [5] is based on overcoming technical, conceptual and organisational barriers in order to map and structure interoperability problems and solutions in accordance with the relevant enterprise levels. The enterprise interoperability framework spans various levels (see Figure 7), each vital for achieving seamless collaboration and efficiency. At the business level, the focus lies on harmonising organisational aspects like work methodologies, legislative adherence, and cultural nuances. This ensures that diverse entities within an enterprise function cohesively. The Battery Pass consortium has left out the business level, since it only plays a subordinate role for the technical consideration of the battery passport system. The process level entails connecting the internal workflows of two distinct companies to establish a unified and streamlined operation. This collaborative effort enhances the efficiency of the combined processes. In terms of IT services, the challenge involves identifying and composing independently crafted IT services. By seamlessly integrating these services, enterprises can create a more comprehensive and cohesive technological landscape. Data interoperability addresses the need to harmonise data formats and models across heterogeneous data sources. This effort facilitates the efficient sharing and retrieval of information, overcoming the barriers posed by disparate data sources. A significant aspect of interoperability involves identification – establishing unique identification methods for products, organisations, and facilities along the entire value chain. Identification is not described as a separate level in the framework, but the consortium has decided to include this aspect due to its outstanding importance and to expand the framework accordingly. [6]

Figure 7: Extended enterprise interoperability framework



Enterprise interoperability encounters several barriers that must be overcome to ensure smooth collaboration and efficient operations. Conceptual barriers arise from differences in the way information is expressed, both syntactically and semantically. Addressing these disparities is essential to ensure that exchanged information is correctly understood and utilised by all parties involved. Technological barriers stem from the incompatibility of information technology systems. These barriers manifest in challenges related to the presentation, storage, exchange, processing, and communication of data. Bridging these technological gaps is crucial for establishing a cohesive and integrated technological environment. Organisational barriers encompass the definition of responsibilities and authorities within the enterprise ecosystem. Clarity regarding who is responsible for specific tasks and who possesses the authority to make decisions is fundamental for coordinated efforts and effective decision-making. [6]

To achieve interoperability, there are three primary approaches: integrated, unified, and federated. Each of these approaches offers a different method for standardising data exchange, catering to the varying needs of participants within a data space.

The integrated approach mandates that every participant uses the same payloads and infrastructure. This means that for communication and data exchange to occur seamlessly, all entities involved must adopt the same software and technical frameworks. Essentially, it's a "one size fits all" model, where all participants agree on a common software stack for all communications. While this can ensure a very high level of compatibility and streamline processes, it can also be restrictive. Organisations may need to overhaul their existing systems to align with the chosen integrated solution, which can be both costly and time-consuming.

In contrast, the unified approach requires every participant to exchange data using the same payloads, though they are allowed to have their underlying infrastructure differ. This model prioritises a common data format across the entire data space, such as the Asset Administration

Shell (AAS) in industrial contexts or NGSI-LD in smart city or cross-domain contexts. The emphasis here is on standardising the "language" of data exchange, while giving entities the flexibility to maintain their existing hardware and software environments. This can reduce the burden of transitioning to a new system, as participants only need to ensure their data outputs match the agreed-upon format.

The federated approach offers the most flexibility among the three. Participants must ensure that the data they offer can be interpreted by a standardised meta-model, but both infrastructure and payload formats are only loosely restricted. This approach acknowledges the diversity of standards across different industries, allowing participants to offer their preferred, compliant exchange format. The federated model supports the idea that what is considered a "de facto standard" in one industry may not apply to another. Thus, it lowers the barrier to entry, as digital product passport (DPP) participants are not forced to adopt an unsuitable data exchange standard just to join a data space. In this approach, interoperability is cultivated through dynamic adaptation. Translator services in conjunction with canonical data models play a key role ensuring every participant translates its data into a single, common model.

The federated approach is particularly important in fostering inclusivity within data spaces. It recognises the varying needs and existing systems across different sectors, offering a way to participate without necessitating significant changes to internal systems. By allowing entities to use their preferred formats and standards, providing they adhere to a common understanding or canonical data model, it encourages broader participation. This inclusivity is crucial for initiatives like DPP, which aim to bring together diverse stakeholders from different domains and continents to share and manage product information efficiently. [6]

3.2.2 European interoperability framework

The European interoperability framework (EIF) is an initiative of the European Union (EU) that aims to promote interoperability in the field of information and communication technology (ICT) within the EU member states. The EIF provides principles, guidelines and recommendations to ensure that public administrations in EU member states design their ICT systems and services to interact well with each other and with citizens as well as the business community. It sets standards and guidelines for open standards, data exchange, security, interoperability architecture and other aspects of ICT system development as well as principles to evaluate (i.e. openness, technological neutrality and data portability, security and privacy) existing standards and solutions. [7]

The framework aims to improve collaboration and data sharing among government agencies in EU countries while facilitating efficiency, transparency and service delivery to citizens and businesses. It aims to reduce the fragmentation of ICT systems in different countries and support the creation of a digital single market in the EU. The European interoperability framework has gone through various versions to reflect current developments in ICT and the digital society. It is an important tool for ensuring that the ICT infrastructure of the EU member states is compatible with each other and enables seamless interaction between different systems. [7]

Based on this analysis a set of critical interoperability issues is derived. Those critical interoperability issues are explained in detail in chapter 6, including recommendations for solutions, when available, or approaches how to achieve improvements.

3.2.3 Battery passport in the data space environment

According to the “Data Spaces Support Center” [8], a data space provides an infrastructure that enables data transactions between different data ecosystem parties based on the governance framework of that data space. Data spaces should be generic enough to support the implementation of multiple use cases.

In the context of DPP in general and specifically for the digital battery passport the following aspects need to be considered:

- Common components specifications
- Common interface specifications
- Rules for system applications
- Governance framework
- Trust framework

DPP system components as listed in Table 3 are required to build the battery passport technical infrastructure. Other aspects of data spaces will be covered in subsections of chapter 6.7.

3.3 Standardisation request analysis results

The current SReq is generally based on the provisions found in the ESPR and the Battery Regulation. Additionally, some feedback and recommendations from the standardisation work have influenced this chapter. In total, the interoperability aspects required by ISO 11354, from data, IT services, processes, and business perspectives, are comprehensively covered. Although the EIF is not explicitly mentioned in the SReq, most of the relevant recommendations are partially addressed. In Table 5 below, the EIF defines how the recommendations relevant for DPP system are covered by SReq, ESPR and Battery Regulation.

Table 5: Analysis of SReq, ESPR and Battery Regulation against the principles of EIF

EIF recommendation (Re), relevant for DPP system	**How EIF are addressed in the modules of standardisation request, ESPR and Battery Regulation**
Accessibility (Re1)	Generally mentioned in Module 3 (Access Rights), web portal as defined in ESPR, no specific requirements defined
Considering the specific needs in the context of privacy and security, especially in the context of public registries (Re2, Re11)	Generally mentioned in Module 2 (Data Carrier), Module 3 (Access Rights Management) and Module 8 (API), no specific requirements defined
Long-term preservation policy for electronic records relating to European public services (Re3)	Addressed in Battery Regulation
Provide Multilingualism (Re4)	Generally addressed in Article 1 of SReq
Technological neutral solutions (Re8)	Generally addressed in Paragraph 19 of SReq, but technology specific solution demanded, e.g. Battery Regulation (QR code for data carrier)

Provide an open (Re22) reusable formalised (Re19, Re20, Re21) component-based service model and a common scheme for connecting services (Re7, Re9, Re10) and using a common taxonomy (Re13)	No service model defined, No reference to reuse existing public service, No scheme defined, no formalism provided or requested
Simplification and transparency of administrative processes including change management (Re15, Re16, Re17)	Administrative processes not addressed yet
Define interfaces to authentic sources (Re12)	Not addressed formally
Support sector-specific and cross-sectoral communities (Re18)	Not addressed formally

3.3.1 Major obstacles based on analysis

There are three major obstacles based on the analysis concerning the EIF:

- Lack of a formal specification for system architecture, system components, and interfaces between the components. These components must be defined in such a way that there is no room for interpretation. This is crucial because the components need to be designed and operated by different stakeholders while also interacting automatically.
- Absence of a specification for the operations model governing the establishment, operation, and maintenance of the DPP system. This includes business and technical processes, IT governance, and transparent specifications for management responsibilities and rules. The ESPR mentions that specifications related to the operations model will be provided in legislative acts at a later stage. This represents a significant weakness since the technical system must be designed in accordance with these specifications.
- Lack of defined specifications for handling various data models and formats required by sector-specific regulations and standards within a single system. This also extends to the implications for procedures, rules, and responsibilities that need to be provided or supported by the technical system.

Furthermore, there are the following major technical contradictions created by ESPR, Battery Regulation, and SReq that need to be resolved:

- There are contradictions between SReq and ESPR, as well as between the modules of SReq and Battery Regulation. For instance, the Battery Regulation requires a QR code, while the ESPR mandates the inclusion of data carrier types that already exist in the market. Being in the market doesn’t necessarily mean adapted by every sector. This is particularly relevant in the automotive industry, where Data Matrix instead of QR codes, especially for batteries, are widely used.
- The data carrier should contain a dual link to both public and restricted data. Currently, the provision of dual links from a single data carrier is not a standardised practice. Here, alternative solutions should be considered. Additionally, the SReq and the ESPR require the provision of offline data while avoiding the need for additional apps to read the data carrier. Reading specific offline data would necessitate a dedicated app. The same issue arises for standardised look-up mechanisms.

- The SReq and the ESPR require the possibility of queries across all passports for specific attributes. Given the substantial amount of data stored in decentralised systems, the performance and effort involved in searching must be investigated.

3.3.2 Required additional system components

Based on the analysis of ESPR, Battery Regulation, and SReq, several additional system components should be required to ensure the complete functioning of the system:

- **Data reporting services**: The need for data reporting, as defined in the Battery Regulation, requires the capability to store aggregated data and perform analysis on both aggregated and individual passport data. Due to the vast amount of passport data, a fully decentralised approach may not be suitable. Therefore, data reporting services, exclusively operated by authorities, must meet specific content and security requirements.
- **Issuing services:** Specialised services are essential for economic operators to facilitate the issuance and registration of new digital product passports within the central registry. These services accommodate both bulk registrations and individual passport entities, requiring each to undergo a thorough validation and verification process by a dedicated service.
- **Validation and verification services:** To ensure completeness and formal and semantics validity of data, provided by the economic operator for issuing a new passport or for updating data, validation and verification services are necessary. Similar to that, verification of persons, organisations and facilities are required to be realised from a central perspective. Data validation services have to be developed and implemented in order to keep passport data reliable and trustworthy.
- **Routing services:** The routing services provide the correct link to the distributed passport data for the requesting audience while following access rights and exchange protocols.
- **EC Company service API:** In addition to the web portal as defined in the SReq and ESPR, several other APIs are required for data access and provision. This includes the EC Company service API for automated mass data feeding and updating.
- **EC Authority portal:** Authorities require additional API functions (e.g. for accessing data reporting services as mentioned above).
- **EC Operations portal:** The EC Operations portal supports the secure, reliable, and cost-efficient establishment, operation, and maintenance of the technical DPP system. This should encompass all IT operations services, as required by IT service management, like monitoring services for operations and ticketing services to support service management. Moreover, this should also cover administration services such as continuous data modelling services to keep the DPP data models up-to-date and policy management services for defining, establishing, and maintaining rules and conditions, e.g. for access control polices based on stakeholder groups.
- **Interoperability services:** These services address various aspects, including translator services for the provision of passport data from differently implemented distributed data sources.

3.3.3 Guiding principles for DPP system standards

Based on the analysis of the SReq, as mentioned above, the following guiding principles for the identification of standards going forward were defined.

Cross-sectoral global interoperability: As the battery passport is just one pilot application for DPP in total, and batteries are used not only in the automotive industry but also in various other regulated sectors, the technical standards should ideally be applicable across all these sectors. Furthermore, the battery industry heavily relies on global supply chains and contingencies. Therefore, a top-down approach must be followed. This implies the need to initially establish sector-independent standards at the ISO level and then harmonise them for the European Union. Simultaneously, consensus on technical standards must be achieved through collaboration with major stakeholders in America, Asia, and Africa.

Strive for inclusivity to the greatest extent possible: In certain areas, overlapping standards exist for various reasons. Standardisation efforts should focus on creating solutions and approaches that facilitate the coexistence of different standards, rather than aiming to select a single standard for the same purpose. Ideally, every stakeholder in the battery passport ecosystem should have the option to choose and adopt a suitable standard without encountering interoperability barriers within their ecosystem. This approach benefits both companies, as they can select standards with fewer openness and cost-related barriers, and allows for the reuse of previously implemented standards for battery passports without additional effort. Consequently, this principle calls for a modular passport system specification.

Reliability first: Given the complexity and limited prior experience, the digital product passport concept should be built upon existing mature standards that are widely adopted in the market. Additionally, standards supported by the existing European quality infrastructure (e.g. with existing certification authorities) should be favoured to ensure a more secure starting point.

Simplicity and cost-effectiveness of the entire system: To reduce organisational and process complexity, consider this principle for the entire life cycle of the technical battery passport system, including definition, implementation, operation, maintenance, and adaptability. This should be managed through a service operating system. The consensus of the Battery Pass consortium is to strive for a reliable and cost-effective system. Under this premise, the technical standard specification should be developed in a manner that:

1) Is easy to establish, operate, and modify.
2) Existing infrastructures (e.g. certification systems) can be reused.
3) Established system providers are readily available.

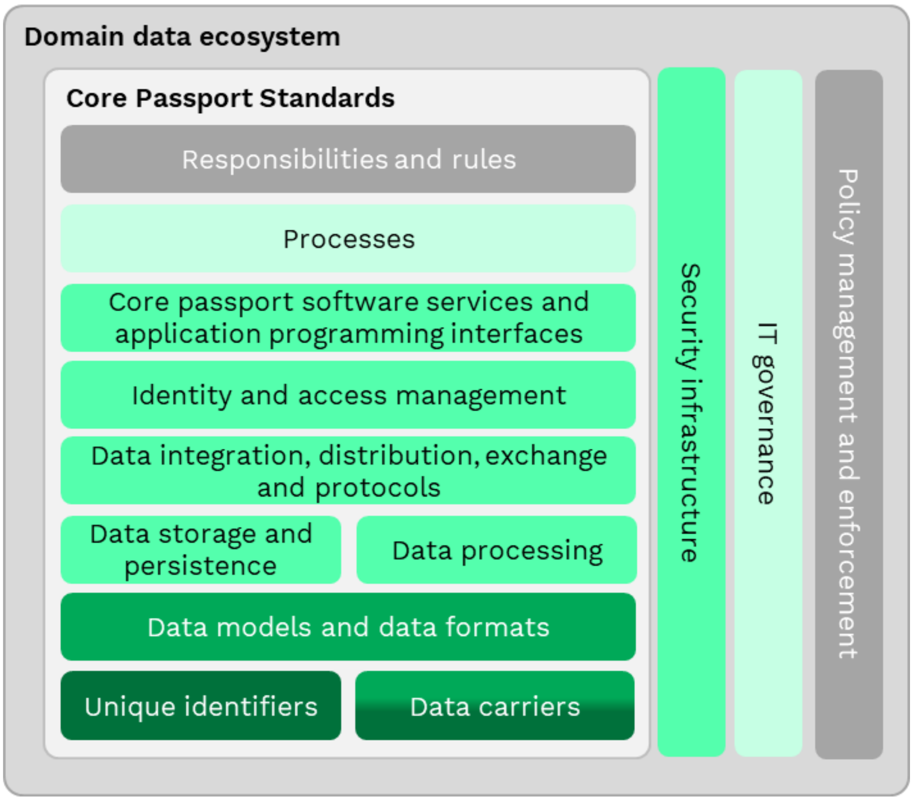
Extendability to support future envisioned development of the battery passport system, including the consideration of upcoming standards.

Fully open, transparent and balanced standardisation process: Given the significant business impact of technical standards for the battery passport, it is crucial to ensure that the standardisation process remains entirely transparent for all individuals and organisations. The various interests of stakeholders and system providers must be balanced to prevent the adoption of proprietary solutions. This entails establishing mechanisms, rules, and responsibilities to enforce technology-agnostic requirements.

4 Technical Standard Stack in detail

The Technical Standard Stack (see Figure 8) comprises essential technical standard building blocks that need to be integrated to form a DPP system. This includes IT infrastructure, (distributed) software functions, management systems, and governance systems. The assessment of these components and of their interaction paves the way for a range of imperative objectives, primarily focused on facilitating safe, secure, and cost-effective passport operations.

Figure 8: Top level view of the Technical Standard Stack


Domain data ecosystem
Core Passport Standards
Responsibilities and rules
Processes
Core passport software services and application programming interfaces
Identity and access management
Data integration, distribution, exchange and protocols
Data storage and persistence
Data processing
Data models and data formats
Unique identifiers
Data carriers
Security infrastructure
IT governance
Policy management and enforcement

The defined objectives for a DPP system encompass various critical tasks, such as performing data collection and exchange, ensuring the safe and secure storage of (distributed) passport data, processing and calculating passport data, provisioning passport and related data to eligible authorities, and verifying these authorities.

At the core of this framework is the capacity to establish a robust management system, a foundation that involves activities like setting up effective governance procedures, accrediting eligible authorities, and monitoring the technical progress of operations while implementing necessary setup measures.

Crucially, these desired capabilities are underscored by key principles. Among them is the reduction of dependencies among distinct components within the Technical Standard Stack, with modularity playing a pivotal role. In cases of technological advancements or shifts in demands, such as increased security requirements or specific regional data processing needs, changes to one component should not necessitate modifications across all other components.

Furthermore, comprehensiveness is essential, with the standards meticulously designed to cover all functional requirements arising from regulations. Formalisation of specifications is also crucial. To ensure smooth operations, all core passport standards specifications must be precisely defined and ready for implementation.

Only the domain data ecosystem specifies this approach for concrete product categories. This makes this comprehensive approach of the Technical Standard Stack not only suitable for battery passports but serves as a solid foundation for digital product passports in general.

In the following sub-chapters the components of the Technical Standard Stack are explained in more detail. This is accomplished by providing a definition, an explanation in the context of the battery passport, and the selection and recommendation of suitable standards. The standard selection process begins with the identification and classification of relevant standards, as listed in the non-exhaustive list provided by the SReq. The classification follows the guiding principles as outlined in sub-chapter 3.3, taking into account three aspects: a top-down approach from ISO standards to sector and local standards, consideration of mature standards already *widely applied* in the industry, and anticipation of *upcoming* standards.

In the context of technical standards, *widely applied* refers to those standards that have achieved a high level of popularity and acceptance in the industry. This popularity is often due to their effectiveness, reliability, and relevance to current technologies and practices. A key factor contributing to the wide usage of these standards is their backing by legislation; they are often incorporated into legal frameworks and regulations, which mandates their adoption and adherence. As a result, these standards become foundational in guiding industry practices, ensuring quality, safety, and interoperability across various domains. *Upcoming* standards are those in the process of development, recently released, or are part of ongoing research and development activities. These standards are not yet established as international ISO standards. They represent the cutting-edge in their respective fields and are in the stages of gaining recognition and acceptance. Their emergence is often driven by new technological advancements, emerging industry needs, or evolving regulatory requirements. These standards hold the potential to shape future practices and technologies once they gain wider acceptance and possibly become the norm. The following table defines the options for classifying standards in Backus-Naur-Form (BNF).

Table 6: Template for standard classification

Level	**Scope**	**Status**
<Global>I<Europe>I<National> <ISO or Mirror Level>I<De Facto>	<General>I<Sectorial>	<Widely Applied>II<Upcoming>

4.1 Domain data ecosystem

Definition

The domain data ecosystem describes the totality of DPP relevant data, in this case batteries, and their relationships to each other. Within this ecosystem, several important aspects converge to enable a holistic understanding:

Description in the context of the battery passport

Batteries operate within a dynamic regulatory landscape, and the governance of the domain data ecosystem ensures that the ecosystem remains up to date with the latest compliance requirements, safety standards, and environmental considerations. In the grand scheme of the domain data ecosystem, roles associated with batteries play a vital role. These roles help define the various stakeholders and their responsibilities within the battery passport domain. Whether it's economic operators, recyclers, regulators, or end-users, these roles provide clarity on who contributes to and who consumes battery passport data.

All of these components collectively contribute to the semantic model. This model acts as the unifying thread that weaves together all the aspects, serving as a common reference point for battery-related terms, definitions, and technologies. It doesn't merely encapsulate the present state of battery knowledge but also dynamically reflects the ever-evolving landscape of battery technology. As advancements continue to shape the industry, the semantic model will evolve with it and remains a beacon, ensuring that we have a shared language and understanding.

Selected standards evaluation

The domain data ecosystem is not covered by the SReq. This absence poses challenges when it comes to understanding and organising data within this context. There are two ontologies that offer a structured approach, particularly in the battery sector, though. These ontologies have been made available in Resource Description Framework (RDF), which is the recommended format for their publication (see chapter 4.9).

Table 7: Standards for domain data ecosystem

Standard	Classification L: Level, Sc: Scope, St: Status	Originator	Short Description
Battery Value Chain Ontology (BVC)	L: Europe, De Facto Sc: Battery St: Upcoming	Fraunhofer ISC	The Battery Value Chain ontology covers the processes along the battery value chain
BattINFO	L: Europe, De Facto Sc: Battery St: Upcoming	n.a.	BattINFO consists of a list of entities representing concepts used in batteries and electrochemistry

4.2 Responsibilities and rules

Definition

The responsibility describes the participation by various roles in completing tasks or deliverables for a project or business process. A business rule defines or constrains some aspect of a business. It may be expressed to specify an action to be taken when certain conditions are true or may be phrased so it can only resolve to either true or false. Business rules are intended to assert business structure or to control or influence the behaviour of the business. Both are fundamental aspects of business interoperability to clarify duties of different partners in an ecosystem. The responsibilities and rules are a basis for the policy management and enforcement component (see chapter 4.12).

Description in the context of the battery passport

In the intricate landscape of a complex IT system like the battery passport system, the concepts of responsibilities and rules emerge as pivotal cornerstones, safeguarding the integrity, security, and efficiency. While this building block doesn't delve into the definition of technical standards, it outlines the specific responsibilities and rules that various stakeholders are entrusted with, particularly in the context of managing life cycle business cases and addressing incidents.

One prime illustration of the significance of these responsibilities and rules arises when contemplating a change in the economic operator responsible for a battery passport. Such transitions must be executed seamlessly so that the continuity of service and data integrity are upheld. Equally paramount is the consideration of bankruptcy scenarios involving companies responsible for data within the battery passport system. In such unfortunate circumstances, it's imperative that the established rules come into play, offering a framework for managing data assets and ensuring that critical information remains accessible and secure. The rules, in this case, serve as a safeguard against the potential chaos that can ensue when data custodians face financial adversity. Furthermore, the maintenance of accurate and up-to-date data within the system is a non-negotiable facet of responsibility for all stakeholders. The battery passport system relies on precise data to operate effectively as any discrepancies or outdated information can have far-reaching consequences. The rules established in this context act as a regulatory force, compelling all parties involved to uphold the highest standards of data accuracy and currency. The specifics of responsibility and regulations are defined with varying degrees of formality within the ESPR, the Battery Regulation, and to some extent in the SReq. The standard for the definitions of responsibilities and rules are not described yet. The defined aim is to develop formalised standards.

Selected standards evaluation

Table 8: Standards for responsibility and rules

Standard	Classification L: Level, Sc: Scope, St: Status	Originator	Short Description
RACI Matrics for Responsibility definition in Projects and Processes	L: Global, De Facto Sc: General St: Widely Applied	n.a.	Classification Scheme and of Responsibilities
eXtensible Access Control Markup Language (XACML)	L: Global, De Facto Sc: General St: Widely Applied	OASIS	Declarative markup language for rule specification and access control

4.3 Processes

Definition

A process is a “set of interrelated or interacting activities” [9] that can be executed to realise one or more given objectives of an enterprise, a network or a part of an enterprise to achieve some desired end-result. There exists typically management, value stream, support as well as data and information flow processes.

Description in the context of the battery passport

The core value processes are the up- and downstream process along the value chain of a battery and its components. Because of the restriction in the ESPR and the Battery Regulation the battery passport originally does not cover the processes from mining to integration. Nevertheless, to understand characteristics of processes, contributing to the passport we cover the specifics as well. Support processes are the operations of technical and organisational resources, required for operating the DPP system. Because of the relevance in the technical battery passport business in addition, we separate **data and information flow processes** along and across the management, core value and support processes.

- **Management processes:** The major management processes for DPP system are resource management, business continuity management, performance management, risk, safety, security management and the engineering change management related to technical standards.
- **Core value processes:** These processes always touch and change material and physical goods. Here the types of processes can by separated into flow, batch and discrete processes. Discrete processes can be separated into mass, configured, individual, one-of-a-kind processes. Common process definitions as well as output specifications across sectors will help to define passport property systematics, e.g. necessary for data analytics, auditing and validation and verification of passport data (e.g. for logic verification of passport data).
- **Support processes:** For the battery passport system these processes are addressing the operations of IT systems (e.g. registries, passport platforms) and the provision of the organisational capacities.

Data and information flow processes: These processes are touching with observation, classification, analysis, control, feedback, transformation and aggregation. These aspects are addressed in particular in the sub-chapters: 4.4 Core passport software services, 4.6 Data integration, distribution, exchange and protocols, 4.8

Data processing.

Selected standards evaluation

There are no standards listed in the SReq, with relevance to processes.

Table 9: Standards for processes

Standard	Classification L: Level, Sc: Scope, St: Status	Originator	Short Description
ISO/IEC 20000-1 Service management system requirements	L: Global, ISO Sc: General St: Widely Applied	ISO/IEC	Provides the complete scope of process definitions and the outcomes for IT service management including IT security and support processes
eTOM Process Framework	L: Global, De Facto Sc: General St: Widely Applied	TM Forum	Defines a library of processes for IT

Standard	Classification L: Level, Sc: Scope, St: Status	Originator	Short Description
			services including a data model.
MESA model	L: Global, De Facto Sc: Manufacturing St: Widely Applied	MESA International	MESA model provide technology independent standard process specifications for manufacturing and manufacturing management
ISO / IEC 62264 series of standards for Enterprise-control system integration	L: Global, ISO Sc: Manufacturing St: Widely Applied	ISO/IEC	Provides the process specification for general value stream processes and its control mechanisms as well as data exchange specifications on all levels of production for discrete manufacturing
IEC 61512 series of standards for Batch control	L: Global, ISO Sc: Manufacturing St: Widely Applied	ISO/IEC	Provides the process specification for general value stream processes and its control mechanisms as well as data exchange specifications for batch processes
ISO 59014 Environmental management and circular economy: Sustainability and traceability of secondary materials recovering - Principles and requirements	L: Global, ISO Sc: General St: Upcoming	ISO	Alongside others, provides terminologies of circularity in respect to sustainability

With ISO/IEC 20000-1:2018, a comprehensive process framework is available to organise the entire management and support processes for the operations of the DPP system. It is widely applied and mature. Further on the process specification is the basis for IT governance as required in the respective components in the Standard Stack. The data model of eTOM can be used as reference for standard data type specifications for management and support processes. IEC 62264 and 61512 provide a widely accepted set of data models, applicable to a broad spectrum of products in both discrete manufacturing and the process industry. These data models can be utilized to standardise the required data for DPP across various industries. The MESA model can contribute as well for finding a joint terminology and generic data objects. The ISO 59014 provides a comprehensive process specification for circularity which can be used for the definitions of rules and logics for passport processes in the downstream (e.g. when changing the economic operator in case of refurbishing).

4.4 Core passport software services and application programming interfaces

Definition

Core passport software services are components for executing processes for establishing, updating, searching, viewing, verifying, validating and comparing of passports along their life cycle and across systems and organisations. An application programming interface (API) is a specific software for interacting between different software systems and users.

Description in the context of the battery passport

Central to the functionality of the battery passport system, and indeed all DPP initiatives, are its core services. These integral services provide the bedrock upon which the system operates, offering a range of essential functionalities that are indispensable for its operation. These core services could be, for example:

- **Onboarding services**: the system's onboarding service, including registration functionalities, serves as the gateway for entities (economic operators and stakeholders with legitimate interest to access restricted data) looking to become part of this ecosystem. It streamlines the process, ensuring that stakeholders can smoothly integrate into the system, thereby becoming active participants.
- **Issuing services**: Dedicated services play a crucial role for economic operators in enabling the creation and registration of new digital product passports in the central registry. Such services are designed to support the registration of passports in large quantities as well as the registration of single passport entities.
- **Update services:** To maintain the system's accuracy and relevance, the data update service is of paramount importance. It empowers stakeholders to keep their information up to date, reflecting the changes or updates that may occur over time.
- **Transfer services:** Transferring responsibilities and data from one economic operator to another is a complex task, and this is where the system's transfer service comes into play. It facilitates the seamless transition of responsibilities and data, ensuring that the handover process is transparent and efficient.
- **Archiving services:** Archiving a passport is yet another vital aspect of the system's functionality. The archiving service securely stores historical passport data, preserving a comprehensive record of past battery information. As defined in the ESPR, archiving passport has to be performed by a third-party DPP system service provider.
- **Search, view and compare services:** the stakeholder-specific search and view service caters to the diverse needs of various user groups, be it the public seeking for information or authorities like market surveillance agencies requiring specific insights. This customisation ensures that stakeholders receive relevant data and insights, enhancing their experience within the system. Compare services are seen outside the core passport services and should be implemented into the comparison context, e.g. in marketplaces.

To implement these services there is the need of the following components: software services on CRUD activities and query operations for searching information, data exchange formats and protocols as well as message handling and exchange. This chapter concentrates on the pure software services and CRUD activities between corresponding systems and organisations as well as roles. The other aspects are defined in the other sub-chapters of the Standard Stack.

To specify the functionality and how the core services can be invoked and interacted with, we recommend the use of a service definition language (SDL). An SDL provides a standardised way to define service interfaces, ensuring that services can communicate and interoperate seamlessly, regardless of the technologies used to implement them. Prominent languages are e.g. WSDL (Web Service Definition Language).

Selected standards evaluation

Because of latest developments, the Catena–X requirements and specifications as well as the best practice guide for API were included into the list. All standards relating to data formats were excluded, because they are the topic of the Standards Stack component 'data models and formats'. Query languages are not part of the current list. One prominent representative is mentioned in the following list as well.

Table 10: Standards for core passport software services and application programming interfaces

Standard	**Classification** L: Level, Sc: Scope, St: Status	**Originator**	**Short Description**
Web Services Description Language (WSDL)	L: Global, De Facto Sc: General St: Widely Applied	W3C	Provides a platform and protocol independent language for the definition of web services
SOAP Messaging Framework	L: Global, De Facto Sc: General St: Widely Applied	W3C	A lightweight protocol intended for exchanging structured information in a decentralised, distributed environment
WS-Business Process Execution Language (WS-BPEL)	L: Global, De Facto Sc: General St: Widely Applied	OASIS	Is an XML-based language for definition of executable business processes
NGSI-LD (Next Generation Service Interface-Linked Data)	L: Europe, De Facto Sc: General St: Upcoming	ETSI	NGSI-LD is an information model and API for publishing, querying and subscribing to context information
REST API	L: Global, De Facto Sc: General St: Widely Applied	n.A.	REST API is a general API style for accessing, send,

Standard	Classification L: Level, Sc: Scope, St: Status	Originator	Short Description
			update and delete of data
OpenAPI	L: Global, De Facto Sc: General St: Widely Applied	Open API Initiative	Builds upon on REST API without requiring access to source code
ACCESS TO BASE REGISTRIES, Good Practices on building successful interconnections of Base Registries ISBN 978-92-79-54899-4	L: Europe, De Facto Sc: General St: Upcoming	European Commission	Provides good practices for setting up registry services
Catena-X Passport Services, e.g. Model Certificate of Decommissioning	L: German, De Facto Sc: Automotive St: Upcoming	Catena-X	Contains the standards in Catena-X directly providing operations service for managing passports
Catena-X Onboarding Services, e.g. Business Partner Gate API	L: German, De Facto Sc: Automotive St: Upcoming	Catena-X	Contains the standards in Catena-X providing functions for onboarding of partners
SPARQL Query Language	L: Global, De Facto Sc: General St: Widely Applied	W3C	Query language for RDF, to express queries across diverse data sources

From a technical standardisation viewpoint, it is essential to develop modular, configurable services. These services should be capable of incorporating and reusing publicly available specifications by applying a universally accepted specification language. By using WSDL for the logical service definition and REST API using e.g. OpenAPI specifications this can be performed in a standardised way. From the core service perspective, current Catena-X standard service catalogue as mentioned in the table above is a good starting point for having a comprehensive service specification including the API. Because the data model specification of the standard stack is using an RDF-based approach (like Catena-X), the SPARQL for searching and querying is proposed as well.

4.5 Identity and access management

Definition

Identity and access management is a framework of business processes, policies and technologies that facilitates the management of digital identities and ensures that the right users, actors and stakeholders have the appropriate access to technology resources and data assets.

Description in the context of the battery passport

The relevant actors and stakeholders in a decentralised battery passport ecosystem shall be identified and granted access to information in line with their respective access rights specified in upcoming delegated acts by the European Commission. According to Battery Regulation (*Recital 124*, *Article 77(2b)*), there are three major groups of actors: a) the public, b) notified bodies, market surveillance authorities and the European Commission, and c) any natural or legal person with a legitimate interest.

All data that is not available to the public needs to be protected by access control components evaluating the securely identified identities and stakeholder roles. This does affect access to battery passport information in all relevant ecosystem components described in detail in chapter 5, e.g. the EC User web portal, the Registry, all involved APIs and the distributed battery passport data repositories.

The SReq covers the identity and access management mainly in section "1.3 Standards on access rights management, information system security, and business confidentiality". Identity management shall ensure that organisations, individuals, machines and services are provided with acknowledged identities. The standard(s) shall define clear rules and requirements related to access control measures to regulate the access to restricted product passport information.

Access rights management shall be attribute-based and product group specific and the economic operators will be responsible for managing the corresponding DPP access rights for their respective battery passport data.

The standard(s) shall also address the issue of how to transfer, delegate and enforce access rights, e.g. to another economic operator, to third-party service providers, to natural persons operating as employees of the before mentioned legal entities as well as legal persons.

Selected standards evaluation

Table 11: Standards for identity and access management

Standard and Title	**Classification** L: Level, Sc: Scope, St: Status	**Originator**	**Short Description**
ISO/IEC 24760-1:2019 - IT Security and Privacy (Link)	L: Global, ISO Sc: General St: Widely Applied	ISO/IEC	A framework for identity management.
ISO/IEC 29146:2016 - Security techniques (Link)	L: Global, ISO Sc: General St: Widely Applied	ISO/IEC	A framework for access management.
W3C DID Decentralised identifiers (Link)	L: Global, De Facto Sc: General St: Widely Applied	W3C	Decentralised Identifiers (DID) are a new type of identifier that enables verifiable, decentralised digital identities.

Standard and Title	**Classification** L: Level, Sc: Scope, St: Status	**Originator**	**Short Description**
W3C VC Verifiable Credentials (Link)	L: Global, De Facto Sc: General St: Widely Applied	W3C	Verifiable Credentials (VC), a mechanism to express credentials on the web in a way that is cryptographically secure, privacy respecting, and machine verifiable.
W3C VP Verifiable Presentations (Link)	L: Global, De Facto Sc: General St: Widely Applied	W3C	Verifiable Presentations (VP), can express data from multiple Verifiable Credentials and contain arbitrary additional data encoded as JSON-LD.
eIDAS Regulation (Link)	L: Europe, De Facto Sc: General St: Widely Applied	EU regulation	eIDAS stands for electronic identification, authentication and trust services. It is a European regulation that created one single framework for electronic identification (eID) and trust services, making it more straightforward to deliver services across the European Union.
Open ID Connect (Link)	L: Global, De Facto Sc: General St: Widely Applied	OpenID Foundation	OpenID Connect is an interoperable authentication protocol based on the OAuth 2.0 framework of specifications.
OID4VCI OpenID for Verifiable Credential Issuance (Link)	L: Global, De FactoSc: General St: Widely Applied	OpenID Foundation	Defines an API for the issuance of Verifiable Credentials.
OID4VP OpenID for Verifiable Credentials (Link)	L: Global, De Facto Sc: General St: Widely Applied	OpenID Foundation	Defines a mechanism on top of OAuth 2.0 to allow presentation of

Standard and Title	Classification L: Level, Sc: Scope, St: Status	Originator	Short Description
			claims in the form of Verifiable Credentials
Gaia-X Trust Framework (Link)	L: Europe, De Facto Sc: General St: Upcoming	Gaia-X AISBL	The Gaia-X Trust Framework is the set of rules that define the minimum baseline to be part of the Gaia-X Ecosystem. Those rules provide a common governance and the basic level of interoperability across individual ecosystems while letting the users remain in full control of their choices.

The European Commission states: "The European strategy for data aims at creating a single market for data that will ensure Europe's global competitiveness and data sovereignty. Common European data spaces will ensure that more data becomes available for use in the economy and society, while keeping the companies and individuals who generate the data in control." [10].

Following this guideline, we must notice that, among others, new identity and access management technology is needed to meet the challenging requirements of a decentralised battery passport system and to be able to provide data sovereignty. To tackle these challenges, we recommend selecting the Gaia-X Trust Framework that implements the concept of Self-Sovereign Identities (SSI) [11], extended by battery passport information like e.g. stakeholder roles. To our knowledge, Gaia-X is the most advanced framework to build decentralised data spaces today and it has already been selected by Catena-X [12] and the Data Space Business Alliance (DSBA) [13] for their individual specifications. Both initiatives share a wide overlap of implemented standards using the common Gaia-X Trust Framework and the respective open standards that are already available to be used, e.g. eIDAS Regulation, Self-Sovereign Identities, Decentralised Identifiers, Verifiable Credentials and Verifiable Presentations.

However, the necessary access control components are not finalised in the standardisation process. The development of technology for decentralised data spaces is still young. But open-source components are under active development, e.g. Eclipse Data Space Components [14] and the FIWARE Data Space Connector [15]. Their promising progress and implementations can be observed in several European Union funded projects and Gaia-X Lighthouse projects.

4.6 Data integration, distribution, exchange and protocols

Definition

Data integration, distribution, exchange and protocols refer to the different ways that systems use to collect and exchange data between different stakeholders and software components. There are e.g. APIs, file sharing platforms and many others. In the following, we will focus on aspects of the technical interoperability in data exchange via APIs.

Description in the context of the battery passport

The EU Battery Regulation defines: "All information included in the battery passport shall be based on open standards and be in an interoperable format, transferable through an open interoperable data exchange network without vendor lock-in, machine-readable, structured and searchable" and "the battery passport shall be fully interoperable with other digital product passports required by Union law concerning eco-design". This does affect several APIs connecting the various battery passport ecosystem components depicted in Figure 11 of chapter 5, e.g. the APIs for accessing the Registry or the distributed data repositories.

The SReq covers the aspects of this chapter in section "1.5 Standard(s) on data processing, data exchange protocols and data formats" and in section "1.8 Standards on APIs for the DPP life cycle management and searchability". The standard(s) shall define rules to exchange data between two or more parties as well as processes to introduce, modify, and update information in the passport. The standard(s) aim at harmonising the APIs for automating the management of the digital product passport throughout its life cycle and serving remote queries. It should cover aspects of syntax and semantics, implementation of security and access control and state of the art operations.

Selected standards evaluation

Table 12: Standards for data integration, distribution, exchange and protocols

Standard	Classification L: Level, Sc: Scope, St: Status	Originator	Short Description
ISO/IEC 19987:2017 - EPC Information Services (EPCIS) Standard (Link)	L: Global, IEC Sc: General St: Widely Applied	IEC	EPCIS enables disparate applications to create and share visibility event data, both within and across enterprises.
W3C Web of Things (Link)	L: Global, De Facto Sc: General St: Widely Applied	W3C	The Web of Things (WoT) seeks to counter the fragmentation of the IoT by using and extending existing, standardised web technologies.
IEC 63278-1 and series - Specification of the Asset Administration Shell Part 2:	L: Global, IEC Sc: General St: Widely Applied	IEC	This document specifies the interfaces as well as

Standard	Classification L: Level, Sc: Scope, St: Status	Originator	Short Description
Application Programming Interfaces (Link)			the APIs in selected technologies for the Asset Administration Shells and its sub-models.
ETSI NGSI-LD API (Link)	L: Europe, De Facto Sc: General St: Widely Applied	ETSI	NGSI-LD is an information model and API for publishing, querying and subscribing to context information.
PEPPOL eDelivery (Link)	L: Europe, De Facto Sc: General St: Widely Applied	PEPPOL	eDelivery provides technical specifications and standards, installable software and ancillary services to allow projects to create a network of nodes for secure digital data exchange.
REST API (Link)	L: Global, De Facto Sc: General St: Widely Applied	n.a.	REST API is a general API style for accessing, send, update and delete of data.
IETF HTTP(S) Hypertext Transfer Protocol (Link)	L: Global, De Facto Sc: General St: Widely Applied	IETF	The Hypertext Transfer Protocol (HTTP) is a stateless application-level protocol for distributed, collaborative, hypertext information systems. Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP).
IETF TCP/IP (Link)	L: Global, De Facto Sc: General St: Widely Applied	IETF	The internet protocol suite, commonly known as TCP/IP, is a framework for

Standard	Classification L: Level, Sc: Scope, St: Status	Originator	Short Description
			organising the set of communication protocols used in the internet and similar computer networks according to functional criteria.
ISO/IEC 21778:2017 JSON (Link)	L: Global, ISO Sc: General St: Widely Applied	IEC	Is a data format for data exchange between different applications.
W3C JSON-LD (Link)	L: Global, De Facto Sc: General St: Widely Applied	W3C	JSON-LD 1.1 is a JSON-based format to serialise linked data.

We recommend the following standards to be the foundation of the battery passport API data exchange: HTTPS over TCP/IP shall be the protocol standard candidates and JSON-LD shall be the standard RDF serialisation format for the battery passport payloads as they already are today, e.g. in Gaia-X, Catena-X and NGSI-LD. Furthermore, "REST API has become the most popular and widely used type of API implementation due to its simplicity, scalability, and flexibility" [16]. This should make REST API the next standard candidate.

The battery passport architecture (described in Figure 11, chapter 5) shows that there are several different APIs necessary to operate the battery passport ecosystem. In general, we distinguish three different categories of APIs:

1) APIs operating with the implementation of a technology agnostic canonical data model (chapter 4.9) of the battery passport. This additional layer of abstraction is necessary to cover the fourth interoperability challenge (chapter 2.5) that is dealing with the access to battery passport data provided by data repositories based on different standard APIs. We have not yet indicated a dominant selection candidate to cover this aspect and to recommend; however, our project's demonstrator is implementing GraphQL for this task [17].
2) APIs operating with the implementation of individual data models from different co-existing standard APIs, e.g. the Asset Administration Shell (implemented in Catena-X), NGSI-LD, Web of Things, EPCIS. No selection must be made here. All standard APIs that fulfil the requirements of the SReq, that can process fine-grained remote search queries and that can provide an adequate translation service adapter (chapter 5.2 - needs to be developed separately) will be able to co-exist at different economic operators.
3) Other supporting APIs. No selection or recommendation of standard APIs is currently possible because the details and specifications of the respective services to be provided are not yet available.

All APIs mentioned in 1), 2) and 3) must also be protected by adequate access control components that fulfil the requirements described in chapter 4.5 and 4.12.

4.7 Data storage and persistence

Definition

Data persistence is the ability of data to survive beyond the current runtime or session. It involves storing data in a way that allows it to be retrieved and used even after the application or system that created it has been shut down. Data persistence is crucial for applications that need to store user preferences, application state, or other types of data for later use. Data storage and persistence refer to the concept of retaining digital information in a way that it can be accessed and retrieved later. This is a crucial aspect of computing and information management, as it allows data to be stored beyond the duration of a single session or use. Data storage ensures that valuable information is not lost when a computer or device is turned off or restarted.

Description in the context of the battery passport

Data storage and persistence are essential for the battery passport. The choice of storage method depends on factors like data volume, access patterns, performance requirements, and data integrity considerations. Due to the intended distributed management of data, multiple of the above-described methods will be applied. The demand from the ESPR that each economic operator or a delegated DPP service provider is responsible for storing the DPPs for which it is responsible leads to a distributed management and storing of DPPs in the frame of a common DPP system. To ensure reliable access to the DPP data it is proposed that data storage is performed through high availability systems. Archiving of DPP data is necessary in order to preserve historical DPP data, which is also relevant for market surveillance.

In the final proposal of the ESPR [18] it is demanded from the economic operator to create a backup of the stored DPPs at an independent third-party service provider to maintain accessibility of DPPs in case of insolvency, liquidation or cessation of activity in the European Union.

It is important to store the DPP data according to the neutral platform independent semantic data model to allow an easy reuse of DPP data. A back-up based on system-specific data formats shall be avoided.

The development of new harmonised standards should appropriately consider the existing relevant standards.

Selected standards evaluation

Table 13: Standards for data storage and persistence

Standard	Classification L: Level, Sc: Scope, St: Status	Originator	Short Description
ISO/IEC 27040:2015(en) Information technology — Security techniques — Storage security	L: Global, ISO/IEC Sc: General St: Widely Applied	ISO/IEC	Focus on securing of data storage
SNIA "Storage Networking Industry Association"	L: Global, Defacto Sc: General St: Widely Applied	https://www.snia.org	Standards for various storage systems

Persistence technologies

- **File storage:** Storing data in files on secondary storage devices, such as hard drives or SSDs, which can be accessed and manipulated by programs.
- **Databases:** Using databases to store structured data in an organised and efficient manner. Databases provide features like querying, indexing, and ensure referential integrity of data.
- **Object storage:** Storing data as objects or BLOBS, often used in cloud storage solutions. Object storage is suitable for unstructured data like images, videos, and documents.
- **NoSQL databases:** These databases are designed for handling large volumes of unstructured or semi-structured data. They offer flexible data models and horizontal scalability.
- **Graph databases:** This type of database is designed to store and manage data using graph structures. In graph databases, data is represented as nodes, which can be thought of as entities or objects, and edges, which represent the relationships between those nodes.
- **Key-value stores:** Storing data as key-value pairs, where the key is a unique identifier for the data.

4.8 Data processing

Definition

Data processing refers to the transformation of data into meaningful and useful information through a series of operations, computations, and manipulations. It involves collecting, organising, analysing and converting data into a structured format that can be interpreted and used for various purposes, such as decision-making, reporting, and generating insights. Importantly, this process must adhere to data privacy principles to protect the confidentiality and integrity of the data being handled. This includes ensuring compliance with relevant data protection regulations, securing personal and sensitive information, and implementing measures to prevent unauthorised access or disclosure. The SReq underscores the importance of integrating data privacy considerations into the processing activities, emphasising the need for organisations to adopt robust privacy practices.

Data processing can encompass a wide range of activities, including data entry, validation, verification, cleaning, aggregation, calculation, and visualisation. The ultimate goal of data processing is to extract valuable insights, patterns, or knowledge from the data to support informed decision-making and improve business processes.

Description in the context of the battery passport

Standards play a significant role in the context of data processing for battery passports. They provide guidelines, specifications, and best practices for collecting, storing, managing, and exchanging data related to batteries throughout their life cycle. Standards ensure consistency, interoperability and reliability in data processing. Though data processing refers to another component of the Standard Stack, there are some standards that provide generic frameworks and definitions of terminology to structure and integrate data in the context of business processes along the value chain which can be considered as a collection of connected process steps each receiving data inputs and generating data outputs based on data processing patterns. Especially in the enterprise context, several best practices and standards have been established that are worth to be considered for the DPP system.

Selected standards evaluation

Table 14: Standards for data processing

Standard	Classification L: Level, Sc: Scope, St: Status	Originator	Short Description
UNECE-UN/CEFACT Supply chain reference data model	L: Global, De Facto Sc: General St: Widely Applied	UNECE	Provides a framework for any cross-border transport-related business and government domains to specify their own specific information exchange requirements whilst complying with the overall process and data structures
IEC 62264-1 Enterprise- control system integration	L: Global, ISO Sc: General St: Widely Applied	IEC	The standard aims to provide guidelines and best practices for integrating various aspects of control systems and manufacturing operations into a cohesive whole.
IEC 62890-1 Industrial-process measurement, control and automation - Life-cycle-management for systems and components	L: Global, ISO Sc: General St: Widely Applied	IEC	This standard provides definitions and reference models related to the life cycle of a product type and the lifetime of a product instance. It defines a consistent set of generic reference models and terms.
IEC 22123-1 Information technology – Cloud computing	L: Global, ISO Sc: General St: Widely Applied	ISO/IEC	This standard is the definitive reference for cloud computing, providing a consolidated cloud computing vocabulary consisting of terms,

Standard	Classification L: Level, Sc: Scope, St: Status	Originator	Short Description
			terminology and definitions.
Enterprise Integration Patterns, Home - Enterprise Integration Patterns	L: Global De Facto Sc: General St: Widely Applied		The Enterprise Integration Patterns provide an approach to design and build distributed applications and integrate existing ones.

4.9 Data models and data formats

Definition

A data model is a structured and organised representation of data that defines the relationships, attributes, constraints, and semantics of various elements within a system or domain. It provides a blueprint for how data should be organised, stored, and manipulated, enabling a clear understanding of the data's structure and meaning. Data models serve as a bridge between the real-world entities and the digital representation of those entities, facilitating effective communication, analysis, and management of data. They are used in fields such as database design, software development, information systems, and more, to ensure consistency, accuracy, and meaningful interpretation of data.

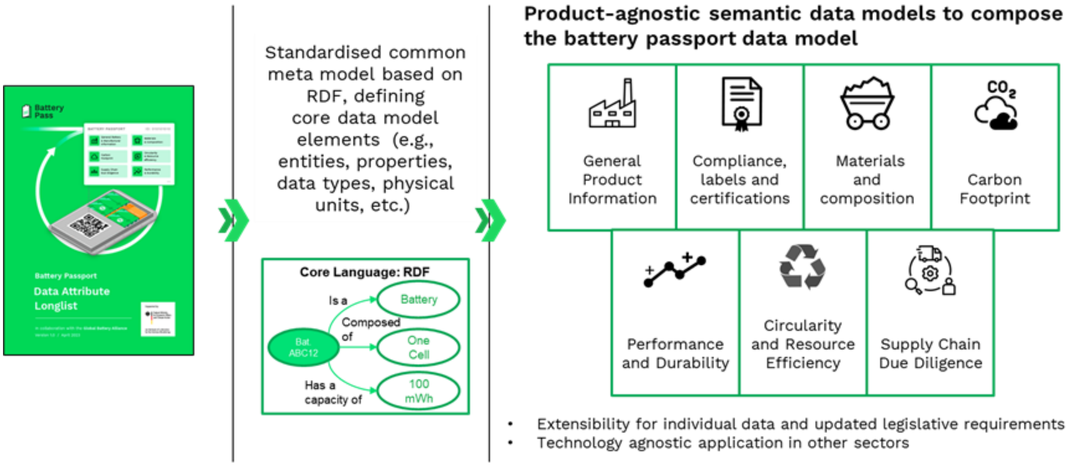
Description in the context of the battery passport

For interoperability purposes a common data model approach is necessary to ensure that data exchange can be performed in a reliable way. The description of a data model shall be performed with a standardised machine-readable formal language. Concurrently maximum flexibility on actual technical implementation should be supported in order to allow technology-agnostic implementation of DPP data repositories that manages battery passport data.

For the representation of the battery passport data points identified in the Battery Pass Content Guidance a meta model based on the W3C Resource Description Framework (RDF) was selected. RDF is a generic description of claims that are based on human representation of claims in sentences by the connection of subject, predicate and object. Hence RDF constructs that are represented in graphs are called triples. The RDF-based meta model defines core data model elements like entities, properties, relations, data types, physical units and others. This follows the Meta-object Facility (MOF) approach proposed by the Object Management Group (OMG).

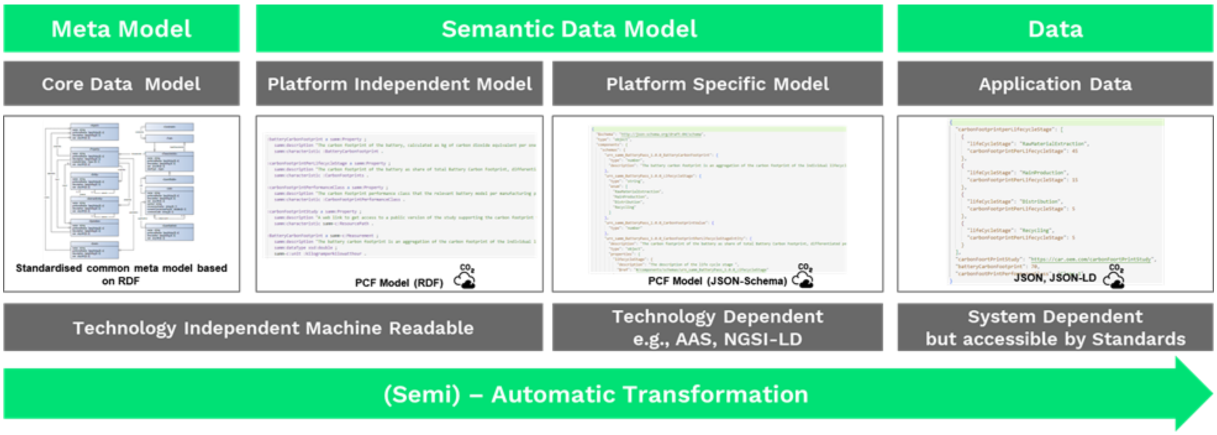
Based on this meta model for each content cluster a semantic data model is composed. Because the content cluster structure is agnostic from a product, they could be used for other product sectors beyond batteries as well.

Figure 9: Battery passport data attributes transformed to platform independent semantic models for each content cluster [19]


Battery Pass
Battery Passport
Data Attribute
Longlist
Standardised common meta model based on RDF, defining core data model elements (e.g., entities, properties, data types, physical units, etc.)
Core Language: RDF
Is a
Battery
Composed of
Bat. ABC12
One Cell
Has a capacity of
100 mWh
Product-agnostic semantic data models to compose the battery passport data model
General Product Information
Compliance, labels and certifications
Materials and composition
CO_2
Carbon Footprint
Performance and Durability
Circularity and Resource Efficiency
Supply Chain Due Diligence
• Extensibility for individual data and updated legislative requirements
• Technology agnostic application in other sectors

The platform independent semantic data model can be automatically transformed into a platform specific model that could be used for implementation. This follows the Model Driven Architecture (MDA) approach proposed by the OMG as well.

Figure 10: Battery example how DPP data is represented and transformed


Meta Model
Semantic Data Model
Data
Core Data Model
Platform Independent Model
Platform Specific Model
Application Data
Standardised common meta model based on RDF
PCF Model (RDF)
PCF Model (JSON-Schema)
JSON, JSON-LD
CO_2
Technology Independent Machine Readable
Technology Dependent e.g., AAS, NGSI-LD
System Dependent but accessible by Standards
(Semi) – Automatic Transformation

The MDA approach based on automated transformation of platform *independent* model into a platform *specific* model ensures maximum flexibility for the implementation of DPP system components based on different standards. At the same time common semantics ensure interoperability between system components that use different platform specific model implementations to represent DPP data with Asset Administration Shell, NGSI-LD, or others.

Selected standards evaluation

Table 15: Standards for data models and data formats

Standard	**Classification** L: Level, Sc: Scope, St: Status	**Originator**	**Short Description**
Resource Description Framework (RDF)	L: Global, De Facto Sc: General St: Widely Applied	W3C (World Wide Web Consortium)	RDF has sufficient mapping power to allow platform-independent semantic data models and ontologies to be described.
Model Driven Architecture (MDA)	L: Global, De Facto Sc: General St: Widely Applied	OMG (Object Management Group)	MDA is an approach to software design and development that focuses on using models. The concept describes platform independent models that can be transformed into platform specific models.
Meta-Object Facility (MOF)	L: Global, De Facto Sc: General St: Widely Applied	OMG (Object Management Group)	MOF provides a set of standards for developing and representing meta models in a standardised way. It is linked to MDA.
Java Script Object Notation JSON	L: Global, De Facto Sc: General St: Widely Applied	W3C / ISO/IEC 21778:2017	JSON is a compact data format that allows serialisation of structured data based on a defined schema described with JSON-Schema notation.
Java Script Object Notation – Linked Data	L: Global, De Facto Sc: General St: Widely Applied	W3C	JSON-LD supports the concept of linked data. It can be used as serialisation of RDF.

Standard	**Classification** L: Level, Sc: Scope, St: Status	**Originator**	**Short Description**
IEC 63278-1: Asset Administration Shell (AAS)	L: Europe, IEC Sc: General St: Upcoming	IEC	AAS provides a meta model to represent semantic data models for digital twins by composition of sub-models. It can be considered as a platform specific representation that can be transformed from a platform independent semantic model based on RDF. This approach is used at Catena-X to ensure data interoperability. A possible serialisation format for AAS models is JSON.
Next Generation Service Interface – Linked Data NGSI-LD	L: Europe, De Facto Sc: General St: Upcoming	ETSI	NGSI-LD uses semantic data models based on JSON-LD which could be considered as an alternative platform specific semantic model that can be transformed from RDF. Domain-specific semantic models will be presented as Smart Data Models.
ISO/IEC 16022: Information technology - Automatic identification and data capture techniques	L: Global, ISO Sc: General St: Widely Applied		Data Matrix bar code symbology specification

Meta Model:

The meta model describes the generic means how to compose a data model. The main elements of a meta model are generic entities that can be used to represent concepts and the relationships between those entities which allows the formal representation of knowledge.

The relations can be subdivided into 3 generic types and their partly inverse relations:

1) Association example (arbitrary relation between entities)
    a. A Battery Passport **represents** a battery
2) Composition example (part-of) and the invers relation Aggregation (has-a)
    a. A battery pack **has a** battery module
    b. A battery cell is **part of** a battery module
3) Specialisation (is-a) and the inverse relation Generalisation (is-of-type)
    a. An individual Battery **is of a** certain battery model
    b. The EV battery **is a** special category of a battery

In addition to the relation types described above each relation can be associated with a cardinality that defines the number of elements that are valid at each side of the relation. Possible cardinalities are 1 to 1 (e.g. one battery passport represents one battery), or 1 to many (1 battery has multiple cells).

A candidate for the representation of a meta model is the RDF (Resource Definition Framework) which allows the definition of canonical elements for the description of ontologies. RDF is based on a generic description of claims that are leaned on human representation of claims in sentences by the connection of subject, predicate and object. Hence RDF constructs that are represented in graphs are called triples. RDF is standardised by the W3C (RDF - Semantic Web Standards (w3.org)). Though the original intent was to use RDF for representation of semantics in the WWW (semantic web) it provides a generic framework to enable a common way of data representation that is a main pre-requisite for the realisation of interoperability both on the level of data but also on semantic level. In summary, RDF is a powerful technology that enables the creation of structured, linked, and semantically meaningful data which is the pre-requisite for enhancing various aspects of data management, integration, and utilization.

The relations between the meta model components can be enriched with certain rules that can be defined as constraints which could be verified during the application of the meta model elements for a semantic model. This would ensure a consistent compilation of a semantic meta model. A mean to formally describe those constraints in the frame of RDF based models is the Shapes Constraint Language (SHACL) that is also standardised under W3C (Shapes Constraint Language (SHACL) (w3.org))

CATENA-X uses an RDF based meta model (SAMM Aspect Meta Model) based on the Eclipse Semantic Modelling Framework for the definition of platform independent semantic data models. These can be transformed to platform specific models like AAS Sub Models for representing standardised digital twins that ensures interoperability in the CATENA-X data space and beyond.

4.10 Unique identifiers

Definition

A unique identifier is a series of characters, which is guaranteed to be unique within a given space. When such an identifier is assigned to an object, it allows that single object to be individually referenced within the space, and in the case of linked data allows for references and relationships between objects to be maintained.

Description in the context of the battery passport

A crucial element in the realm of battery passports is the utilisation of a unique, non-significant string of characters designed to distinguish individual items or models. The SReq covers the unique identifiers in section “1.1 Standard(s) on unique identifiers”. The standards shall define requirements for uniqueness of each identifier (i.e., the same identifier shall not be assigned to different products, different economic operators, or different facilities). This unique identifier assumes a central role, serving as the reference point for the seamless exchange of battery passport data among all relevant stakeholders, encompassing both individual batteries and various battery types.

Fundamentally, each battery, without exception, must be assigned its distinct and exclusive identifier. This imperative step ensures that every battery can be identified uniquely within the system, facilitating effective tracking, monitoring, and management. Moreover, the scope of unique identifiers extends beyond batteries themselves. Organisations, individuals and facilities involved in the battery ecosystem are also required to possess unique identifiers. This broader application is necessary to maintain clarity and precision in passport information, ensuring that every relevant entity involved is easily distinguishable. In cases where specific equipment is a requisite component of passport information, these too must be assigned unique identifiers. One noteworthy linkage specified by the standard is the serialisation of component identifiers to the overall battery identifier. This linkage ensures that all components within a battery system and their corresponding data, regardless of their complexity, can be systematically linked to the overarching identifier.

Selected standards evaluation

Table 16: Standards for unique identifiers

Standard	**Classification** L: Level, Sc: Scope, St: Status	**Originator**	**Short Description**
ISO/IEC 9834-8:2014: Generation of universally unique identifiers (UUIDs) and their use in object identifiers (Link)	L: Global, ISO Sc: General St: Widely Applied	ISO/IEC	A UUID is a globally unique identifier which requires no central registration process.
Uniform Resource Names (URNs) (Link)	L: Global, De Facto Sc: General St: Widely Applied	IETF	A Uniform Resource Name is a persistent, location-independent resource identifier using a well-defined syntax
Universally Unique Identifier URN Namespace (Link)	L: Global, De Facto Sc: General St: Widely Applied	IETF	The defined syntax and grammar for the URN namespace can be used to map existing proprietary identifiers as URNs

Standard	Classification L: Level, Sc: Scope, St: Status	Originator	Short Description
Decentralised Identifiers (DIDs) (Link)	L: Global, De Facto Sc: General St: Upcoming	W3C (World Wide Web Consortium)	The DID scheme is designed to enable organisations to generate their own identifiers using systems they trust.
Economic Operators Registration and Identification number (Link)	L: Europe, De-Jure Sc: General St: Widely Applied	Regulation of the European Parliament (EC) No 648/2005	EORI is an identifier for businesses which undertake the import or export of goods into or out of the EU.

Multiple identifiers are required throughout the data held within the battery passport, linking various data entities and ensuring smooth traversal of the knowledge graph. When choosing the identifier used for accessing the battery passport itself, the requirements for a free of charge ID to be generated at the economic operator and resolving to a decentral service endpoint would indicate the usage of Decentralised Identifiers (DIDs) as a recommendation and the basis of the overall identity of the battery passport data.

With the battery passport data, it is assumed that further identifiers will be required, but pre-existing identifiers should be reused where possible to avoid unnecessary duplication of work. To ensure consistency across ID formats whilst allowing for maximum flexibility, it is recommended that all such identifiers should be URNs. As a last resort, where a new internal identifier is required, and if no pre-existing identifier can be found a UUID can be used.

4.11 Data carriers

Definition

A data carrier, in the context of information technology and data management, is a medium or device used to store, transport, or transmit data. Data carriers come in various forms and technologies (e.g. Data Matrix code, QR code, NFC Tag) and they serve as containers for digital information.

Description in the context of the battery passport

The Battery Regulation specifies a QR code as a data carrier to access the battery passport (Article 77(3)), but leaves the option open for alternative types of smart labels (e.g. RFID, NFC tags, Date Matrix Codes) within the scope of delegated acts (Article 13(8)).

A QR code (Quick Response code) is a two-dimensional barcode that can store a significant amount of information in a compact format. QR codes are designed to be easily scanned and read by QR code scanners or smartphones and tablets.

The QR code “shall be printed or engraved visibly, clearly legibly and indelibly on the battery”; or, if not possible, affixed to the packaging or accompanying documents (Article 13(7)). The data carrier shall comply with ISO/IEC 15459:2014 (on procedural requirements to maintain identities) and with ISO/IEC 18004:2015 (on requirements for QR codes) according to the Battery Regulation (Recital 44, Article 77(3)).

According to the SReq, the data carrier should enable the access to product passports without requiring additional software downloads. A key question that needs to be clarified is what data is stored in the QR code and its consequences on the technical implementation. While storing a URL to access the DPP is standardised by ISO/IEC 18004 and supported by major operating systems (Android, iOS, Windows) and widely available apps, there are benefits of storing additional information as **offline data** within the QR code. Offline information storage offers independence from online connections, security benefits, and flexibility. However, it also faces limitations regarding data size, readability, app dependencies, and the need for standardisation. These pros and cons should be carefully weighted when considering the use of QR codes for offline data storage in various applications. Similar considerations must be made if **more than one URL** is to be stored in the data carrier, as is currently being discussed for public and restricted information.

Selected standards evaluation

Table 17: Standards for data carriers

Standard	**Classification** L: Level, Sc: Scope, St: Status	**Originator**	**Short Description**
ISO/IEC 15459:2014	L: Global, ISO Sc: General St: Widely Applied	ISO/IEC	ISO/IEC 15459:2014 specifies a unique string of characters for the identification of individual transport units
ISO/IEC 18004:2015	L: Global, ISO Sc: General St: Widely Applied	ISO/IEC	ISO/IEC 18004:2015 defines the requirements for QR codes
IEC 61406-1: Identification Link	L: Global, IEC Sc: General St: Upcoming	IEC	IEC 61406-1:2022 specifies minimum requirements for a globally unique identification of physical objects which also constitutes a link to its related digital information.

Standard	Classification L: Level, Sc: Scope, St: Status	Originator	Short Description
IEC 63365: Digital Nameplate	L: Global, IEC Sc: General St: Upcoming	IEC	Concept and requirements for the digital nameplate
ISO/IEC 22603-1: Information technology - Digital representation of product information	L: Global, ISO Sc: General St: Widely Applied	ISO/IEC	ISO/IEC 22603-1 defines the general requirements for electronic product labelling
ISO/IEC 21471: Information technology - Automatic identification and data capture techniques	L: Global, ISO Sc: General St: Widely Applied	ISO/IEC	Extended rectangular Data Matrix (DMRE) bar code symbology specification
GS1 Digital Link	L: Global, De Facto Sc: General St: Widely Applied	GS1	GS1 Digital Link provides a syntax for expressing GS1 identifiers in a format to be used in the web
ISO/IEC DIS 18975: Information technology - Automatic identification and data capture techniques	L: Global, ISO Sc: General St: Upcoming	ISO/IEC	Encoding and resolving identifiers over HTTP
ISO 26324: Information and documentation -Digital object identifier system	L: Global, ISO Sc: General St: Widely Applied	ISO	Digital Object Identifier (DOI) is a standardised and persistent identifier used to uniquely identify and locate digital resources on the internet

4.12 Policy management and enforcement

Definition

Policies are used to represent permitted and prohibited actions over a certain asset, as well as the obligations required to be met by actors and stakeholders. In a data exchange context, policy management and enforcement refer to the way terms and conditions related to data access and usage are expressed and operationalised. Typically, this includes using specific policy management tools or frameworks, languages or processes to ensure that policies can be defined, evaluated, enforced and monitored consistently. It shall also ensure data sovereignty to data providers, especially in decentralised global data space environments.

Description in the context of the battery passport

The three major actor groups mentioned in chapter 4.5 shall be granted access to information in line with their respective stakeholder group access rights which the European Commission will specify in upcoming delegated acts. All data that is not available to the public needs to be protected and adequate policies must be defined, distributed, managed and enforced respectively. This does affect battery passport information in all relevant ecosystem components, e.g. the EC User web portal, the Registry, all involved APIs and the distributed battery passport data repositories.

The SReq covers the policy management and enforcement mainly in section "1.3 Standards on access rights management, information system security, and business confidentiality". The standard(s) shall define clear rules and requirements related to access control measures to regulate the access to restricted product passport information. Access rights management shall be attribute-based and product group specific and the economic operators will be responsible for managing the corresponding DPP access rights.

Selected standards evaluation

Table 18: Standards for policy management and enforcement

Standard	**Classification** L: Level, Sc: Scope, St: Status	**Originator**	**Short Description**
ISO/IEC 29146:2016 - Security techniques (Link)	L: Global, ISO Sc: General St: Widely Applied	ISO/IEC	A framework for access management
W3C ODRL – ODRL Model (Link)	L: Global, De Facto Sc: General St: Widely Applied	W3C	Open Digital Rights Language (ODRL) is a flexible and interoperable policy expression language (used in Catena-X).
XACML v3 (Link)	L: Global, De Facto Sc: General St: Widely Applied	OASIS	The eXtensible Access Control Markup Language (XACML) is an XML-based standard markup language for specifying access control policies (used in Catena-X).
Dataspace Protocol v 1.0 ()	L: Global, De Facto Sc: General St: Upcoming	IDSA	The Dataspace Protocol is a set of specifications designed to facilitate interoperable data sharing between entities governed by usage control and

Standard	Classification L: Level, Sc: Scope, St: Status	Originator	Short Description
			based on web technologies.

ODRL is a powerful, flexible, semantics-based standard for the definition of policies. We recommend selecting ODRL as the external policy expression language in decentralised data spaces. This recommendation is aligned with Gaia-X having officially chosen ODRL to be its policy expression language. IDSA, FIWARE and BDVA support that decision in their DSBA “Technical Convergence Discussion Document” [13].

However, respective ODRL policy enforcement components are not finalised in the standardisation process. The development of technology for decentralised data spaces is still young. But open-source components are under active development, e.g. Eclipse Data Space Components [14] and the FIWARE Data Space Components [15]. It is to be noted, policy enforcement components must not necessarily implement ODRL because external ODRL policies could be translated into other policy expression languages as basis for the internal processing of police enforcement.

Another often-discussed topic of data exchange and access control in decentralised data spaces is the aspect of contract negotiations and contract agreements based on presented polices. In Gaia-X it is part of the separate Data Exchange Services Specifications [20], not the Gaia-X Trust Framework. And IDSA has developed the Dataspace Protocol that covers the contract negotiations and should be evolved into a future global standard [21].

During the standardisation, the aspects of policy negotiation and contracting should be discussed intensively. Policy negotiations and contract agreements for each individual battery passport data access might be a considerable burden for bulk quantity business processes. Possible solutions should introduce (semi-) automated negotiation short cuts without effort-prone manual steps involved, or some overarching contract agreements to govern the relationship between data space participants based on their individual stakeholder roles in general without individual negotiations. A third option could be to establish higher level policies that include all batteries of an economic operator and only require one negotiation process at the first visit.

4.13 IT governance

Definition

IT governance, or information technology governance, refers to the framework and processes used to ensure that an organisation's IT resources are effectively managed and aligned with its strategic goals and objectives. It involves defining and implementing policies, procedures, and decision-making structures to oversee and control IT-related activities within an organisation.

Description in the context of the battery passport

The IT governance describes the efficient oversight and management of the technical infrastructure necessary for the functioning of the battery passport system. This module encompasses a set of responsibilities, principles, and processes that ensure the seamless operation of the battery passport system and its associated functions. IT governance involves a systematic approach to decision-making and control, aiming to align IT strategies with broader objectives. Within the realm of the battery passport system, this governance structure encompasses several key functions that play a pivotal role:

- General management encompasses tasks such as information security management and reporting, ensuring that data within the international data space is secure and compliant with relevant regulations.
- Core IT service management covers essential aspects like capacity and performance management, ensuring that the technical infrastructure can handle the demands placed on it efficiently and effectively.
- Technical management is responsible for overseeing infrastructure and platform management, ensuring that the underlying technological foundation of the battery passport system remains robust and reliable.

In addition to these functions, the IT governance module oversees the accreditation, monitoring, and auditing of eligible partners who operate passport functions within the battery passport system. This includes ensuring that these partners adhere to the established guidelines and standards, maintaining the integrity of the entire value chain processes. In essence, the IT governance module provides a comprehensive framework to regulate, manage, and optimise the technical components of the battery passport system.

Selected standards evaluation

Table 19: Standards for IT governance

Standard	**Classification** L: Level, Sc: Scope, St: Status	**Originator**	**Short Description**
COBIT (Control Objectives for Information and Related Technologies)	L: Global, De Facto Sc: General St: Widely Applied	ISACA	IT governance framework focusing on aligning IT with business objectives, ensuring risk management, and maintaining control over IT processes
ISO/IEC 38500:2015 - Information technology - governance of IT for the organisation	L: Global, ISO Sc: General St: Widely Applied	ISO/IEC	ISO/IEC 38500:2015 provides principles and guidelines for corporate governance of IT
ITIL (Information Technology Infrastructure Library)	L: Global, De Facto Sc: General St: Widely Applied	Axelos	ITIL is a set of best practices for IT service management (ITSM)
ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection	L: Global, ISO Sc: General St: Widely Applied	ISO/IEC	While it primarily addresses security, it plays a crucial role in IT governance by

Standard	Classification L: Level, Sc: Scope, St: Status	Originator	Short Description
			ensuring that information assets are protected and aligned with business objectives
ISO/IEC 20000	L: Global, ISO Sc: General St: Widely Applied	ISO/IEC	ISO/IEC 20000 specifies requirements for an IT service management system (ITSM), helping organisations deliver quality IT services that align with business requirement

4.14 Security infrastructure

Definition

Security infrastructure refers to the way security is implemented and maintained within a system. It typically includes aspects of access control, application security, behavioural analytics, firewalls, virtual private networks, vulnerability management, intrusion detection and prevention, virus protection, security and integrity monitoring.

Description in the context of the battery passport

Cyberattacks are an ongoing and ubiquitous threat to IT security infrastructure, carrying the risk of disrupting operations and causing damage to a company's reputation. Today, there are diverse reasons for cyberattacks: Theft, blackmail, sabotage, terrorism, information warfare, etc. The same risks apply to the decentralised infrastructure that will operate the different functions and services of the battery passport ecosystem.

The SReq covers the security infrastructure in section "1.3 Standards on access rights management, information system security, and business confidentiality". The standard(s) shall define clear rules and requirements related to access control measures to regulate the access to restricted product passport information as well as also identify rules to guarantee IT security, cybersecurity, and data protection.

Selected standards evaluation

Table 20: Standards for security infrastructure

Standard	Classification L: Level, Sc: Scope, St: Status	Originator	Short Description
ISA/IEC 62443 Series of Standards - The World's Only Consensus-Based Automation and Control Systems Cybersecurity Standards	L: Global, De Facto Sc: General St: Widely Applied	IEC	The ISA/IEC 62443 series of standards define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS). The approach to the cybersecurity challenge is a holistic one, bridging the gap between operations and information technology as well as between process safety and cybersecurity.

The before mentioned table shows the well-accepted standard IEC 62443 for establishing security infrastructure. It has also been the foundation for the IDSA certification schemes [22]. However, such standards tend to be complex and costly. In the battery passport ecosystem (and other DPP domains), the economic operators are mainly responsible for providing the battery passport data. The mandatory standards that might be applied should be practically well-balanced to not become a too high burden.

In general, the goal to create a decentralised battery passport system contributes to harden the system against various attacks because the data is not stored in a single place and can't be compromised in a single attack.

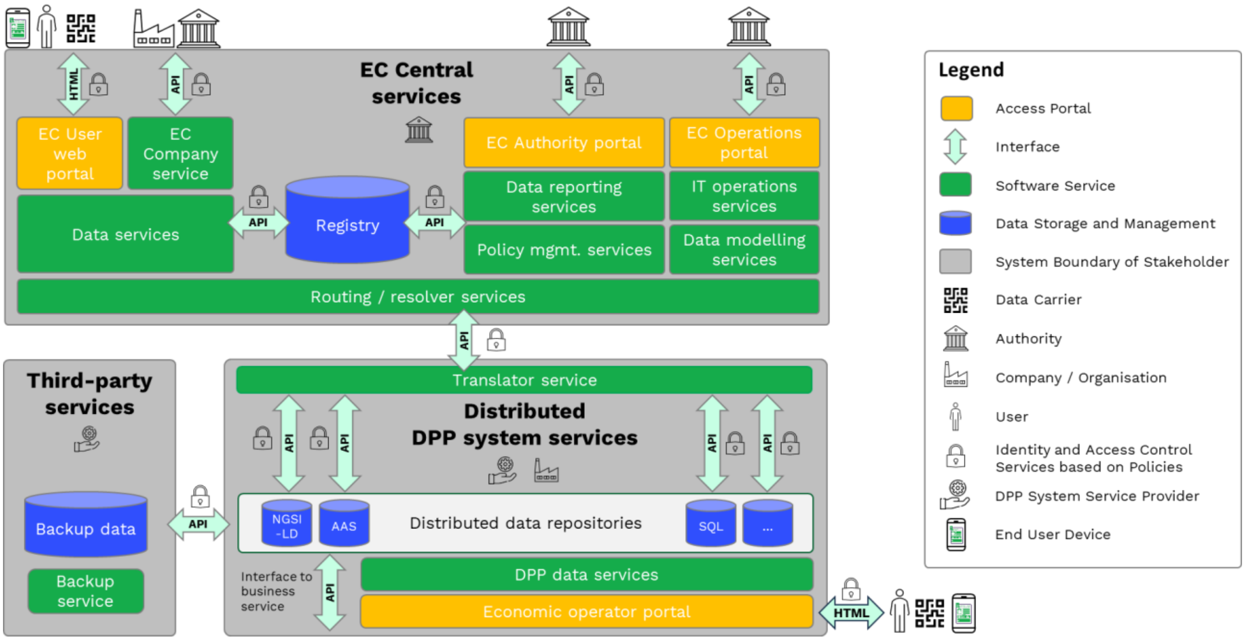
5 System Architecture

In this chapter an architecture description will be provided as a proposal to implement the Standard Stack into an executable system. First an overview of the architecture will be provided and in the next sub-chapter each component is explained.

Architecture Overview

The system architecture is divided into three major service-oriented components: the EC Central services, the distributed DPP system services, and the third-party services. The EC Central services fall under the responsibility of the European Commission, while the distributed DPP system services are required to be established and operated by the economic operator or a designated service provider. The third-party services must be established, as mandated, by an external service provider.

Figure 11: Principal system architecture



In the following sub-chapter, the components indicated in the figure are briefly defined.

5.1 EC Central services

Identity and access control

The identity and access control service components are indicated with the several lock symbols. They protect the different API endpoints and the access-restricted data across the DPP system. The identity and access control service components will evaluate and enforce access control policies based on the securely identified identities and stakeholder roles.

Interfaces (API/HTML)

Within the battery passport system, data exchange between different stakeholders and software components will be conducted via interfaces, application programming interfaces (APIs) (see chapter 4.6) and webpages (HTML). There are several APIs serving varying purposes and stakeholders, indicated by the two-sided arrows, tagged with the word API. The only two arrows which are not a representation of an API are in the top left and in the bottom right corner of the system architecture figure (Figure 11). They are representing HTML webpages rendering the requested battery passport after having scanned a battery QR code.

EC User web portal

The Commission will set up and manage a publicly accessible user web portal allowing stakeholders (e.g. customers, economic operators) to search and compare information included in product passports in line with their respective access rights. (ESPR, Article 12a)

The EC User web portal should link to information already stored by the economic operator in its individual decentral data repository providing the product passport data. (ESPR Annex, Recital 34a)

EC Company service

The aforementioned EC User web portal is not intended for bulk editing of battery passport data. Therefore, it is not suitable for companies managing thousands if not millions of battery passports. We expect the need for adequate company-owned applications with graphical user interfaces which allow the defined services from chapter 4.4 to be carried out locally and in bulk by the economic operator. The EC Company portal will provide an API for machine-to-machine communication that also enables bulk transfer of battery passport data.

EC Authority portal

While customs authorities are foreseen to access battery passport data from the Registry via the EU Customs Single Window Certificates Exchange, there is a need for a dedicated portal for national authorities, the Commission and market surveillance with elevated access rights and functionalities, such as data reporting services (see below), to fulfil their responsibilities.

EC Operations portal

The EC Operations portal for the DPP system is an interface designed to empower administrators and authorised personnel to efficiently manage and oversee the ecosystem of digital product passports. This centralised hub serves as the command centre for monitoring and maintaining the entire system.

Data services

- Verification services: The verification services are cryptographically proving or checking the correctness of data provided as input to the battery passport system. This could include the verification of signatures provided within Verifiable Credentials.
- Validation services: Data validation services check the data to be delivered into the battery passport system for quality, and specificity. Without data validation, you run the risk of receiving incorrect data that is not accurately represented according to necessary data structure and values. It involves comparing structured or semi-structured data from the data source to the battery passport data models, verifying that they match. It

is important to have all relevant validation schemas and criteria available in time because without them no validation checks can be conducted, and the incoming data must be rejected with a telling error message. Incoming data that does not pass the validation checks shall be rejected, too.

- CRUD operations: create, read, update, and delete, which are the fundamental operations used in databases and web applications to manage data.
- Issuing services: Service to publish DPPs (see chapter 4.4)
- Querying services: Querying refers to the process of requesting or retrieving specific data from a database or dataset, in this case distributed data repositories, by using a query language or command. The objective of querying is to filter and extract relevant information that matches certain common criteria or conditions.
- Logging services: Logging refers to the practice of recording events, actions, or transactions that occur within the DPP system. It involves capturing specific information, such as messages, events, errors, and status updates, and storing it in a log file or a centralised log repository for later analysis, monitoring, troubleshooting, and auditing.

Data reporting services

These services are specifically designed for governmental and regulatory authorities, aimed at enhancing the efficiency of reporting and supporting the tasks of market surveillance. This component facilitates the performance of various analyses, such as impact assessments, by utilising anonymised data to ensure privacy while extracting meaningful insights.

The data reporting services provide a suite of software services dedicated to data analytics. They are adept at offering both prescriptive analytics, including detailed statistics for immediate insights, and predictive analytics, like regression analysis, to anticipate future trends based on current data patterns. This dual capability empowers authorities with the data-driven insights necessary for informed decision-making and policy formulation.

IT operations services

The IT operations services, as defined by ITSMF, require the following major components: service management and service desk software. Service management software comprises monitoring, analysis, and reporting within the context of service level agreements (SLAs), as well as tools for capacity planning and management. The relevant service desk software includes performance monitoring, alert tracking and management, support ticket management, and configuration management.

Data modelling services

The data modelling services are centrally designed to ensure interoperability of DPP data across various sectors. The hub service mandates that all DPP data adhere to pre-defined data models, which are crucial for facilitating seamless communication and data exchange both within specific industries and across different sectors. Recognising that legislations can change, or new ones may be introduced, the data models provided through these services are subject to regular updates and adaptations. These modifications are directly overseen and provided by the European Commission, ensuring that all stakeholders have access to the most current and compliant data models.

Registry

The Commission will set up and maintain a secure digital Registry, ensuring the storage of essential identifiers, including unique product identifiers, unique operator identifiers, unique facility identifiers, and a unique registration identifier. For products intended for the “release for free circulation” customs procedure, the registry will also house the product commodity code, along with batteries' unique identifiers as outlined in Article 77(3) of Regulation (EU) 2023/1542. (ESPR, Article 12)

National authorities, customs authorities and the Commission will have direct access to the data stored in the registry. Where needed to further facilitate enforcement, the Commission should, as appropriate, specify other information included in the product passport that needs to be stored in the registry. (ESPR Annex, Recital 32, 36)

In upcoming delegated acts further information which, in addition to being included in the product passport, shall be stored in the registry will be defined, in order to allow for the verification of the authenticity of the product passport, and to improve the efficiency and effectiveness of market surveillance checks and customs controls.

Routing / resolver services

The DPP system is a distributed system, where the DPPs are stored in distributed data repositories. The routing services act as intermediaries that ensures that distributed DPPs, can be centrally accessed via a portal or an API.

Policy management services

Policy management services are a set of functionalities within the DPP system that are designed to handle the creation, management, distribution, and monitoring of policies, guidelines, or rules. These services are accessed and managed exclusively by the European Commission. The economic operators are responsible for the policy enforcement.

5.2 Distributed DPP system services

Distributed data repositories

An important component of the DPP system is the data repository for DPPs that allows storage and management of battery passports. It is proposed that the DPP data repository is managed by an economic operator, or a nominated DPP-as-a-service provider authorised to act on their behalf. The implementation can be done with different technical implementations. Interoperability in the DPP system is ensured by usage of a semantic data model that is derived from the common platform independent semantic data model. The API of the DPP data repository shall be defined in a way that it supports standard CRUD as well as query operations. A translator service allows the translation of generic API calls into system specific API calls.

Translator service

As mentioned before, this service translates platform independent generic REST API calls for creating, reading, updating and deleting (CRUD) of DPP data objects into platform specific REST API calls dependent on the technical implementation (considering all aspects of a REST API call e.g. method, headers, payloads, paths, query-parameter and query language implementations).

Interface to business software

The major data source for the battery passports is managed in company specific backend systems like ERP, SCM, PLM, SCM, Traceability Solutions. The latter allows gathering of data from the upstream value chain which is important for a number of data attributes in the battery passport (e.g. PCF, recycled content, etc.). It is in the responsibility of the economic operator to implement this interface. Based on the proposed semantic data model for the battery passport, the data from the backend-system need to be correspondingly processed, aggregated and mapped to the required data attributes in the battery passport that are represented by a standardised data model.

Since not all companies are willing and capable to develop an own DPP data repository the ESPR proposes that this task can be transferred to a DPP-as-a-service provider. This shall allow economic operators to comply with the Battery Regulation and the linked ESPR without intensive CAPEX.

To ensure access to the DPP data, ESPR mandates from an economic operator to make available a backup copy of the product passport through an independent DPP-as-a-service provider that shall provide a corresponding backup service.

Economic operator portal

The economic operator portal provides decentralised access to DPP data services as an alternative to the centralised access via the EC User web portal. It facilitates direct business-to-business (B2B) and business-to-consumer (B2C) relationships. This model empowers economic operators to provide stakeholders with direct access to DPPs, enabling a more immediate and personalised interaction with product data.

Through this decentralised approach, companies can manage and share their DPP information directly with their business partners or customers, bypassing the need for intermediation by the central platform. It supports customisation and flexibility, allowing businesses to tailor the access and presentation of DPP data to meet specific operational needs or customer expectations.

5.3 Third-party services

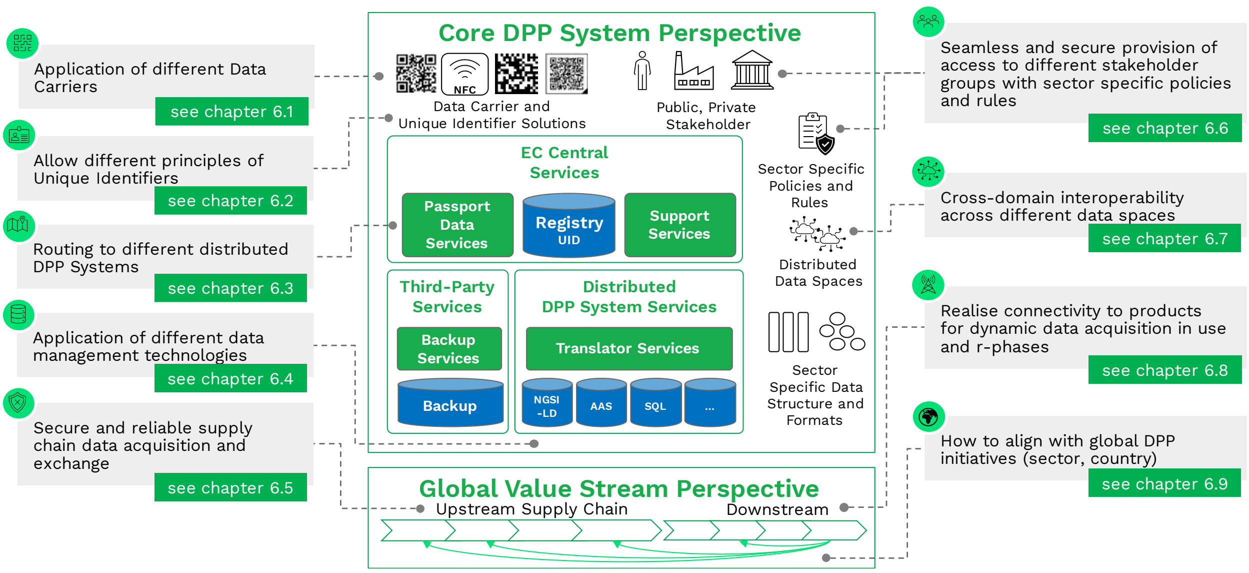
Backup service

As per regulation [18], economic operators shall make available a backup copy of the DPP when placing a product on the market through a certified independent third-party DPP service provider. This backup shall include backups of the most updated version of the DPP and ensures access after an insolvency, a liquidation, or a cessation of activity in the Union of the economic operator.

6 Key challenges and recommendations

This chapter highlights the most pressing challenges that must be addressed as we move forward with the development of the Battery Passport system. It outlines key areas that merit significant focus and dedication from stakeholders involved. These challenges are pivotal in ensuring the successful implementation and functionality of the system and deserve dedicated space and attention by the reading audience.

Figure 12: Key challenges


Application of different Data Carriers
see chapter 6.1
Allow different principles of Unique Identifiers
see chapter 6.2
Routing to different distributed DPP Systems
see chapter 6.3
Application of different data management technologies
see chapter 6.4
Secure and reliable supply chain data acquisition and exchange
see chapter 6.5
Core DPP System Perspective
NFC
Data Carrier and Unique Identifier Solutions
Public, Private Stakeholder
EC Central Services
Passport Data Services
Registry
UID
Support Services
Sector Specific Policies and Rules
Distributed Data Spaces
Third-Party Services
Backup Services
Backup
Distributed DPP System Services
Translator Services
NGSI -LD
AAS
SQL
...
Sector Specific Data Structure and Formats
Global Value Stream Perspective
Upstream Supply Chain
Downstream
Seamless and secure provision of access to different stakeholder groups with sector specific policies and rules
see chapter 6.6
Cross-domain interoperability across different data spaces
see chapter 6.7
Realise connectivity to products for dynamic data acquisition in use and r-phases
see chapter 6.8
How to align with global DPP initiatives (sector, country)
see chapter 6.9

6.1 Application of different data carriers

The Battery Regulation specifies a QR code as a data carrier to access the battery passport (Article 77(3)), but leaves the option open for alternative types of smart labels (e.g. RFID, NFC tags, Date Matrix codes) within the scope of delegated acts (Article 13(8)).

A QR code (Quick Response code) is a two-dimensional barcode that can store a significant amount of information in a compact format. QR codes are designed to be easily scanned and read by QR code scanners or smartphones and tablets. QR codes have gained popularity due to their versatility, ease of use, and widespread compatibility with various devices. They have applications in marketing, advertising, ticketing, contactless payments, authentication, and many other fields where quick and convenient access to data is essential.

The QR code "shall be printed or engraved visibly, clearly legibly and indelibly on the battery"; or, if not possible, affixed to the packaging or accompanying documents (Article 13(7)). The data carrier shall comply with ISO/IEC 15459:2014 (on procedural requirements to maintain identities) and with ISO/IEC 18004:2015 (on requirements for QR codes) according to the Battery Regulation (Recital 44, Article 77(3)).

While the ISO/IEC 15459:2015 defines the structure and usage of identifiers encoded into data carriers, the ISO/IEC 18004:2015 specifies the requirements for QR codes. It provides comprehensive guidelines for the symbology, data structure, encoding methods, error correction techniques, and other aspects related to QR codes. The standard covers both the technical specifications and practical considerations for generating, printing, and scanning QR codes.

The data carrier itself has been identified as a core component of the DPP system and is consequently placed in its own category in the standard stack. The properties of the data carrier and the requirements placed on it are significantly influenced by the information stored in it. For this reason, the unique identifier and the data carrier are dependent on each other and cannot be considered separately.

The implementation of QR codes as gateways to dynamic digital product passports presents a unique challenge due to the inherent nature of the information QR codes carry versus the evolving data they aim to link to. QR codes themselves store static information; once generated, the data encoded within them, such as website URLs or specific product information, cannot be altered. This static nature contrasts with the decentral content of digital product passports, where responsibilities are able to change.

The primary challenge, therefore, lies in ensuring that the static QR code consistently directs users to up-to-date DPP. This necessitates a robust infrastructure capable of managing updates to the digital product passports in a way that the static link provided by the QR code remains valid and reliable. Flexible routing mechanisms that can seamlessly update the linked DPP without needing to change the QR code itself are recommended to be considered. Solutions may include implementing dynamic linking mechanisms where the QR code points to a stable URL that acts as an intermediary, redirecting users to the latest DPP data.

Another key question that needs to be clarified is what data is stored in the QR code and its consequences for the technical implementation. While storing a URL to access the DPP is standardised by ISO/IEC 18004 and supported by major operating systems (Android, iOS, Windows) and widely available apps, there are benefits of storing additional information as **offline data** within the QR Code.

In sum, two variants with different characteristics for storing data in a data carrier to access a battery passport are conceivable:

1. Direct access URL: Undeniably the easiest variant for the end user. Storing a URL to access the DPP is standardised by ISO/IEC 18004 and supported by major operating systems (Android, iOS, Windows) and widely available apps.
   Various standards exist for embedding IDs in URLs, such as GS1 Digital Link [23] or the EN IEC 61406-1:2022 also known as the "Digital Nameplate", where the domain of a company, such as the economic operator, acts as an ID.
2. UID and offline data: Furthermore, it is possible to store the UID and, if necessary, other data available offline, such as basic product information, in the data carrier. While variant 1 is already supported by end devices without further ado, this variant requires dedicated resolvers, however. While the domain name system (DNS) [24], as a core element of the internet, already translates URLs for us with the help of any browser and returns the desired information, dedicated apps and services are required for variant 2. The envisaged registry of the Commission could take over some of the tasks of a resolver, but access is still limited to the Commission itself.

The following table summarises the pros and cons of storing information other than a direct access URL to the DPP.

Table 21: Pros and cons of URL versus UID and optional offline data in the data carrier

Pro	Con
• Independent from an online connection, data available offline • Adding checksums for security • More flexibility of data, not limited to rules of an URL • Phishing attacks by redirecting to fraudulent websites by tampered data carriers could be avoided • URLs could get outdated, a dedicated app with a resolver could handle updates	• Limited amount of information • Size on products like t-shirts are limited (limited size for data carrier and size for storage) • Development and maintenance of An app is required; the app needs to work for a long time, for different operating systems • The more data, the bigger the QR code and the less readable it is • Many existing standards excluded

6.2 Allow different principles of unique identifiers

Unique identification is a core pillar of a DPP. It is necessary to ensure that no two objects can have the same ID globally, and every object has only one ID. Ideally, unique identifiers (for a battery, battery model, battery passport, organisation, facility, plant location, etc.) should be generated purely according to the economic operator's preferred generation scheme. In many cases such identifiers already exist within the data currently held at the economic operator. The SReq states that the standards shall consider the diversity of identifiers currently used by economic operators and accommodate them as much as possible. Unnecessary duplication of effort for additional ID generation should be kept to a minimum with referencing to central reference and master data.

The definition of Decentralised Identifiers (DIDs) allows for an alternative ID generation to be linked directly to a service endpoint which can then be used to access the data. Furthermore, a DID has the advantage of being free of charge and allows for a persistent identifier to be generated at the economic operator for use throughout the life cycle of the battery itself.

Multiple competing generation schemes exist and are already in use (e.g. EORI number for identification of a trading business, GTIN for product identifiers). However, whilst supporting a plurality of such identifiers, it is, to a certain extent necessary to restrict the definition of what legitimately constitutes a valid unique identifier within a DPP, so that the data generated and held within a DPP can continue to support multiple competing protocols and generation tools whilst avoiding overlap in IDs and potential clashes of identifier.

At a minimum we recommend that all internal identifiers are URNs as defined by IETF RTC 8141, and follow the following standardised syntax:

urn:<NAMESPACE-IDENTIFIER>:<NAMESPACE-SPECIFIC-STRING>

Where a well-formed namespace identifier is sufficient to ensure that competing schemes can be identified for example the following GTIN number:

urn:epc:id:sgtin:1234567.089123.12334

Is readily identifiable as a GTIN followed by a numeric key, and an EORI can be readily identified using the following URN:

urn:eori:DE12345678908

The aim in all cases shall be to allow the co-existence of standards for the reuse of identifiers where they are already in use, but not to prescribe specific identity schemes so narrowly as to promote vendor log-in. In any case, duplication and collision of IDs can be avoided by enabling the user to pre-search for existing ID (a concept already available within the CATENA-X data space).

The exclusion of the extended character set, defined within IRIs, should reduce the opportunity for homograph attacks and potential fraud. And it is recommended that implementations always use lowercase letters within the namespace where they have a choice in case, unless there is a good reason otherwise, since according to the accepted URN definition, alphabetic characters within the namespace specific string of a URN will remain case sensitive.

Due to the distributed nature of DPP data, unique identifiers can also effectively be used to define foreign key relationships, and therefore defined URNs should be as consistent as possible and avoid the requirement for additional lexical equivalence algorithms.

A mechanism of directly encoding of data within the unique identifier, as occurs within vehicle identification numbers, was considered but the risks of unauthorised data mining and potential exposure of potential sensitive commercial information outweigh the minimal gain of readability when doing so.

Where no existing de-facto identification standard exists or is in use at the economic operator, or if any new, unique but essentially meaningless identifier is required, a random UUID using the urn:uuid: namespace can be used which should provide a trivially low chance of ID collision. UUIDs also have the benefit of being a free of charge option.

The SReq mentions some other criteria that would be fulfilled with the concept described before. It allows “centralised” and “decentralised” identifiers, and it considers a diversity of identifiers currently used by economic operators using contextual prefixes. Additionally, the SReq lists a maximum length of the unique product identifier to be 70 characters, a requirement not coming out of the different regulatory sources.

6.3 Routing to different distributed DPP Systems

The Battery Regulation (*Recital 126*) states: “To ensure that the battery passport is flexible, dynamic and market-driven and evolves in line with business models, markets and innovation, it should be **based on a decentralised data system**, set up and maintained by economic operators”.

The distributed nature of a decentralised data system requires a flexible routing mechanism that meets the requirements of the battery passport ecosystem. There are scenarios foreseen in which the economic operator changes and the responsibility for maintaining and delivering the battery passport data must be transferred. Furthermore, economic operators might cease to exist. In those scenarios, the flexible routing mechanism needs to ensure that requests for battery passport data always interact with the correct and current economic operator data repository, considering all respective validation and verification services required. We have considered and recommend the routing service in the principal system architecture in chapter 5 to serve that purpose.

6.4 Application of different data management technologies

In Annex II, the SReq mentions that the reliability of the DPP-system is very important for policy implementation and enforceability so “that a full cross-sectoral interoperability can be guaranteed”. This far-reaching requirement includes a growing number of sectors and many different actors and stakeholders across different continents and countries to work together. It renders implementing the DPP system a significant challenge.

The Enterprise Interoperability Framework in chapter 3.2.1 describes three primary approaches to achieve interoperability for standardised data exchange: integrated, unified, and federated. However, considering the complexity and wide reach of the required DPP system, we could not find ubiquitous standards for standardised data exchange available throughout multiple sectors. Lacking such dominantly positioned data exchange standards in the market, our recommendation is to select the federated approach, the most flexible among the three options given.

Following the federated approach, participants must ensure that the data they offer can be interpreted by a standardised meta-model, but both infrastructure and payload formats are only loosely restricted. This approach acknowledges the diversity of standards across different industries, allowing participants to offer their preferred, compliant exchange format and keeping the implementation efforts low. The federated model supports the idea that what is considered a "de facto standard" in one industry may not apply to another.

However, as mentioned in chapter 3.2.1 and shown in Figure 11, the federated approach also requires developing, implementing, and operating additional translator services to ensure that every participant is constantly able to translate its own data into a single, common model. This includes levelling out the different design and feature characteristics of the involved REST APIs as described in chapter 4.6. Data from the technology agnostic canonical data model and from the individual data models, implemented in different co-existing standard APIs (e.g. the Asset Administration Shell (implemented in Catena-X), NGSI-LD, Web of Things, EPCIS), must be bidirectionally translated.

Moreover, all different data management technologies and co-existing standard APIs, applied to the DPP system, must implement a minimal set of API functionality that needs to be specified in the standardisation process (e.g. query language capabilities, single/multi-entity responses, access control capabilities on data attribute level). They are essential to enable the stable operation of the DPP system with reliable provision of the battery passport data, independent from the different data management technology applied to each individual battery passport.

6.5 Secure and reliable supply chain data acquisition and exchange

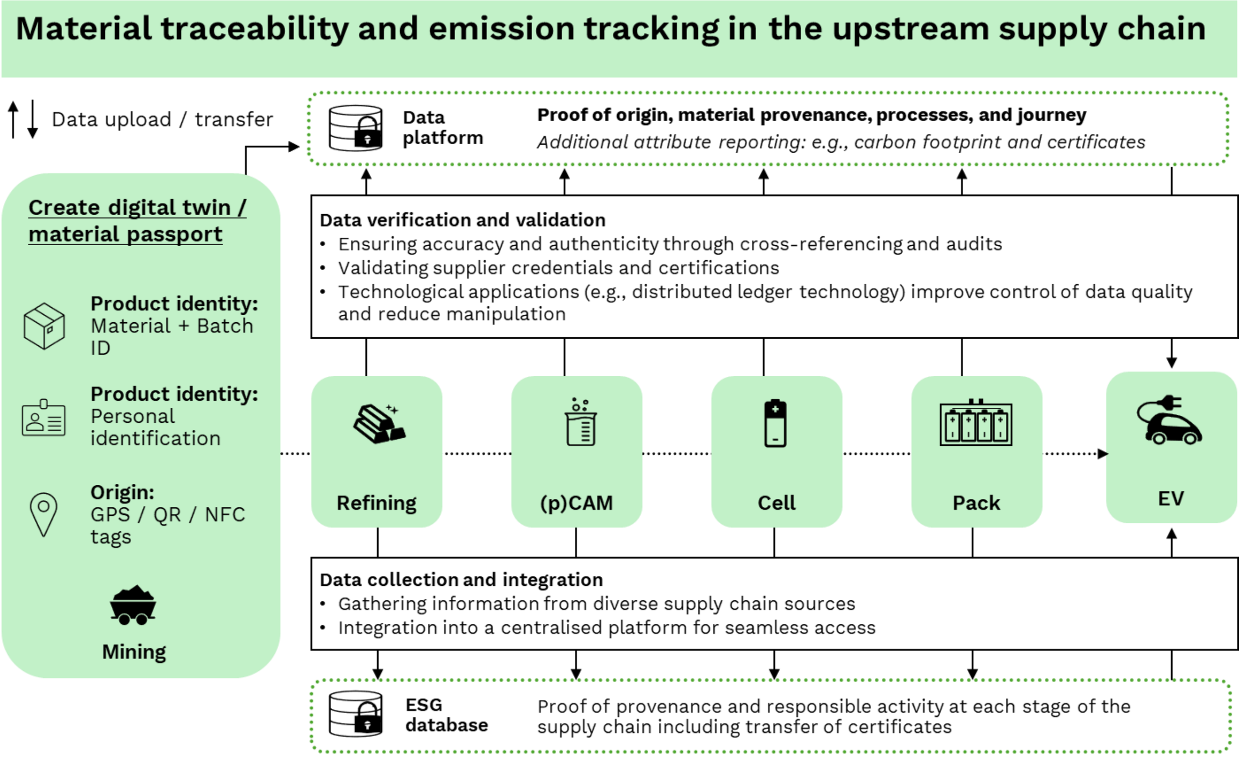
The battery passport is often misperceived as a tool for upstream value chain traceability. Since the battery passport will only appear when a battery enters the European market many steps to produce batteries are performed a long time in advance. However, the European Battery Regulation requires certain information in the battery passport that in fact originates from the upstream value chain represented by a corresponding supply chain. Batteries are produced in global supply chains beyond Europe, since many of the required raw materials, refining facilities and cell production plants are not necessarily located in Europe. Already existing and upcoming regulatory requirements on the provision of reliable ESG metrics force companies to throw light on their supply chains which have often been opaque in the past. A means to perform this are supply chain transparency systems.

A supply chain transparency system is a mechanism or set of processes and tools that enables organisations and stakeholders to track and trace the flow of products, materials, and information across the various stages of a supply chain. The goal of such a system is to provide clear visibility into the origin, movement, and handling of goods, allowing for better management, accountability, sustainability and ethical practices. The following is an overview of certain aspects of supply chain transparency systems that require common standardisation.

1) **Data collection and integration:** The process starts with collecting data from various sources within the supply chain. This data can include information about suppliers, manufacturers, distributors, transportation, and more. Data integration involves consolidating information from different systems and sources into a centralis
2) **Data verification and validation:** The collected data is verified and validated to ensure its accuracy and authenticity. This can involve cross-referencing information (e.g. mass-balance), conducting audits, and validating supplier credentials and certifications.
3) **Digital records and identification:** Each product, component, or batch is represented with a digital record and includes an identifier. This could be a unique serial number encoded with optical machine-readable digital identifiers such as barcode, QR code, or RFID tags. These digital identifiers are associated with the relevant data points for that product or batch.
4) **Tracking and tracing:** As products move through the supply chain, their digital identifiers are scanned or recorded at various checkpoints. Further various data is collected at each checkpoint on the specific characteristics of the commodity or component that will be aggregated in corresponding data points at the battery passport like material composition, origin of material, e.g. primary (mine) or secondary (recycler) source, carbon footprint, certificates and more. This creates a chronological record of the product component's journey, showing its movement from one location to another.
5) **Real-time visibility:** Modern supply chain transparency systems often provide real-time visibility into the movement and status of products. This visibility is made possible through technologies like Internet of Things (IoT) sensors, GPS tracking, and data sharing among supply chain partners.
6) **Data sharing and collaboration:** Supply chain transparency involves collaboration among different stakeholders, including suppliers, manufacturers, logistics partners, and consumers. Data is shared securely among these parties, allowing each stakeholder to access relevant information.
7) **Distributed ledger technology (optional):** Some supply chain transparency systems leverage distributed ledger technology (DLT) to enhance data security by providing means for tamper-evidence. DLT can provide a tamper-proof record of transactions and changes, adding an extra layer of trust to the system.
8) **Reporting and analytics:** The collected data are analysed to generate insights and reports. Organisations can monitor key performance indicators (KPIs), identify bottlenecks, optimise processes, and track compliance with regulations or ethical standards and mitigating risks through early insights which helps to strengthen the resilience of supply chains.
9) **Transparency for consumers:** Data from supply chain transparency systems can be aggregated to individual data points in the battery passport to extend visibility to end

consumers allowing them informed buying decisions. By scanning a QR code of a battery passport using mobile apps, consumers can access information about the origin, production methods, and ethical practices associated with the battery they purchase.

Figure 13: Digital data chain in a traceability system


Material traceability and emission tracking in the upstream supply chain
Data upload / transfer
Data platform
Create digital twin / material passport
Product identity: Material + Batch ID
Product identity: Personal identification
Origin: GPS / QR / NFC tags
Mining
Refining
(p)CAM
Cell
Pack
EV
ESG database

Proof of origin, material provenance, processes, and journey

Additional attribute reporting: e.g., carbon footprint and certificates

Data verification and validation

- Ensuring accuracy and authenticity through cross-referencing and audits
- Validating supplier credentials and certifications
- Technological applications (e.g., distributed ledger technology) improve control of data quality and reduce manipulation

Data collection and integration

- Gathering information from diverse supply chain sources
- Integration into a centralised platform for seamless access

Proof of provenance and responsible activity at each stage of the supply chain including transfer of certificates

Overall, a supply chain transparency system works by integrating data, tracking product components and raw material, sharing information, and leveraging technology to create a clear, traceable, and accountable path for goods as they move through the supply chain. Standardisation on data, communication and unique identifiers is crucial for all the above-described aspects to allow seamless integration of upstream value chain data with the battery passport.

6.6 Seamless and secure provision of access to different stakeholder groups with sector-specific policies and rules

Data protection is the process of securing digital information while keeping data usable for business purposes without trading customer or end-user privacy. This is of utmost importance for trust in a decentralised data system that is requested by the Battery Regulation (*Recital 126*). Secure access control to access-restricted data is an integral part of data protection that will be integrated with sector-specific policies and rules for the different stakeholder groups in the battery passport ecosystem.

Market experience shows and also the European strategy for data emphasises that trust and data sovereignty are critical aspects of decentral data spaces and cross-company data sharing initiatives. Data sovereignty, an extension to data protection, is the concept of retaining authority and control over one's data, allowing individuals or organisations to determine who can access their data and for what purposes. Self-Sovereign Identities contribute a lot to data sovereignty as individual identity holders can fully control and choose to present their own

Verifiable Credentials not only for access rights to non-public data validation purposes. Both concepts are closely linked to the topics of identity and access management (chapter 4.5) and policy management and enforcement (chapter 4.12).

According to these principals and different from the so-called platform economy, data must not be stored, administered and protected centrally. To meet this demand, cutting-edge technology is needed. We recommend that the following two concepts should play an important role in providing secure access to different stakeholder groups with specific policies and rules in the battery pass ecosystem. Both have already been implemented in the Gaia-X Trust Framework [25] and several data space innovators in Europe have already started activities and partnerships towards implementing the Gaia-X Trust Framework.

> **W3C Decentralised identifiers** (W3C DID) [26] are cryptographic digital identifiers, not tied to any central authority, email addresses or social media account with no reference to personal data. It provides individuals and organisations with greater security and privacy, along with more control over their online information.
>
> **W3C Verifiable Credentials** (W3C VC) [27] are a set of standards and protocols created by the World Wide Web Consortium (W3C) for creating, issuing, and verifying digital credentials in a decentralised and secure manner. They are a way to represent and exchange information about a person, an organisation, or a thing in a digital format that can be cryptographically verified. VCs will be issued and signed by registered Trust Anchors of the data ecosystem and can be used for a variety of purposes, such as proving identity, qualifications, and permissions. It can represent all the same information that a physical credential represents, and digital signatures make Verifiable Credentials more tamper-evident and more trustworthy than their physical counterparts.

However, those are a relatively new technical concept and the same applies for the Gaia-X Trust Framework. New infrastructure components must be implemented and continuously further developed. Authorisation policies, decisions, processes and enforcement systems must be adopted in a new and different way by evaluating access control policies based on Verifiable Credentials. And user onboarding, registration and management processes also differ from the traditional ones just to mention a few examples.

To summarise: Mature and battle-tested standards, technical components, processes as well as robust operational user experience must be created and built up quickly to enable trusted data exchange around the battery passport ecosystem for February 2027. We trust in the capabilities and the potential of the Gaia-X Trust Framework, but it will require substantial, concentrated efforts to meet the requirements of the Battery Regulation to realise the decentralised battery passport system, set up and maintained by the economic operators. In that context, the above-mentioned aspects of data protection/sovereignty are of utmost importance to be demonstrated and proven in Lighthouse projects like Catena-X. Dedicated funded projects or working groups with clear and transparent responsibilities should orchestrate the relevant actors and conduct and openly communicate the necessary activities to all relevant DPP stakeholders to meet the given ambitious goals in the name and order of the European Commission. A well-prepared number of low–priced, user-friendly and certified independent third-party service provider offers could be a suitable fallback solution. in case not all economic operators have their own infrastructure ready on time.

6.7 Cross-domain interoperability across different data spaces

The Battery Regulation (*Recital 126*) states: “To ensure that the battery passport is flexible, dynamic and market-driven and evolves in line with business models, markets and innovation, it should be **based on a decentralised data system**, set up and maintained by economic operators”. This renders into a significant **data space challenge**.

The Data Space Support Centre (DSSC) [28], started as an integral part of the European Data Strategy [10], defines a data space in its glossary v1.0 [8] as follows:

> “An infrastructure that enables data transactions between different data ecosystem parties based on the governance framework of that data space. Data spaces should be generic enough to support the implementation of multiple use cases.”

Setting up operational data spaces requires to solve aspects and challenges of many different fields of expertise: technical, governance, business and legal. It is a resource intensive exercise that has already been conducted several times. However, one important market requirement has not yet been fully met: overall interoperability across each other. That was one of the core reasons to kickstart the Data Space Business Alliance (DSBA) [29], an independent initiative to accelerate business transformation in the data economy. The DSBA is composed of the Gaia-X European Association for Data and Cloud AISBL (Gaia-X), the Big Data Value Association (BDVA), the FIWARE Foundation (FIWARE), and the International Data Spaces Association (IDSA). One of the main goals of the DSBA is to work on the technical convergence to improve interoperability among data spaces. The latest results are documented in the “Technical Convergence Discussion Document” [13].

Data spaces aim to provide a federated data infrastructure and ecosystem. Current examples are CATENA-X, a data space currently focused on providing a digital ecosystem for data-driven business models in the automotive industry and the Mobility Data Space which focus on the transportation and mobility sector. In the future it is expected that there will be other sector-specific data spaces that will serve as data sources for DPP data as well as distributed data environment for DPPs itself. This not only refers to different industry sectors but could also be related to different geographical regions on a global scale, which poses several challenges:

1) **Data formats and standards:** different data spaces often use different formats, structures and standards for the representation and storage of data. To achieve interoperability across DPP solutions, these formats and standards need to be harmonised to enable seamless data exchange between different data spaces.
2) **Semantic interoperability:** Even when data formats are compatible, it can be difficult to ensure that the semantics of data elements is understood consistently across domains. To achieve semantic interoperability, common vocabularies, ontologies and semantic mappings must be defined to enable accurate interpretation of the data.
3) **Data governance, trust and security:** Sharing data across different data spaces raises data governance issues, including privacy, security and compliance. Establishing trust frameworks, privacy mechanisms and access controls is critical to address these concerns while facilitating interoperability between different data spaces.
4) **Contextual differences:** Data generated in one data space may have different contextual meanings and use cases compared to data in another data space. Understanding and balancing these contextual differences is critical to ensure that shared data remains relevant and meaningful across different domains.
5) **Business models and incentives:** The interests, business models and incentives for data sharing may differ across stakeholders in different data spaces. Aligning these interests and creating a fair framework for data sharing and collaboration is critical to promoting interoperability.
6) **Regulatory and legal considerations:** Regulatory frameworks for data sharing, privacy and intellectual property rights can vary across countries and industries. Compliance

with the relevant regulations and the removal of legal barriers are essential to enable cross-border interoperability.

7) **Existing systems and infrastructure:** Many organisations operate legacy systems and infrastructure that may not have built-in support for interoperability standards and technologies. Upgrading or replacing these systems to support interoperability can be costly and time consuming.
8) **Semantically linked data:** An important principle of managing data in a decentralised manner is "linked data". Following the semantic web concept, this is a method of publishing, sharing, and interconnecting structured machine-readable data on the web. The key principles of linked data are: Use of URIs, RDF, triple structure, interlinking structured data, open standards and formats, resolving URIs. It makes data more discoverable, accessible, and interconnected for building a web of data. However, decentral IT systems often work with own master data and do not yet support or implement linked data.

Addressing these challenges requires collaboration between stakeholders from different data domains, including industry consortia, standardisation organisations, policymakers and technology providers.

6.8 Realise connectivity to products for dynamic data acquisition in use and r-phases

According to the Battery Regulation (*Recital 46*, *Article 77(4)*) the economic operator placing the battery on the market shall ensure that the information in the battery passport is accurate, complete and up to date. However, the term "up to date" is not further specified. This aspect has already been raised in the project's "Position Paper on content requirements of the EU Battery Passport". It has been requested to clarify details on this requirement as soon as possible, because it has a significant impact on the technical implementation of the battery passport and the volume of data being transferred, processed and stored.

Other important aspects are confidentiality and/or privacy issues. It is unclear whether end-users must actively opt-in and confirm the provision of battery data to the battery passport during continuous private use and whether the status of this confirmation must be somehow administered, filed and archived until final revocation or expiration.

However, the most important question to clarify is the connectivity of batteries and their BMS to the internet. There are many practical reasons for not having connectivity for just some limited time or not at all. Here some examples:

- A battery has no modem or other mechanism for connection to the internet
- A battery has not been or cannot be connected to the internet
- A user denies providing data

Temporary connection outages could be tackled by remote databases and synching mechanisms that are well-known from mobile app development. This would add a great deal of complexity to the technical stack, but it could be technically solved (more easily so for expensive EV batteries than for cheaper batteries like home storage batteries).

Permanently non-connected batteries will comprehensively fail to provide dynamic information for the battery passport. In these cases, the economic operator cannot ensure that the battery passport information is up to date due to missing data. Today, an economic operator might be missing any contact information of the owner of a battery if the sale process has been conducted anonymously and/or was lacking documentation of the serial numbers.

It must be considered that any such data gaps might have direct negative consequences for aspects of data aggregation, data reporting, data filtering, or data analytics, just to mention a few. Incomplete data might lead to incorrect results and processing errors. Data interpolation and preparation might be a way to mitigate the problem of data gaps in some cases – but not if a battery sends no data at all – and it is costly and only ever approximate.

Some connectivity problems are inevitable to a certain degree and the dynamic data will not be delivered with 100% accuracy, be complete and timely. While a separate new data attribute that classifies the actual mode of dynamic data provision for each individual battery would not help to fill the data gaps, it could at least be a means to separate and filter battery passport data in a more controllable way.

Another way to mitigate the risk of missing dynamic data could be to make the provision of contact data and dynamic battery data mandatory to the battery owner by implementing further regulations accordingly. This would, however, likely touch the area of GDPR and have other implications that we currently cannot oversee.

Re-considering the expected value of the dynamic battery passport data based on real user stories could help to find other means of practical and useful mitigation. But the current Battery Regulation simply has the above-mentioned terms included. Changes of those terms would mean changes to the Battery Regulation itself.

6.9 How to align with global DPP initiatives (sector, country)

The trends in data-driven economies, sustainability, and circularity, coupled with the digitalisation of both private and public sectors, are leading to significant developments in digital product passport (DPP) initiatives, including those for batteries. The Battery Pass consortium is actively engaged in activities mainly in Asia, Australia, and America. These activities are guided by similar yet distinct socio-economic and political objectives, resulting in initiatives at various stages of development, each following their own structured approaches and concepts. Even the Global Battery Alliance is working towards consensus building. Currently, a global interoperability approach for DPP is not evident.

However, the global economic and sustainability impacts of batteries, as well as the present and future global value chain, necessitate common content and technical standards. At present, there is a lack of globally organised management in this area. Due to differing regional objectives, an integrated or unified approach to interoperability does not seem feasible. The Battery Pass consortium suggests initiating a joint work program under ISO Level, led by CEN CENELEC and based on proposals from JTC24. Collaborations with well-known institutions for standards interoperability, such as the National Institute for Standards and Technology (NIST) in the US, should be considered.

7 Outlook

The Technical Guidance document for the digital product passport (DPP) system is envisioned as a dynamic and evolving blueprint, designed to adapt to the changing landscape of digital product information management.

As indicated in the document, the design, development, and deployment of the entire DPP system must be conducted collaboratively by the responsible stakeholders: the European Commission, economic operators, and DPP system service providers. This necessitates coordination and the establishment of an organisational foundation. However, the formation of such an organisation remains undecided. In this context, the document's update is also pending, underscoring the necessity for a dedicated entity or collaborative mechanism to maintain its relevance and effectiveness over time. This document aims to be a "living document" that undergoes regular updates and revisions, recognising the importance of staying current with technological advancements and regulatory changes. An opportunity for synchronisation of efforts could be organised in conjunction with the creation of the JTC 24 under CEN CENELEC.

Critical to the document's utility is the need for its content to be rigorously challenged, validated and fed back into the standardisation and regulatory working groups. This process is essential for ensuring that the guidance provided remains accurate, practical, and reflective of the latest industry standards and legislative requirements. To support this objective, the document calls for the development of methodologies and tools specifically designed to assess the implementation of the DPP system. These tools, whose specific identities are not yet known, will help identify gaps, challenges, and opportunities for enhancement. This will ensure that the system evolves effectively to meet the needs of all stakeholders.

As a technical specification blueprint, the document outlines the foundational requirements and standards for the DPP system, serving as a comprehensive guide for its development and implementation.

To ensure the DPP system's relevance and effectiveness across the entire value chain, the working group that created the Technical Guidance document advocates for extending its scope to more comprehensively cover both upstream and downstream activities. This holistic approach is crucial for capturing the full life cycle of products and enhancing transparency and sustainability practices across industries.

Furthermore, the document highlights the importance of inclusive innovation, recommending the implementation of lighthouse demonstrations and testbeds that go beyond focusing on large companies. It stresses the need to involve small and medium-sized enterprises (SMEs) and to tailor the system also to their specific requirements, ensuring that the benefits of the DPP system are accessible to businesses of all sizes.

Finally, the document calls for the development of detailed roadmaps to guide the phased implementation of the DPP system. These roadmaps will provide clear milestones and objectives, facilitating coordinated efforts among stakeholders and ensuring that the system's rollout is both strategic and effective.

8 References

[1] European Commission, “European Green Deal,” 2019. [Online]. Available: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en. [Accessed 26 11 2023].

[2] European Parliament/Council, “Proposal for a Regulation of the European Parliament and of the Council concerning batteries and waste batteries, repealing Directive 2006/66/EC and amending Regulation (EU) No 2019/1020,” 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5469_2023_INIT&from=EN. [Accessed 20 03 2023].

[3] European Commission, “COM (2022) 142: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a framework for setting ecodesign requirements for sustainable products and repealing Directive 2009/125/EC”.

[4] European Commission, “Standardization Request for Digital Product Passport,” 2023.

[5] International Organization for Standardization, “ISO 11354-1:2011. Advanced automation technologies and their applications”.

[6] D. Chen, “Enterprise Interoperability Framework,” in *EMOI - INTEROP'06, Enterprise Modelling and Ontologies for Interoperability, Proceedings of the Open Interop Workshop on Enterprise Modelling and Ontologies for Interoperability*, Luxembourg, 2006.

[7] European Commission, “ISA² - Interoperability solutions for public administrations, businesses and citizens,” [Online]. Available: https://ec.europa.eu/isa2/eif_en/. [Accessed 28 August 2023].

[8] Data Spaces Support Center, “DSSC Glossary | Version 1.0 | March 2023,” [Online]. Available: https://dssc.eu/space/Glossary/55443460/DSSC+Glossary+%7C+Version+1.0+%7C+March+2023. [Accessed 05 11 2023].

[9] International Organization for Standardization, “ISO 9000:2015. Quality management systems - Fundamentals and vocabulary”.

[10] European Commission, “European data strategy,” [Online]. Available: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en. [Accessed 17 03 2024].

[11] TNO, “Self-sovereign identity: a simple and safe digital life,” [Online]. Available: https://www.tno.nl/en/technology-science/technologies/self-sovereign-identity/. [Accessed 18 03 2024].

[12] Catena-X, “Gaia-X and Catena-X on a joint mission,” [Online]. Available: https://catena-x.net/en/vision/gaia-x. [Accessed 18 03 2024].

[13] Data Spaces Business Alliance, “Technical Convergence,” 2023. [Online]. Available: https://data-spaces-business-alliance.eu/wp-content/uploads/dlm_uploads/Data-Spaces-Business-Alliance-Technical-Convergence-V2.pdf.

[14] Eclipse Foundation, “Eclipse Dataspace Components,” 2024. [Online]. Available: https://github.com/eclipse-edc/.

[15] FIWARE Foundation, “FIWARE Data Space Connector,” 2024. [Online]. Available: https://github.com/FIWARE/data-space-connector.

[16] Developer Experience Knowledge Base, “REST API,” [Online]. Available: https://developerexperience.io/articles/rest-api. [Accessed 17 03 2024].

[17] GraphQL, [Online]. Available: https://graphql.org/. [Accessed 17 03 2024].

[18] European Parliament/Council, “Proposal and Annexes for a Regulation establishing a framework for setting ecodesign requirements for sustainable products and repealing Directive 2009/125/EC,” 30 03 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0142. [Accessed 15 08 2023].

[19] Battery Passport Consortium, “Battery Passport Content Guidance,” 2023. [Online]. Available: https://thebatterypass.eu/assets/images/content-guidance/pdf/2023_Battery_Passport_Content_Guidance.pdf. [Accessed 05 03 2024].

[20] Gaia-X, “GXFSv2 - Data Exchange,” 2023. [Online]. Available: https://docs.gaia-x.eu/technical-committee/data-exchange/23.11/dewg/.

[21] International Data Spaces Association, “Dataspace Protocol,” 2024. [Online]. Available: https://github.com/International-Data-Spaces-Association/ids-specification?tab=readme-ov-file.

[22] International Data Space Association, “White Paper Certification,” [Online]. Available: https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-White-Paper-certification-scheme-V.2.pdf. [Accessed 18 03 2024].

[23] GS1, “GS1 Digital Link,” [Online]. Available: https://www.gs1.org/standards/gs1-digital-link. [Accessed 31 August 2023].

[24] Internet Engineering Task Force (IETF), “RFC 8499,” 2019. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8499. [Accessed 08 02 2024].

[25] Gaia-X, “Gaia-X Trust Framework,” [Online]. Available: https://docs.gaia-x.eu/policy-rules-committee/trust-framework/22.10/. [Accessed 12 02 2024].

[26] W3C, “Decentralized Identifiers (DIDs) v1.0,” 2022 July 19. [Online]. Available: https://www.w3.org/TR/did-core/. [Accessed 17 03 2024].

[27] W3C, “Verifiable Credentials Data Model v1.1,” 03 March 2022. [Online]. Available: https://www.w3.org/TR/vc-data-model/. [Accessed 17 03 2024].

[28] Data Spaces Support Centre, [Online]. Available: https://dssc.eu/. [Accessed 17 03 2024].

[29] Data Spaces Business Alliance, [Online]. Available: https://data-spaces-business-alliance.eu/. [Accessed 18 03 2024].

Battery Pass

Have a look at our Website — EXPLORE

Follow us on LinkedIn — FOLLOW

Subscribe to our Newsletter — REGISTER

Drop a line for more information — CONTACT US

CONSORTIUM LEAD

SYSTEMIQ

CONSORTIUM PARTNERS

acatech

BASF We create chemistry

BMW GROUP

Circulor

FIWARE FOUNDATION

Fraunhofer IPK

TWAICE

umicore

VDE RENEWABLES

* under subcontract

This project receives funding from the German Federal Ministry for Economic Affairs and Climate Action by resolution of the German Bundestag under grant agreement No 16BZF335.

Supported by:

Federal Ministry
for Economic Affairs
and Climate Action

on the basis of a decision
by the German Bundestag