Getting to understand product passports

Towards future-proof battery passports

TNO Public | ONGERUBRICEERD Releasable to the public

TNO 2024 R10003

October 2024

ICT, Strategy & Policy
www.tno.nl
+31 88 866 00 00
info@tno.nl

TNO 2024 R10003 – October 2024

Towards future-proof battery passports

Getting to understand product passports

Author(s)	Oskar van Deventer (oskar.vandeventer@tno.nl) Sjoerd Rongen Erik Hoedemaekers Rieks Joosten Theodor Chirvasuta Subhajeet Rath Dayana Spagnuelo Erwin Somers
Classification report	TNO Public | ONGERUBRICEERD Releasable to the public
Title	TNO Public | ONGERUBRICEERD Releasable to the public
Report text	TNO Public | ONGERUBRICEERD Releasable to the public
Appendices	TNO Public | ONGERUBRICEERD Releasable to the public
Number of pages	38 (excl. front and back cover)
Number of appendices	0
Sponsor	Ministry of Economic Affairs
Programme name	Herstelfonds - Batterij technologie
Project name	GTD-E
Project number	060.49019/01.03

Summary

This report presents a design and implementation of a battery passport, applied to rechargeable Lithium-ion batteries that start their life in the mobility domain, e.g., for electric vehicles.

A battery passport is a (possibly distributed) storage means that contains a set of static and dynamic data about a battery pack and its modules. Some of the data may be collected, stored and accessed locally, whereas other parts of the data are maintained “in the cloud”. The rationale of introducing battery passports is that they are assumed to add value during their life cycle (“reduce, reuse, repair, recycle, recover”). Electric vehicles and hence their batteries change ownership. Batteries need repair and maintenance. Batteries may be reused in other sectors, like power-grid balancing. And waste batteries contain valuable materials and hazardous chemicals, for recycling and recovery. Well-maintained battery data, and associated access control, would support and improve decision-making, resulting in both positive economic and environmental effects. It is for these reasons that Europe developed regulations concerning batteries and waste batteries.

TNO has executed the project with two foci.

1. Data model.
   Unambiguous standardised data syntax and semantics are essential for battery passport to be used by multiple party in different scenarios. TNO has developed a battery-passport profile, based on a data model from the European Battery Pass^{TM} program, European regulation, feedback from the project partners and a selected application scenario. TNO has applied its semantic-technologies expertise (Turtle, Owl, Semantic Treehouse) for this purpose.
2. Architecture.
   A clear architecture is needed for the many aspects of a battery passport: when, where and how data is generated (manufacturing, battery-management system, ...), where it is data stored (locally, cloud), how can data be interfaced and accessed (controller area network bus, remote/internet), who can access which data (access control policies, identification of users, confidentiality/privacy), what are the assurances with the data, etcetera. TNO has designed an architecture for a battery passport, based on the selected application scenario and requirements coordinated with the project partners. TNO has applied its dataspaces and self-sovereign identity (SSI) expertise for this purpose.

The project has resulted in a first-time-engineering demonstrator that illustrates how a battery passport may work like in practice, as well as the look-and-feel to its users. The demonstrator implements the above-mentioned data model and architecture.

The project was executed as part of the 25-partner Green Transport Delta – Electrification (GTD-E) program in the context of Herstelfonds - Batterij technologie of the Dutch Ministry of Economic Affairs. TNO thanks in particular the partners ELEO, Cleantron and NXP for their contributions to this project.

Contents

Abbreviations

Abbreviation	**Meaning**
BMS	Battery Management System
CAN bus	Controller Area Network bus
GTD-E	Green Transport Delta – Electrification
GUI	Graphical User Interface
IDS	International Data Spaces
SSI	Self-Sovereign Identity
STH	Semantic Treehouse
UI	User Interface

Preface

This work is the result of a year of work by TNO in close collaboration with our GTD-E partners Cleantron, ELEO and NXP. We thank these partners for their reviews and feedback on our intermediate results. Nevertheless, this document is fully our responsibility.

The authors

1 Introduction

1.1 Product passports

Provenance and traceability of products and goods have become increasingly important to our society. From the production side, customers want to have assurances that a product was made under ethical conditions, as well as get insight in its environmental impact and carbon footprint. Quality and hazards in supply chains need to be traceable, e.g., tracing food contaminations to their source in order to prevent and remedy these. Military suppliers are required to keep track of where their products go, to keep them away from rogue/enemy entities. A product's usage history may be input to its maintenance planning and assessment of remaining value, e.g., the odometer of a car. Also, other parts of a products life cycle may benefit from this data, in order to "reduce, reuse, repair, recycle, and recover" products, its components and its materials.

Ubiquitous digitization and internet access have accelerated developments, potentially improving cost and reliability over paper-based solutions by orders of magnitude. Around 2017, a "peak of inflated expectations" in the hype cycle for blockchain technologies has triggered a plethora of provenance projects in food, logistics, industry, commerce, fintech, admintech, mobility and other. More recently, (International) Data Spaces[1] (IDS) are being developed in a wide variety of sectors, domains and applications. Stakeholders in a data space collaborate on the exchange of data, coordinating their syntax and semantics, their exchange interfaces, business models and monetization, and the required governance.

Also, European and national regulators have become active in this area. Triggered by the technological possibilities and potential societal benefits. New regulations are arising on "product passport" as well as governmental funding[2], both of which further stimulates stakeholders to assess the opportunities.

[1] E.g, https://internationaldataspaces.org/, https://dssc.eu/
[2] E.g. https://hadea.ec.europa.eu/calls-proposals/digital-product-passport_en

Figure 1: Digital Product Passport, a set of static and dynamic data that goes with a product[3].

The above is equally applicable to the mobility domain and the life cycle of batteries used in that domain (e.g., electric vehicles). However, due to the high utilization of critical raw materials, traceability in raw material sourcing and reusing or recycling of batteries and the material therein is key to ensure strategic autonomy for entities having little direct access to these raw materials. This is the case for most of Europe and the EU as a whole, as such, battery passports are a key focus area for European policy makers[4]. The remainder of this section will introduce the concept of a managed battery, a battery passport, the Green Transport Delta – Electrification (GTD-E) project, and the research questions addressed in this report.

1.2 Concept of a managed battery

Batteries for mobility applications are always managed by a battery-management system (BMS)[5]. A battery pack is composed of one or more battery modules. Each battery module has multiple connected battery cells, a set of sensors (e.g., voltage per cell, current, temperature, ...) and electronics for readout of those sensors, control of the battery cells and communication towards the BMS. The modules are typically controlled by a master unit in the BMS that gathers all information, controls the individual modules (which typically act as slaves) and communicates with the application (e.g., vehicle, energy storage system, etc.). The BMS manages the battery, and it keeps track of many parameters, like charging status, charging history and technical health of the individual cells. The BMS connects with other microcontrollers and devices in the electric vehicle, e.g., typically through a CAN-bus[6].

[3] Source of illustration: https://gceurope.org/digital-product-passport-what-is-it-and-what-does-it-imply-for-the-textile-industry/

[4] EU Press statement on battery passports: https://www.europarl.europa.eu/news/en/press-room/20221205IPR60614/batteries-deal-on-new-eu-rules-for-design-production-and-waste-treatment

[5] Battery Management System: https://en.wikipedia.org/wiki/Battery_management_system

[6] Controller Area Network, https://en.wikipedia.org/wiki/CAN_bus

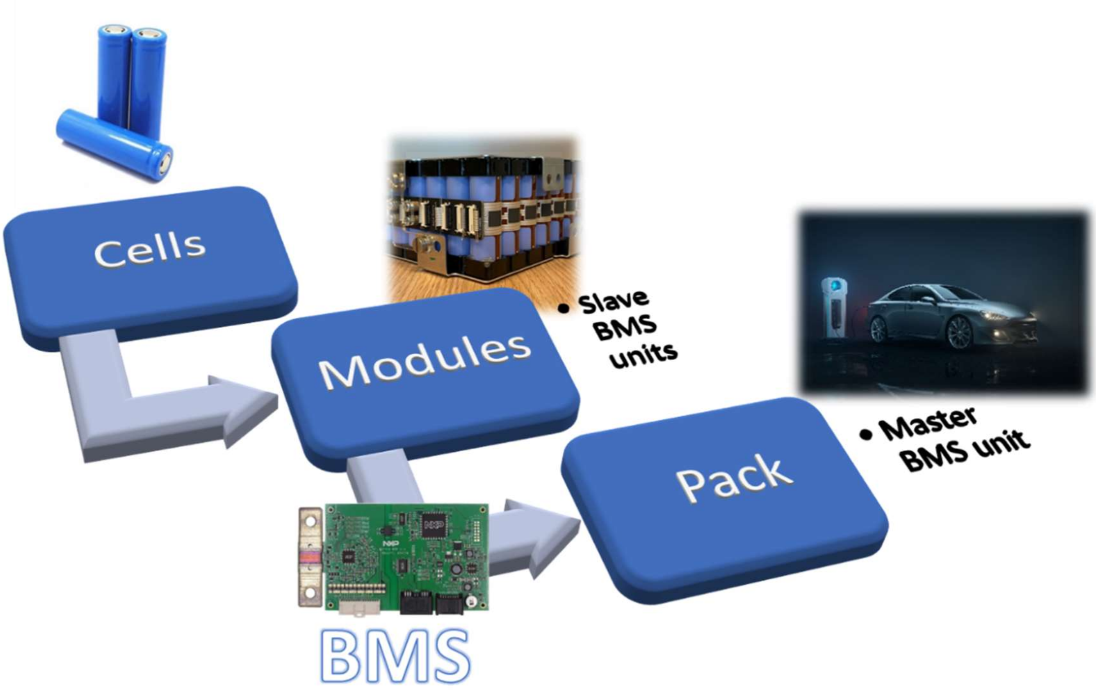


Figure 2: An electric-vehicle battery and its components.

1.3 Concept of a battery passport

Like any product, batteries have a supply chain. Raw materials like lithium are mined and processed. Battery cells are assembled from processed materials. Battery modules contain battery cells, electronics, and other parts. Electric vehicles have a battery pack with one or more battery modules and a BMS. Battery packs may be maintained and repaired, including repair and replacement of battery modules. Electric vehicles and their battery packs may change ownership. Battery packs may have a second life for, e.g., electric grid balancing, when their quality has degraded to a point that they are no longer viable for mobility use. Materials from waste batteries may be recycled, recovered, or disposed of in an environmentally acceptable way.

The starting point of the project has been the following understanding of the concept of a battery passport, based on discussions between TNO experts from the departments Powertrains and Data Ecosystems.

- A battery passport is a (secure) digital container that contains static and dynamic data related to one specific battery, that are to be used for a variety of applications, including recycling, maintenance, carbon footprint tracking, or to determine its (remaining) value for sale, amortization, or replacement.
- A battery passport keeps a log of “life events” (e.g., charging history, maintenance), generated by its Battery Management System (BMS).
- Formal standards for a battery passport do not yet exist. Some manufacturers may have their own proprietary standards. There are some relevant initiatives to be considered, e.g., Battery Pass[7] where a of list of battery-passport data attributes[8] are provided.
- There is a European Regulation[9] that includes the obligation of a battery passport and prescribes basic requirements.[10]
- The rationale of a battery passport is that it adds value to the product (money, environment) and that it is obligated by European law.
- Ownership of a battery passport, i.e., the capability of deciding which parties can create, read, update, or delete data within such a passport (within the limitations of applicable legislation), should be transferrable. However, 'ownership of a battery passport' needs additional clarification/specification; for example, it is currently unclear whether ownership of a battery passport should coincide with ownership of the battery itself. Battery-passport data needs CRUD[11] actions: the data needs to be stored somewhere (“data vault”), it needs to be maintained/updated, it needs to be accessible and exchanged with others.
- Battery passport data has confidentiality: there need to be enforced policies/rights/mandates to read the data (e.g. “verifiable verifier”).
- Battery passport data has integrity and provenance: all data needs to have traceable electronics signatures (a.k.a. “verifiable issuers”), and the data is protected against integrity-violating modifications or deletions.

[7] Battery Pass: https://thebatterypass.eu/resources/

[8] Battery_Passport_Data_Attributes: https://thebatterypass.eu/assets/images/content-guidance/pdf/2023_Battery_Passport_Data_Attributes.xlsx

[9] EU Battery Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:PE_2_2023_INIT

[10] Note that this regulation defines a battery passport as a collection of data, rather than (an IT-component that provides) a secure storage facility that includes such data. The requirements would thus pertain to the data, not to the secure storage.

[11] CRUD: create, read, update and delete, https://en.wikipedia.org/wiki/Create,_read,_update_and_delete

1.4 The GTD-E program

The Green Transport Delta – Electrification (GTD-E)[12] project is a 25-partner Dutch program in the context of Herstelfonds of the Dutch Ministery of Economic Affairs. The program is focussed on the electrification of transport and mobility in The Netherlands. This report is about the part of the program about battery passports. In this project TNO experts from the departments Powertrains[13] and Data Ecosystems[14] collaborate with experts of the battery suppliers ELEO and Cleantron, as well as chip provider NXP.

1.5 Research questions

Based on discussions between TNO experts from the departments Powertrains and Data Ecosystems, the following main research question was formulated.

> Can battery passports be technologically viably used in the mobility domain (Electric Vehicle, including heavy mobile machinery) and grid-battery industry?

This main research question was divided in the following sub-questions.

1. Is sufficient harmonization of battery-passport data possible between manufacturers?
2. Can the integrity and provenance of battery passport data be sufficiently guaranteed?
3. Is there an access control model for battery passport data that would be acceptable to all relevant stakeholders, for managing confidentiality, regulatory access to data, ownership (control, possession), and transfer of ownership, and such?
4. Can the questions above answered positively, such that they also comply to the applicable European regulation?
5. Can the questions above answered positively, such that the battery passport adds relevant value to battery+BMS products in terms of money and environment?

The following aspects have been declared out of scope.

- Formal contributions to Standards Developing Organisations (e.g., CENELEC, IEC).
- Detailed market analyses, or financial business-case analyses for individual partners.
- Make-or-buy analyses, RFP-RFI-RFQ procurement support, vendor selection.
- Legal advice, or binding guarantees about legal analyses.
- Legal-entity establishment with chamber of commerce, notary, and legal contracts.
- Demonstration of the rapid prototypes outside the stakeholder sessions.
- Blockchain.

1.6 This report

This report is the main deliverable of the project. It has been made publicly available via the TNO Repository[15] (search “Battery Passport”)

Associated deliverables are:

- slide sets that have been used at the stakeholder sessions,

[12] Solarmagazine, “GTD-E werkt aan Nederlandse batterijwaardeketen: ‘Recycling maatschappelijk wenselijk en economische kans’ ”, https://solarmagazine.nl/nieuws-zonne-energie/i27555/gtd-e-werkt-aan-nederlandse-batterijwaardeketen-recycling-maatschappelijk-wenselijk-en-economische-kans, 6 July 2022

[13] TNO Expertise Powertrains: https://www.tno.nl/nl/over-tno/organisatie/units/mobiliteit-logistiek/tno-onderzoek-gebied-powertrains/

[14] TNO Expertise Data Ecosystems: https://www.tno.nl/nl/over-tno/organisatie/units/informatie-communicatie-technologie/data-ecosystemen/

[15] TNO Repository: https://ris.tno.nl/

- a first-time engineering demonstration of a battery passport (research software), and
- a video demonstration of this battery-passport implementation[16].

Please contact the authors for further information on these, or for a demonstration.

The remainder of the report addresses the following.

- Demo scenario
- Data model
- Architecture and implementation
- Demonstration
- Conclusions and recommendations

Each section concludes with our learning experiences, as learning has been the purpose of this first-time engineering. Also, a set of appendices is provided with further details on the data models, implementation, as well as a generic conceptual model of product passports that was developed in this project.

[16] Video: https://docu.digital-passport.org/demo

2 Demo scenario

2.1 General

In the GTD-E project a demonstrator will be realized to present a minimum version of a battery passport implementation. This deployment serves to gather feedback on what a battery passport should be able to do, as a demonstration to industry partners on the current technical capabilities and as a technical basis for future developments to build upon.

2.2 Three roles: owner, manufacturer, service provider

In the demo we recognize the following participants in three different roles:

- ELEO: Battery manufacturer, responsible for at least production provenance data.
- Cleantron: Battery manufacturer, responsible for at least production provenance data.
- TNO: Battery passport service provider, responsible gathering, storing and exposing real-time battery data (e.g. sensors).
- User 1: Battery owner (and user), responsible for interpreting and using the available battery data.
- User 2: Battery owner (and user), responsible for interpreting and using the available battery data.

These participants share battery related data with each other to enable the tracing of battery packs, and modules within these packs throughout their life cycle. The tracing of individual battery cells is out of scope and cells are considered to be a permanent part of the module they are placed in.

2.3 Battery-passport data space

To facilitate the data sharing between the aforementioned participants a Data Space[17] is used. Data Spaces enable scalable data sharing between parties without the owner of the data having to give up control over this data. Data Spaces don’t enforce any message model and only provide technical interoperability between participants which have deployed a standardized data space connector. This provides us with the high-level deployment presented below. Within this deployment the batteries are physically deployed, and they periodically push the data from the BMS to a cloud environment from where it is accessible to the data space connector. These data space connectors are deployed for this demo by TNO, together with the facilitating data space components. The users are for demonstrative purposes and will only be implemented as a small user interface to interact with the data space connectors.

[17] Data Space: An infrastructure that enables data transactions between different data ecosystem parties based on the governance framework of that data space. Data space should be generic enough to support the implementation of multiple use cases. As defined by the DSSC.

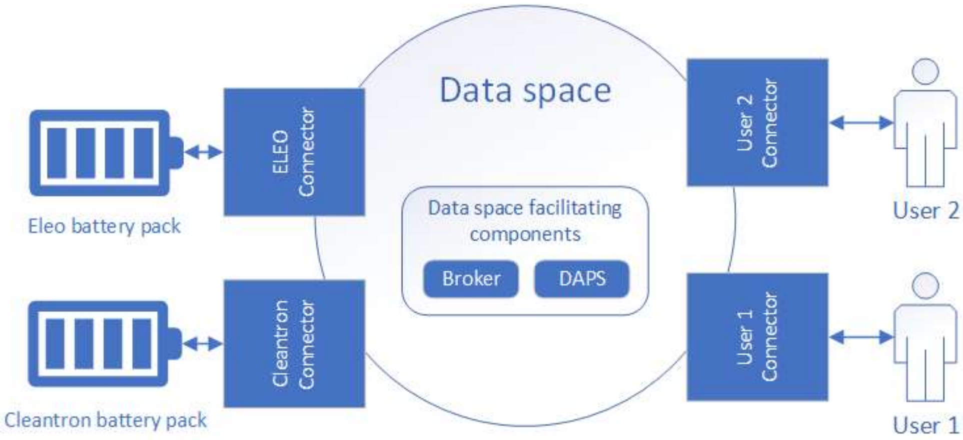


Figure 3: Battery-passport data space.

2.4 Use case: data access, ownership transfer

Within the demonstration we demonstrate the ability of a battery user/owner to access data about the battery. And that this owner cannot gain access to other batteries. That is to say, if user 2 uses the ELEO battery back it is possible to access ELEO data, but not Cleantron data.

Within this demo we also demonstrate how a battery passport could model the second life of a battery when it is transferred from a single battery in e.g., an EV to a static battery for e.g., grid storage solutions. This is demonstrated by both users determining the batteries have degraded and changing their location. Moreover, we demonstrate how the modules within these batteries can be split from their pack and merged into new packs. In the demonstration this is shown by one of the users splitting of 2 modules from their pack and transferring these to the other user who then merges them with the rest of the modules to build a bigger battery pack. Although this use case of combining battery modules from different companies is not currently commonplace in practice it does demonstrate the flexibility afforded by the battery passport solution when it comes to transfer of ownership, splitting, and merging of products without losing traceability of these products.

The information flow of this demonstration is further specified below. Note that the structure of the messages shared is defined in an ontology and from this ontology derived message models. In the sequence diagram the functional flow of information is presented, leaving out for example the data space specific calls to enable peer-to-peer data sharing.

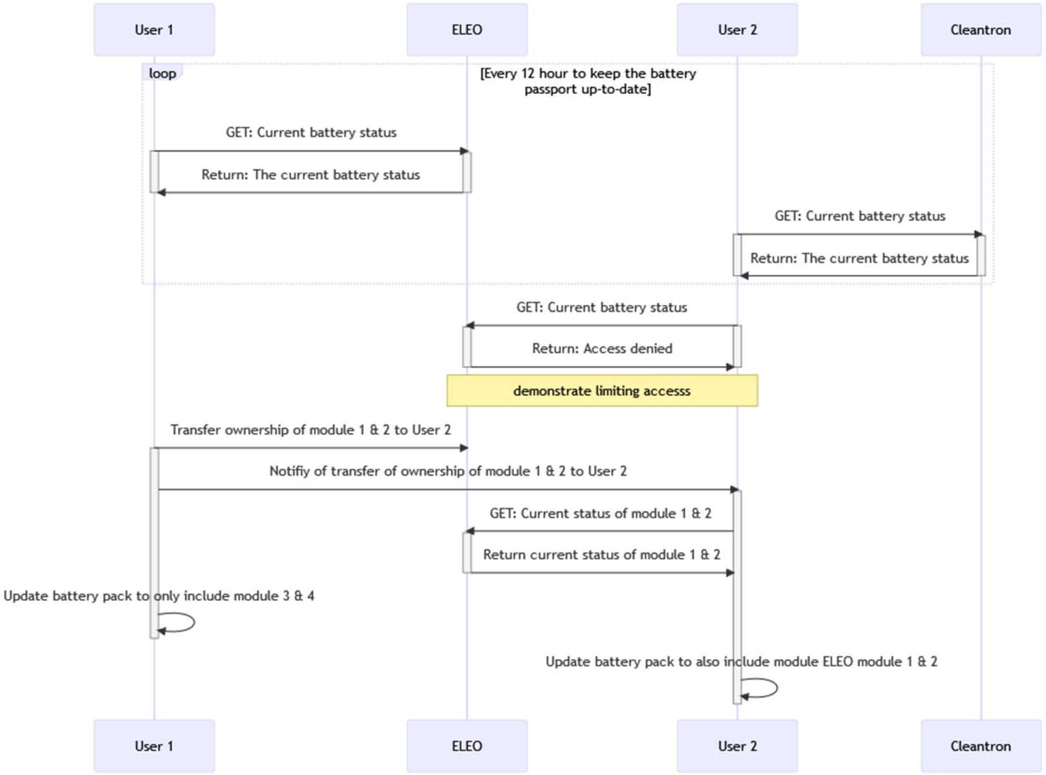

User 1
ELEO
User 2
Cleantron
loop
[Every 12 hour to keep the battery passport up-to-date]
GET: Current battery status
Return: The current battery status
GET: Current battery status
Return: The current battery status
GET: Current battery status
Return: Access denied
demonstrate limiting accesss
Transfer ownership of module 1 & 2 to User 2
Notifiy of transfer of ownership of module 1 & 2 to User 2
GET: Current status of module 1 & 2
Return current status of module 1 & 2
Update battery pack to only include module 3 & 4
Update battery pack to also include module ELEO module 1 & 2
User 1
ELEO
User 2
Cleantron

Figure 4: Functional information flow in our battery-passport scenario.

2.5 Learning experiences

From our discussions with the stakeholders ELEO, Cleantron and NXP, we learned a number of things on the real-world use cases of batteries. Primarily, to which level traceability is relevant, and when it no longer is. Specifically, as battery cells are often glued within the battery module it is not currently feasible to reuse or remanufacture these without processing the whole battery module. As such, we decided to trace down to the modules and not the cell level. Besides that, some theoretical use cases were discussed, such as mixing battery modules from multiple manufacturers in a single pack, something which currently does not happen in practice, but which may be of interest in the future. As such, this use case is included in the demo storyline. Finally, we discussed the 2nd life of battery modules, when they are degraded to the point of no longer being useful for EVs, but still of use to static grid scale installations. This use case is expected for batteries, but currently very few have degraded to the point of not being useable for EVs as such it is mostly a theoretical addition to the demonstration.

3 Data model

3.1 General

The purpose of battery passports is to trace a battery throughout its whole life cycle, in which multiple organizations are involved. As such, their data needs to be interoperable with each other in order to facilitate any sort of analysis of the data. Or, put in another way, the different organisations need to speak the same language and have the same understanding of the words therein, in order to interoperate (work together) with each other.

Within this project we build upon other initiatives and broader European trends for standardizing a battery passport data model. Specifically, the initiatives by Catena-X and the Battery Pass consortium. These have published an ontology and list of recommended attributes respectively. Within this project we combine these to define an ontology to structure the shared data with. For ease of use of the ontology, we use the TNO developed tool *semantic treehouse*[18] to generate a JSON message from this ontology. This gives us the semantic richness of a full ontology, but the ease of use of a simple JSON file. This JSON message model is implemented in the demo described in chapter 2 and allows easy analysis of the data without limiting us to the exact demonstration scenario.

3.2 European regulation

Within the European Union the main piece of relevance for this project is the recent Regulation concerning batteries and waste batteries[19] which has entered in force in July 2023. This regulation applies to the whole variety of portable batteries and updates the former regulatory demands (from 2006) by completing the legislation framework particularly on batteries waste management. The focus of the newly adopted regulation is to promote fair and circular economy in the battery sector, by addressing all stages of their life cycle, from design to recycling, and waste.

In order to support and ensure fairness in the battery market, the regulation also introduces demands for transparent practices through the *battery passport*[20]*.* That is, an electronic record attached to a physical battery (particularly batteries for light means of transport, or LMT, industrial batteries with a capacity greater than 2 kWh and electric vehicle batteries) that contains labelling and information about the batteries' components, composition, performance, and recycled content, among others. This passport is meant to maximize exchange of information, provide information to the public, and support market surveillance. While the implementation of such passport is part of the regulatory demands of the new regulation, in order to give the market enough transition time, the passport is mandatory as of 18 February 2027.

[18] The Semantic Treehouse tooling: https://www.semantic-treehouse.nl/
[19] REGULATION (EU) 2023/1542 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 12 July 2023 concerning batteries and waste batteries, amending Directive 2008/98/EC and Regulation (EU) 2019/1020 and repealing Directive 2006/66/EC [2023] OJ L 191/1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1542
[20] *Ibid.* Article 77

The regulation defines categories of data to be placed in the passport according to the audience they are intended:

1) Information **available publicly** about the manufacturer, and the manufacturing of battery, its composition (materials, recycled content, and hazardous substances), carbon footprint, capacity, voltage, original power capability and other performance attributes, expected lifetime, and applicable warranty, among others.
2) Information available to **persons with a legitimate interest**[21] **and the commission** on detailed composition of the battery, parts and components, dismantling information, and safety measures.
3) Information available to **supervisory bodies and the commission only** on results of test reports demonstrating compliance to the regulation; and
4) Information available only to **persons with a legitim interest only** on values for performance and durability of the battery when placed on the market, and when it is subject to change, state of health, status of the battery (i.e., original, repurposed, re-used, remanufactured, or waste), and dynamic information resulting from its use, including number of charging, accidents, and periodically recorded information on the operating conditions.

The description of information under each category is provided throughout the regulation. In

[21] The regulation provides no explicit definition for "persons with a legitimate interest", however in its recital 124 it offers the following list: repairers, remanufacturers, second-life operators and recyclers, as well as *"those who have purchased the battery or parties acting on their behalf for the purpose of making the battery available to independent energy aggregators or energy market participants, evaluating its residual value or remaining lifetime for further use, and facilitating the preparation for re-use, preparation for repurposing, repurposing or remanufacturing of the battery"*.

Table 1 we summarize the most relevant articles and annexes referring to the passport and describing requirements for the information to be contained by it. The order of presentation in our table does not follow the order in which content appears in the regulation, instead we opt for a more natural order for the reader who is not familiar with its contents, as it gradually expands on previous demands. Note, our table is only indicative, and it does not intend to be exhaustive (nor replace the regulation when studying compliance with requests for battery passports).

Table 1 - Articles and Annexes relevant to battery passports

Reference	Title	Summary
Art. 77	Battery passport	Main article describing the batteries for which a passport shall be in place, with pointers to the information to be contained by the passport, and where applicable the purposes for accessing such information.
Annex XIII (1)	**Publicly accessible information relating to the battery model**	**Describes information to be contained by the passport regarding general information on the battery, material composition, carbon footprint, responsible sourcing, recycled content, share of renewable content, rated capacity, voltage with temperature ranges, original power capability with temperature ranges, expected lifetime, capacity threshold, temperature ranges the battery can withstand when not in use, commercial warranty, round trip efficiency, battery cell and pack resistance, c-rate, marking requirements, EU declaration of conformity, and prevention and management of waste.** **Includes pointers to other articles and annexes providing more details.**
Annex XIII (2)	Information relating to the battery model accessible only to persons with a legitimate interest and the commission	Describes information to be contained by the passport regarding detailed composition, part numbers for components and contact details of sources for replacement spares, dismantling information, and safety measures.
Annex XIII (3)	Information accessible only to notified bodies, market surveillance and the commission	Describes information to be contained by the passport regarding results of test reports proving compliance to the regulation.
Annex XIII (4)	**Information and data relating to an individual battery accessible only to persons with a legitimate interest**	**Describes information to be contained by the passport regarding values for performance and durability parameters, state of health, status, and information resulting from the battery's use.** **Includes pointers to other articles providing more details.**
Annex VI Part A	General information on batteries	Describes information to be contained by the passport regarding the manufacturer, category of battery, place and date of manufacturing, weight, capacity, chemistry, hazardous substances, and critical raw materials.
Art. 7	Carbon footprint of electric vehicle batteries, rechargeable industrial batteries and LMT batteries	Describes the a carbon footprint declaration to be drawn up for each battery model per manufacturing plant, containing at least admirative information about the manufacturer, information about the battery model, geographic location of manufacturing plant, the carbon footprint of the battery (with description of how to calculate it), a web link to a study supporting the values for carbon footprint. Includes pointers to other articles and annexes providing more details.

Reference	Title	Summary
Art. 52(3)	Disclosure of information on battery due diligence policies	Describes the report on the battery's due diligence policy, to be reviewed on an annual basis, containing information that is easily comprehensible for the end-use and clearly identifies the batteries concerned. The report shall contain, among others, the steps taken to comply with obligations, including impacts and risks, how they have been addressed, summary of findings by third-party verifications, and where relevant the public participation in decision-making on environmental matters.
Art. 8(1)	Recycled content in industrial batteries, electric vehicle batteries, LMT batteries and SLI batteries	Describes documentation containing information on percentage share of cobalt, lithium or nickel present in the active materials, and the percentage of lead that has been recovered from waste, for each battery model per year and manufacturing plant.
Art. 13	Labelling and marking of batteries	Describes a label containing information where applicable on battery's capacity, minimum average duration of battery when used in specific applications, indicating 'separate collection', among others.
Art. 18	EU declaration of conformity	Describes the Articles to which the declaration of conformity shall state compliance.
Art. 74(1)	Information on prevention and management of waste batteries	Describes information regarding the role of end-users in contributing to waste prevention, separate collection, treatments available for waste batteries, the necessary safety instructions, meaning of symbols and labels, the impact of substances, in particular hazardous, among others.
Art. 10	Performance and durability requirements for rechargeable industrial batteries, LMT batteries and electric vehicle batteries	Describes documentation to accompany batteries containing values for the electrochemical performance and durability parameters.
Art. 14	Information on the state of health and expected lifetime of batteries	Sets out requirements for information regarding state of health to be contained in the battery management system.
Annex IV	Electrochemical performance and durability requirements for LMT batteries, industrial batteries with a capacity greater than 2 kWh and electric vehicle batteries	Describes parameters related to electrochemical performance and durability (Part A), including rated capacity and capacity fade, power and power fade, internal resistance and internal resistance increase, where applicable, energy round trip efficiency and its fade, and the expected life-time of the battery under reference conditions. Describes elements to explain the measurements above (Part B).
Annex VII Part A	Parameters for determining the state of health of electric vehicle batteries, stationary battery energy storage systems and LMT batteries	Describes parameters for determining state of health of batteries. For electric vehicles: state of certified energy (SOCE). For stationary battery energy storage systems and LMT: remaining capacity, evolution of self-discharging rates, where possible the remaining power capacity, round trip efficiency, and ohmic resistance.

Reference	Title	Summary
Annex VII Part B	Parameters for determining the expected lifetime of stationary battery energy storage system sand LMT batteries	Describes the parameters: date of manufacture of battery, and date of putting into service, energy throughput, capacity throughput, tracking of harmful events, and the number of equivalent charge-discharge cycles.

As described in section 2, the demo considers participants in two roles: battery manufacturer and user. In the scope of the regulation, the battery manufacturer represents both a) the *economic operator placing the battery on the market*, which is responsible for ensuring the information in the passport is accurate, complete and up to date[22]; and b) a *person with legitimate interest*, as a potential repairer of its own manufactured batteries. While the user, according to the definitions of the regulation, represents a member of the public audience. We expect a user (or end-user) might be seen as a person with legitimate interest, but at the moment this is not defined in the regulation. The regulation merely states that the Commission will adopt implementing acts specifying which persons are to be considered persons with a legitimate interest by 18 August 2026[23]. For this reason, and for the purpose of demonstration, we consider in scope of our work the following two categories of passport information: publicly accessible information relating to the battery model, and information and data relating to an individual battery accessible only to persons with a legitimate interest. These are marked in bold in

[22] Battery Regulation, Article 77(4)
[23] Battery Regulation, Article 77(9)

Table 1.

Annex A summarises the demo requirements extracted from the regulation, keeping their original reference, as well as a parallel comparison with data attributes identified by the Battery Pass consortium, which is further described in the following section.

3.3 Battery Pass

To model the semantic model of an electric vehicle battery, we referred to the existing European initiatives of CatenaX and the Battery Pass. Specifically, we leveraged the semantic model provided by CatenaX [1]. Since the formatting of the meta model was not built considering the W3C Semantic Web Standards[3], but instead using the Semantic Aspect Meta Model (SAMM) we have assessed it would take longer to update existing tooling based on RDF Ontologies to support this meta model than it would to manually model the CatenaX concepts as RDF-based semantic model. As such, we've taken the input from the CatenaX model and used this to develop our own RDF ontology.

The translation process began by designing a base class *BatteryPass* as the domain of all the properties of the EV battery, physical and regulatory documentation, required in a battery passport. We also aimed for a low complexity of the ontology which can be easily visualized and understood by non-specialized people. Therefore, we have grouped all attributes based on the larger concept they refer to, resulting in a tree-like structure of the data with the *BatteryPass* class as the root and the low-level physical properties as the leaves.

However, the properties already modelled in the CatenaX meta model were not sufficient to address all the requirements presented in the Battery Pass data attribute longlist[2], thus we have introduced an additional module that builds on top of the existing properties. This is done by introducing new properties with as domain an already existing high-level concept. Unfortunately, some properties could not be attributed to an already existing high-level concept and thus we had to introduce new concepts ourselves. To maximise alignment with existing initiatives we have copied the explanations and the attribute titles from the Battery Pass longlist into the newly introduced concepts and properties.

The full ontology of the implemented battery is available from the authors.

3.4 Co-creation with partners

The ontology development for the demo battery passport was done in coordination with GTD-E partners Cleantron, ELEO and NXP in several sessions at the TNO Helmond location. No major issues were identified.

3.5 Learning experiences

We learned that sufficient information is publicly available to develop a battery-passport ontology that is usable for practical implementation.

4 Architecture and implementation

4.1 Considerations and Requirements

While the basics of a battery passport seem simple enough - it is a secure storage facility for data pertaining to a particular battery, there are some considerations that imply complexity. Here are some examples:[24]

1. The objectives that battery passports should contribute to realizing require **many distinct kinds of parties to have different kinds of access to specific parts of the battery data**. Such objectives include the support of sustainable production, enable authorities to verify compliance with legal obligations, enable transition to circular economy, provide new business opportunities for economic actors, and support consumers in making sustainable choices.
2. **The rights (and duties) to particular kinds of access change over time** as the battery proceeds through the value chain it happens to have become part of. Such changes occur, e.g., when batteries are included in, or removed from larger components (e.g., a car), or are imported/exported, etc.
3. **The kinds of data that may or must be included in a batter passport varies over time** yet must be maintained at a high level. Variations are induced, e.g., by changing legislation, or the need to support new business opportunities arise that need battery passport support. This requires the design of battery passports to cater for lots of flexibility.
4. For a battery passport to be effective, **the quality of its data must continuously be maintained**, i.e., the data must be correct, verifiable, and complete.
5. For a battery passport to be effective, it must **comply with various applicable EU regulations and/or directives**. This not only includes the new Batteries Regulation, but also the GDPR, the Digital Services Act, the Digital Markets Act, and possibly others.

From considerations such as these it will be obvious that providing a complete architectural description for battery passports cannot be included in a whitepaper such as this.

Also, these considerations lead us to believe that a generic architecture for battery passports should provide a minimal set of generic functionalities, each of which should be highly configurable. This would imply that a (complete) architecture should also include (generic) processes for the creation and maintenance of the various configurations, as well as mechanisms to ensure such processes are actually being run during the lifetime of the battery passport (which may exceed the lifetime of the battery itself).

This section proposes a (partial) architecture of battery passports that attempts to address various concerns related to the flexibility requirements that follow from the above considerations.

[24] Saari, L., Heilala, J., Heikkilä, T., Kääriäinen, J., Pulkkinen, A., & Rantala, T. (2022). *Digital product passport promotes sustainable manufacturing: whitepaper.* VTT Technical Research Centre of Finland, https://cris.vtt.fi/ws/portalfiles/portal/67162320/DPP_white_paper.pdf.

4.1.1 The battery passport

In its simplest form, a battery passport (BP, or just 'passport') is an IT-system (component) whose main function is to securely store data that pertains to a single battery (called the 'subject' of the BP), and to execute code (called 'scripts') that implements a specific functionality and enables such data to be processed (created, read, updated, deleted, archived, etc.) accordingly.

The functional flexibility required for BPs suggest to also include means for storing and manipulating objects other than battery related data. Scripts are examples of such objects, but there are others, such as configuration files, policy objects, or any data that is needed for the correct functioning of a BP.

In particular, the ability to upload, update and delete scripts is an essential capability for managing the functional flexibility of BPs. This capability allows BPs, e.g., to combine and/or anonymize data, to list the kinds of data or scripts in a BP, to provide data that identifies the BP's subject, to have the BP participate in cryptographic multi-party computation protocols, to move battery-related data to another BP, and so on.

To drive the execution of scripts, BPs would have both machine interfaces (APIs) and human interfaces (UIs) at (configurable) service endpoints, that enable them to receive requests for the execution of a script, and to return responses to.

We propose that BPs have:

- **access-control policies (ACPs)** that they use to determine whether or not to service such requests.
- **execution-control policies (ECPs)** that they use to guide the execution of the script, and
- **response-control policies (RCPs)** that they use to construct responses for the request and to determine where to send them to and what communications channel and/or protocol to use for that.

A BP can be in three states, which are transgressed sequentially (there is no going back to a previous state):

1. In its initial (unbound) state, the BP is not bound to any battery. In this state, a default set of scripts, policies, and data can be installed, e.g., for setting ownership of the BP, for binding a battery to the BP and filling it with the initial data for that battery.[25] The precise nature of such data depends on the regulations that need to be complied with, as well as any data needed for features that the manufacturer of the BP has implemented, e.g., as unique selling points.
2. When a battery is bound to the BP, the second state kicks in. In this state, the BP owner controls which scripts and policies are made available, e.g., to comply with legal obligations, but also to make certain business applications possible. This then determines who (else) can access which kinds of data in the BP, and/or use other functionalities.
3. When the battery that is bound to the BP ceases to exist, e.g., it is dismantled or otherwise put out of service, the BP enters its third state, in which battery-related data can no longer be created or updated. The BP shall cease to exist after the

[25] In case a (new) battery is created out of refurbished or otherwise reused materials, it is considered a new battery that needs (to be assigned) a new passport. However, in this case any data that is relevant for retaining history, should then be included in the initial data.

battery has been recycled[26]. Note that batteries, or their composite materials may be refurbished/reused, in which case a new battery is created that will need a fresh, new passport.

The essence of how a BP works is simple: it awaits requests, processes such requests, and returns responses, as illustrated in the figure below:

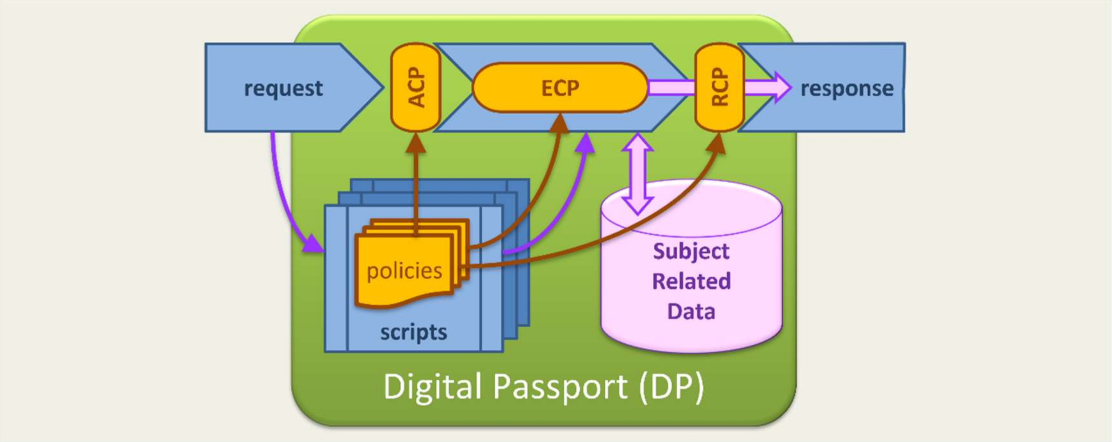


Figure 5: the conceptual working of a Digital Battery Passport

In a bit more detail, a BP becomes active when it receives a request to do something, either through an API (in case the request is done from some other IT component), or through a UI (in case the request originates from a person). This starts a session, which is the time interval between receiving a request and sending the response (after processing). A request specifies the script that its sender wants the BP to execute, and typically contains additional data that is needed by (and specified for) the particular kind of request. Such data would typically be included to help evaluate the ACP, ECP and RCP associated with the script, or to execute the script itself. If a request does not specify all necessary data, the BP may engage in further communications until all data has become available (either from such communications, or from the BP's internal storage means) or the sender quits the session[27].

When a BP has received a request to execute a specific script and all other necessary data, the ACP associated with the script is evaluated to determine whether the request should be serviced. If the request is to be serviced, the script is executed, taking the guidance of the corresponding ECP into account. The result of this processing is then stored in the BP's internal data store and/or converted into a response, which is subsequently output in accordance with the RCP, which specifies how, and by means of which communications channel (implying an interface and a protocol), the result will be conveyed as the response to the request.

For transparency and traceability, any changes in the internal data set, as well as any requests received and responses given to such requests, are (to be) securely logged, meaning that it should be practically impossible to rewrite the history of such log so that it can serve as evidence in cases of disputes.

[26] Battery Regulation, Article 77(8)
[27] This is in line with the DEMO pattern of a business transaction.

4.1.2 Session-, Identity and Access Management

Whenever a BP receives a service request, it determines whether or not it has a script that could service the request. If it does not, it responds with a 'cannot service the request' exception. If there is such a script, it starts a session at the script's service request entry point. When execution returns, the session is terminated.

Every (active) session has an identifier that enables it to be distinguished from all other sessions within the BP. Scripts are provided with the identifier, enabling them to keep all communications relating to the service request within a single context (the session), which is required, e.g., for executing the same service request from different users simultaneously.

A BP has a registration that enables scripts to manage and use characteristics of parties that it communicates with, such as roles, permissions, or mandates that they have been assigned, or configurations and/or preferences (e.g., of user interfaces). We use the term **account (of a user)** (or: user account) to refer to the registration of all such characteristics that pertain to a single user.

Typically, accounts contain data (e.g., a username and password, or an API-key) that enables scripts to determine which of them is associated with the user from which it has received a service request.[28] They may also contain data that states the communications channels (networks, protocols and endpoints) through which they can be reached, as well as other data that all scripts could use.

Accounts also contain data about users that is particular to scripts, and that (therefor) is also managed by the individual scripts, such as the permissions, roles or mandates that are assigned to users. Thus, scripts can maintain session states in the accounts of their users.

The management of the account registration of a BP is just another function that BPs can perform. This implies BPs will have a corresponding script that itself might use the registration in which it maintains the permissions, roles and mandates associated with account management.

Note that scripts are not required to use this registration. Scripts that do not maintain states don't need such a registration, as they will obtain all information they need from the service request or subsequent communications with the user.[29]

4.1.3 Scripts and their Policies

As a BP needs scripts and associated policies to function, it helps if there are (preferably standardized) mechanisms for their support and management. In this section, we highlight some principles that could help establish these.

4.1.3.1 Scripts

First, every script implements a particular function that serves particular and specified purposes. Regulations, such as the EU regulation for batteries, already state various such

[28] This process is commonly referred to as (identification and) authentication.

[29] This is the way that various webshops work: customers may choose whether or not to create an account. If they do, they won't need to provide their addresses, phone numbers etc. in subsequent visits. If they don't, they must provide that data again.

purposes, as well as different (high level) functions that BPs should support. It also states that other functions could exist, e.g., for commercial purposes.

We propose to base the design of a script on the DEMO transaction model, which consists of three phases:

1. In the first phase, the user and the script exchange data with each other that enable them to decide whether or not to proceed with executing the actual function (transaction). This not only entails establishing whether or not the user is entitled to have the function executed, but also that all data that is necessary for completing the transaction is available. We postulate that the Access Control Policy (ACP) of a script specifies what data is necessary, and how it can be established that this data is valid for making this decision (and completing the transaction).
2. In the second phase, that starts after both the user and the script have implicitly or explicitly decided that the function will be executed, such execution takes place. This may entail further communications with the user, or not. Execution of a function may include other transactions – calling other scripts. We postulate that the Execution Control Policy (ECP) of a script specifies the details of that, e.g., what the user interface would look like, what configuration parameters or preferences exist, etc.
3. In the last phase, the end-result is communicated to the requesting party, through an appropriate communications channel. The Response Control Policy (RCP) of a script specifies how this result is packaged, and through which communications channel it is transmitted. Packaging a result may be, for example, converting the result into a verifiable credential that is subsequently issued to the requester, or turning it into a PDF that is sent to the requesters e-mail address,

The following sections will provide some more details about these stages.

4.1.3.2 Access Control Policies (ACPs)

A function typically consists of a coherent set of activities that can be performed on some data object (or coherent set of data objects). The ACP needs the ability to determine

- whether a user is entitled to have such an activity executed. We will use Role Based Access Control (RBAC) for this.
- whether all data that the execution of such an activity requires, is available (in the expected syntax and semantics), and is valid (which means that when the data is used for further processing in the activity, any risk associated with the data not being valid, is acceptable).

4.1.3.2.1 RBAC

It is a common practice that (coherent) subsets of such activities can be executed by specific actors. We say that a **role** is the set of rights/duties for executing a particular, coherent subset of activities (that belong to a particular function or script). Actors can be assigned roles, which means that the script will execute any of these activities upon such an actor's request.

Some roles (i.e., their names, and rights/duties) are already (partly) defined by the EU regulation, such as the economic operator, independent operator, manufacturer, importer, authorized representatitve, distributor, fulfilment service provider, etc.[30] Others can be added as needed.

[30] Battery Regulation, Article 3(22).

For each role in every function, it must be defined who should be allowed to perform such a role (i.e., what conditions should be satisfied), how such roles are assigned in practice, both in terms of assessing whether the conditions are satisfied, and in terms of creating artifacts that (a) attest to this role assignment, (b) can be made available to appropriate BPs and (c) can be verified and validated by such BPs. Such artifacts could be, e.g., a verifiable credential, or a record in an identity- or account registration.

Particular attention must be paid to situations in which role assignments have to be revoked (or suspended), as we know from practice that this is often overlooked, and is known to be a vulnerability that can lead to fraud.

4.1.3.2.2 Data Verification and Validation

The kinds of data that a script needs to execute a particular activity are part of its design. However, this design should not only specify these kinds of data – their syntax, and semantics, but also what acceptable sources for such data are and what assurances must come with such data in order to be accepted as valid for the activity to use. This is not a trivial exercise.

A script must have the means to request for such data, and in such a way that the responder (typically: the user) would be able to not only provide the data, but also the proofs that the script needs to determine its validity for using it in the particular activity. This can be done, e.g., using Presentation Requests and Presentations as being developed by W3C.[31]

4.1.3.3 Execution Control Policies

Executing a task that produces specified results, such as the servicing of a particular request, can usually be done in a variety of ways. For example, a request to obtain the full status of a battery would produce a status-object, the contents of which might depend on the role(s) or other characteristics of the user from which the request was received. Manufacturers, for example, might see manufacturer-related data that non-manufacturers might not get.

Execution control policies need not be identifiable objects; they could be integrated in the code of the script. This is an easy way of working, but the consequence is also that a change in the execution control policies would then require an update of the script.

4.1.3.4 Response Control Policies

After a particular result (e.g., some data elements, process status, etc. that is requested, or a denial of a service request, or some exception/error condition) has been produced, it needs to be sent to the user. However, a single result may be sent to the user in different ways, and they are not only distinguished in terms of a GUI (for human users) or an API (for IT-components). And sometimes, the result needs to be 'packaged', similar to a (physical) letter that is packaged into an envelope.

Response control policies determine how a result is sent to the user, i.e., which communication channels may be used, and for each of them, whether (and how) the result needs to be converted and/or packaged before it is transmitted. For example, some results can be sent through an API after being converted to, e.g., JSON or XML, and/or packaged, e.g., into (verifiable) credentials or certificates.

[31] W3C Verifiable Credentials Data Model, v 2.0, and W3C Verifiable Presentations Request spec.

As with the other policies, RCPs can also be integrated in the code of scripts. Alternatively, a library of conversion and packaging routines might be created that all scripts can use.

4.1.4 Script Management

Script management is about the processes that deal with all kinds of changes that affect scripts, such as changes in:

- Legislation. Such changes could imply changes in the data that must be kept in the battery passport, or their processing, which would affect certain scripts.
- Battery ownership. Such changes need to become available in the battery passport, and may affect a script that has a hard-coded policy with a hard-coded battery owner.
- Passport ownership. A new owner could revise the set of scripts within the passport, as well as changes in the various policies.
- Passport data ownership. It is realistic to assume that a battery passport contains data that is owned by others than the battery or passport owner. It is also conceivable that data owners are given the right of having particular scripts installed that operate on their data.
- Business opportunities. New business opportunities could imply changes in the set of scripts

It is conceivable that a 'script management script' is designed and developed that enables parties that have particular rights (or duties) to download, upload and/or remove scripts from battery passports.

4.2 Implementation

4.2.1 Digital passport system explained

In order to get a grip on the world of digital passports a website[32] is being build, containing a blueprint for the construction and operation of the Digital Passport system. The information found, will help readers understand who the stakeholders are, what the regulations are and which architectural viewpoints should be taken into account.

4.2.2 Technical infrastructure

To have a scalable and manageable environment for the implementation of the data space, a kubernetes[33] cluster (k8s) is used to deploy the needed services and data space connectors. Kubernetes also allows for managed deployment using Helm[34]. Using this platform a participant connector can easily be added to the data space.

Using helm scripts, docker images (containers) are configured and deployed in the k8s cluster, containing the minimal necessary service to provide the data space functionality.

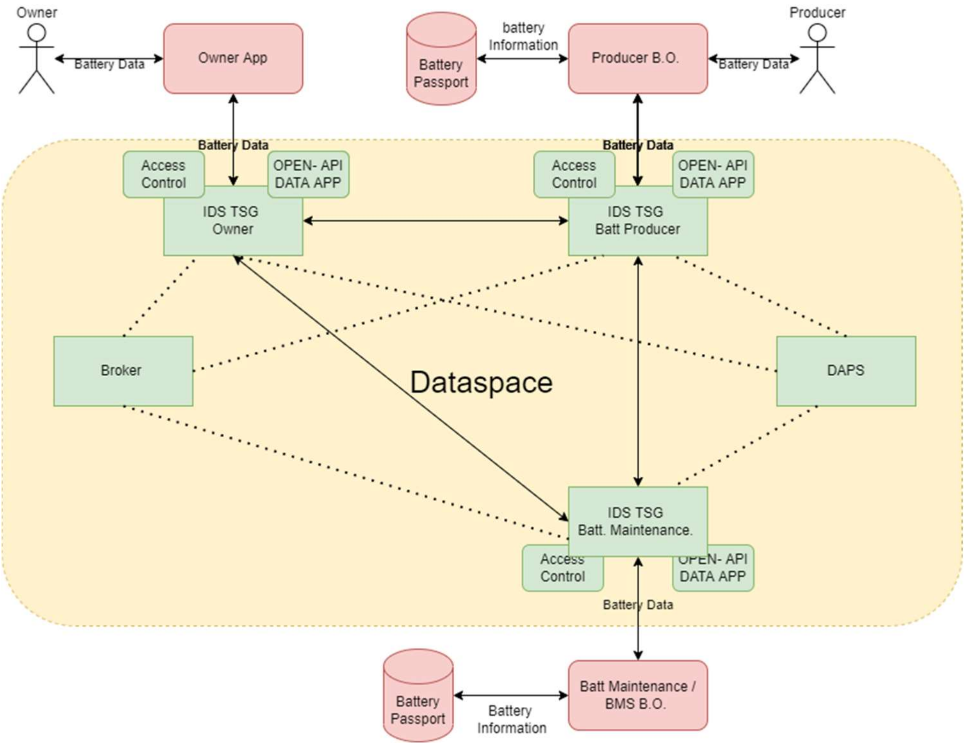
The data space infrastructure is based on the RAM 3.0 (Reference Architecture Model)[35], published by the IDSA

Used services:

[32] Introduction | TNO Digital Passports (digital-passport.org)
[33] Kubernetes is an open-source system for automating deployment, scaling, and management of containerized applications
[34] Helm is the package manager for Kubernetes
[35] IDS-RAM 3.0 - International Data Spaces

- Dynamic Attribute Provisioning Service (DAPS), used for identification and authentication of data space participants
- Metadata Broker, contains an endpoint for the registration, publication, maintenance, and query of Self-Descriptions.

To provide the connectivity between the data space - and the participant environment, the TSG (TNO Secure Gateway)[36] is used. This open-source connector implements the specifications outlined in the IDSA RAM and the IDS Information Model[37]



The above high level architecture image depicts the connections between the different services and components used to create the dataspace. The red parts are situated in the participant domain and the green parts are hosted part of the data space

4.2.3 Identification and Authentication

On of the most important parts of a data space is the ability to identify and authenticate the participants in the data space. Due to the legal regulation metioned before access to data has to be provided to certain participants in the data space, and in order to give access to data, a data owner needs to know who he gives access to. The DAPS (managed by a trusted authority) will provide the identities used in communication and can add attributes to enable participants to identify types of participants and with this information grant or deny access to data.

[36] TNO Security Gateway Documentation (tno-tsg.gitlab.io)
[37] International-Data-Spaces-Association/InformationModel: The Information Model of the International Data Spaces implements the IDS reference architecture as an extensible, machine readable and technology independent data model. (github.com)

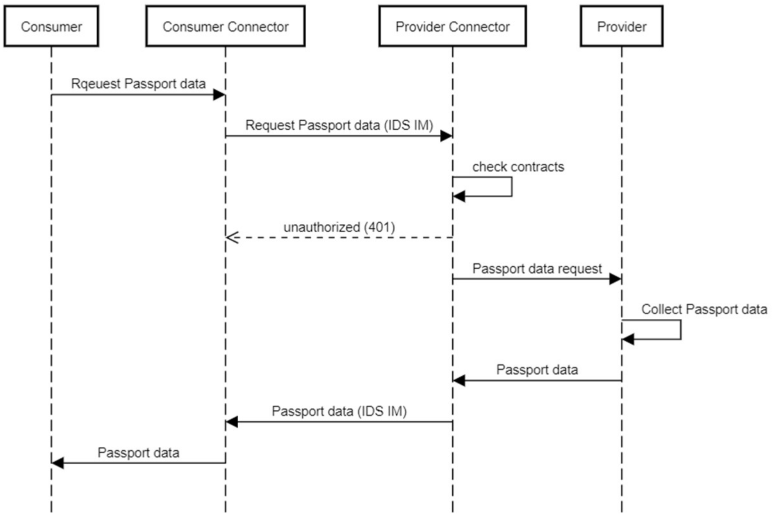
For this demo implementation a scenario with a set of known participants is created and although possible the ability to give access to data based on the participant's provided attributes is not implemented into the scenario.

4.2.4 Authorization to access Distributed Passport Data

With the principles of data sovereignty in mind, the passport data is located in the domain of the data owner, which enables the owner (data provider) to control access to the data.

Access control is handled by the TSG. Built into the connector is an authorization module, which is based on contract agreements, described in the Open Digital Rights Language (ODRL)[38], between participants (data consumers and data providers), can allow or deny the request and therefor access to data. Every request will be passed through this module and checked against the agreed contracts between the consumer and the provider.

Once authorized the request will be passed to the data provider, who then can handle the request and send the requested data back to the consumer.



4.2.5 OpenApi

Request for battery passport content are formatted according to the OpenAPI[39] specification[40] designed specifically for the Digital Battery Passport. Using the open-source TSG Open-API Data app[41], created by TNO, the participant environment plugs into the TSG and handles the request from both the data-consumer and the data-provider.

[38] ODRL Information Model 2.2 (w3.org)
[39] Home 2024 - OpenAPI Initiative (openapis.org)
[40] API | TNO Digital Passports (digital-passport.org)
[41] TNO Security Gateway / Data Apps / OpenAPI · GitLab

4.3 Learning experiences

On first sight sharing Digital Battery Passport information does not seems different to many other data sharing environments, but after looking more into this particular subject more regulations and details came to light. We learned from this to not only look into the ability of sharing data but also keep sight of the rules and laws concerning the data.

Due to the above mentioned laws and rules in combination with data sovereignty, linked data comes into view. Sharing multi level linked data, links to links, requires a different look at authorization in combination with laws and rules.

5 Demonstration

This section describes the operation of our demonstration implementation of a battery passport. It includes screenshots of the demo walk-through, demo scenario, user interface, snippets of code, as well as some documentation. The full documentation and further details can be found at https://docu.digital-passport.org/docs/System%20Architecture/sysarch-overview/. Please contact the authors for a demonstration, or for trying out our demo implementation yourself. You can see a video recording of a demonstration here: https://docu.digital-passport.org/demo.

To show the functionalities described in previous chapters, a demonstrator was build. This demonstrator contains the basic functionalities needed to show the sharing and access control of passport data between different parties.

The demonstrator consists of a data space for three business roles (see also section 2.2):

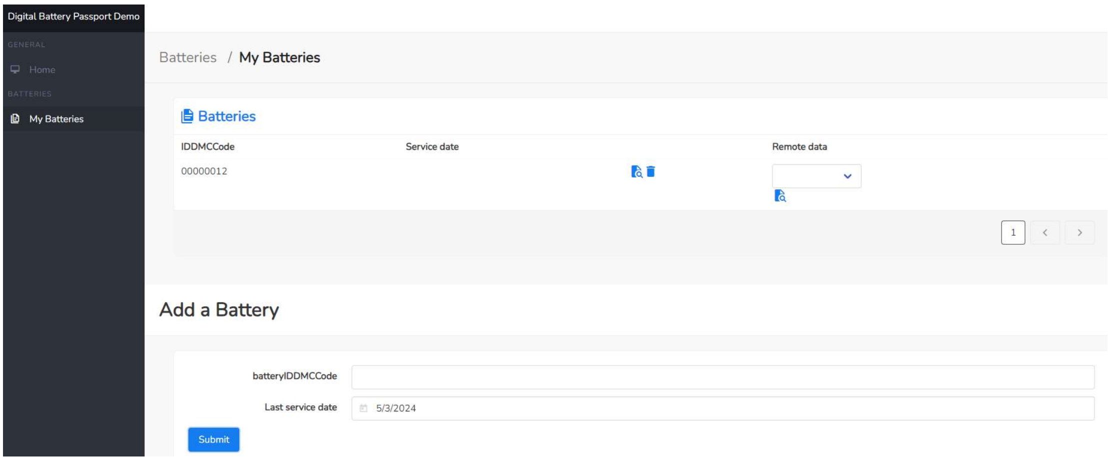
- Battery owner, e.g. the owner of the vehicle;
- Battery passport service provider;
- Battery manufacturer.

Each of the participants holds part of the passport data. In this demonstrator, this is represented by basic data such as manufacturer date, last service date, and a few basic sensor reading from the management system.

Each participant has his own web application, data storage and an API to access the stored passport data, which is situated in the participant’s own infrastructure (e.g. a mobile phone app or a back-office application). The data is shared through the data space when another participants requests the data, and has access to it. Connection to the data space is handled by a standard connector configured with an OpenAPI specification. For this demonstrator the participant UI is web based, though this is only a front-end visualization and could be implemented on various platforms in a multitude of ways.

5.1 User interfaces for the three roles

Because the three roles in this demonstrator have different passport data they each have their own user interface (UI), see Figures 6, 7 and 8.



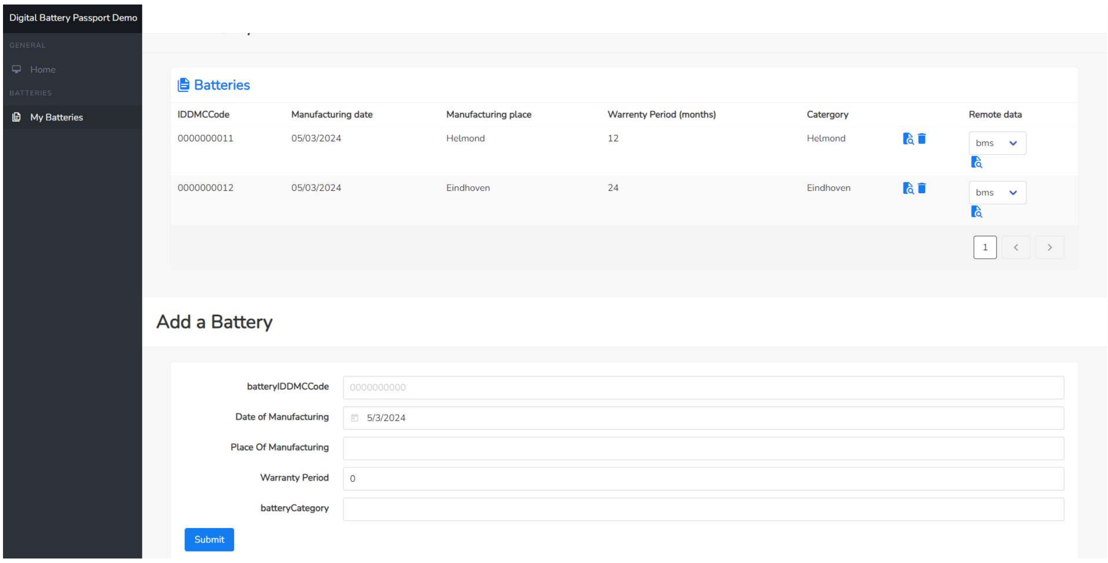
Batteries

IDDMCCode	Service date		Remote data
00000012			

Add a Battery

batteryIDDMCCode	
Last service date	5/3/2024

Figure 6: Web user interface for the battery-owner role. E.g. service history.



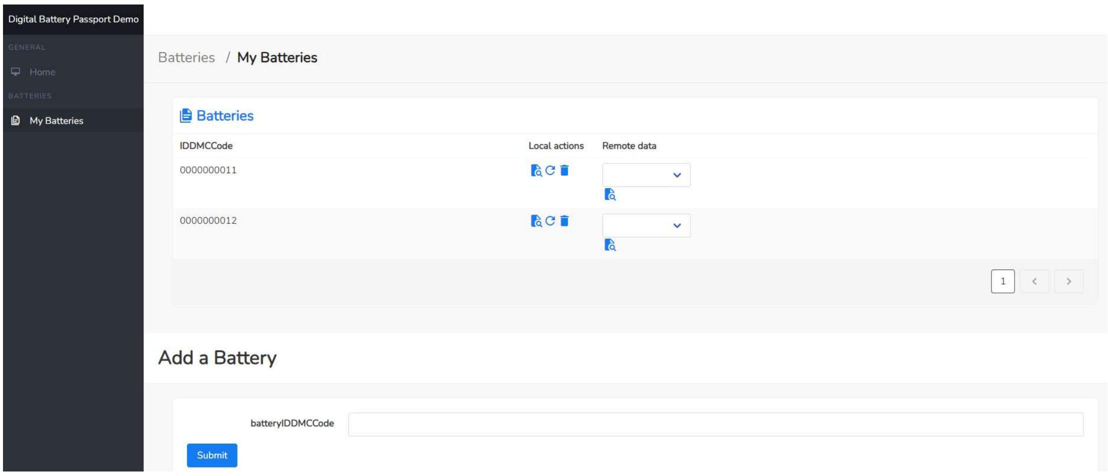
Batteries

IDDMCCode	Manufacturing date	Manufacturing place	Warrenty Period (months)	Catergory		Remote data
0000000011	05/03/2024	Helmond	12	Helmond		bms
0000000012	05/03/2024	Eindhoven	24	Eindhoven		bms

Add a Battery

batteryIDDMCCode	0000000000
Date of Manufacturing	5/3/2024
Place Of Manufacturing	
Warranty Period	0
batteryCategory	

Figure 7: Web user interface for the battery-manufacturer role. E.g. manufacturing provenance.



IDDMCCode	Local actions	Remote data
0000000011	🔍 ↻ 🗑	⌄ 🔍
0000000012	🔍 ↻ 🗑	⌄ 🔍

Figure 8: Web user interface for the battery-passport-service-provider role. E.g. sensor data.

In each UI, batteries can be added which will be stored locally in the corresponding environment. The battery-passport-service-provider UI has one extra feature: when a battery is added the data from the back office sensor data storage is accessed to request the last known sensor values.

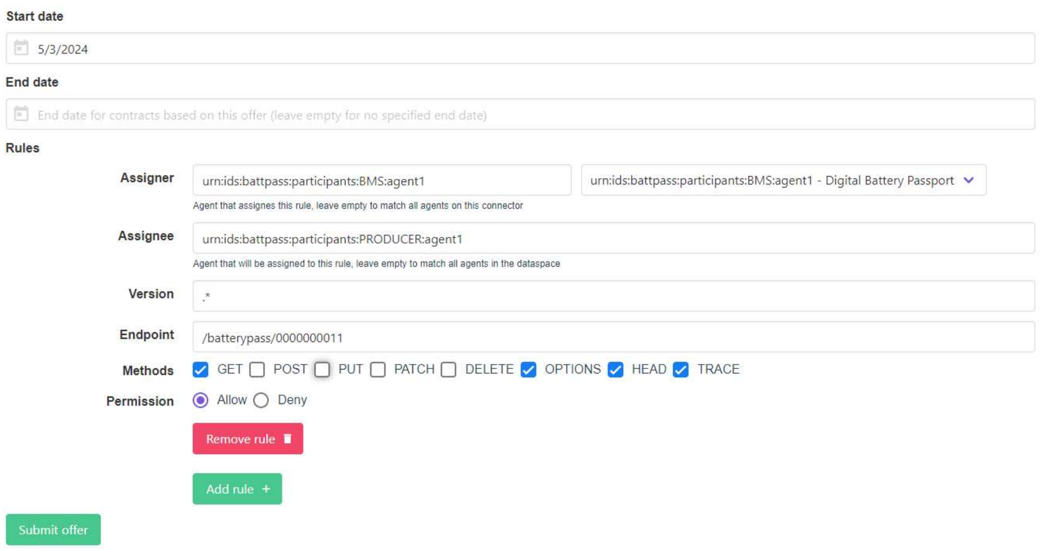
When a battery is added it will be shown in the table with the functionalities available for this UI, see Table 2.

Table 2: Actions on selected battery passport via the user interface (UI)

Icon	Meaning
🔍	Show the details for this battery passport
↻	Refresh sensor data from systems (service provider only)
🗑	Remove this battery passport from the local storage
⌄ 🔍	Get access to data stored and managed by another party.

5.2 Providing access to battery data

Any of the three roles acts as data owner for their own data. Any of the three roles can request others for access to their data. Providing this access is done through an open-api data app where the data owner (“assigner” in the demo) creates a so called “offer” to the data requestor (“assignee” in the demo), see Figure 9.



Start date

5/3/2024

End date

End date for contracts based on this offer (leave empty for no specified end date)

Rules

Assigner: urn:ids:battpass:participants:BMS:agent1 | urn:ids:battpass:participants:BMS:agent1 - Digital Battery Passport

Agent that assignes this rule, leave empty to match all agents on this connector

Assignee: urn:ids:battpass:participants:PRODUCER:agent1

Agent that will be assigned to this rule, leave empty to match all agents in the dataspace

Version: .*

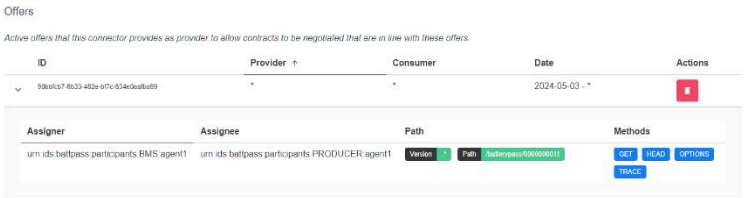
Endpoint: /batterypass/0000000011

Methods: ☑ GET ☐ POST ☐ PUT ☐ PATCH ☐ DELETE ☑ OPTIONS ☑ HEAD ☑ TRACE

Permission: ● Allow ○ Deny

Figure 9: Example offer, where Assigner BMS:agent1 gives access to Assignee PRODUCER:agent1 to their data for battery 0000000011.

As there may be multiple offers for the connector from the assigner to an assignee (e.g. multiple batteries), these are collected in a list, see Figure 10.



Offers

Active offers that this connector provides as provider to allow contracts to be negotiated that are in line with these offers

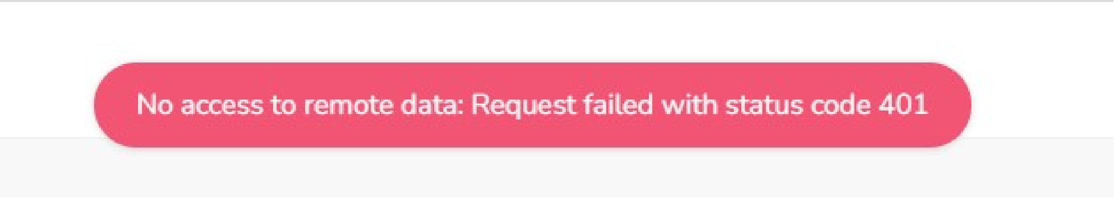
ID	Provider ↑	Consumer	Date	Actions
90bbfcb7-6b33-482e-bf7c-634e0aafba99	*	*	2024-05-03 - *	

Assigner	Assignee	Path	Methods
urn:ids:battpass:participants:BMS:agent1	urn:ids:battpass:participants:PRODUCER:agent1	Version .* Path /batterypass/0000000011	GET HEAD OPTIONS TRACE

Figure 10: List of offers for a specific connector

This offer will be used when this participant requests access to another participants data. In this example access is given to a specific battery passport, but by using wildcards for either the “Endpoint” or the “Assignee” contract will be agreed upon without restrictions on which battery passport is requested of by whom it is requested.

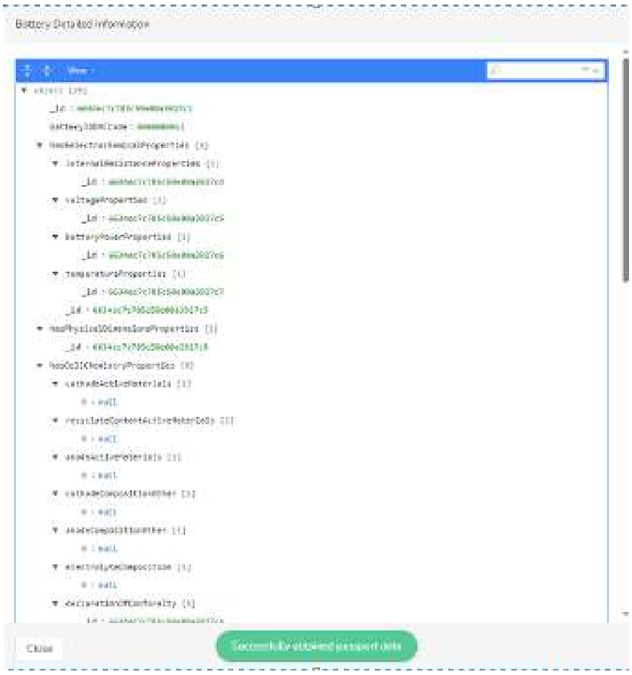
When the offer is accepted and access is agreed, the passport data will be sent. If there is no offer or the permission is set to denied the participant will receive a HTTP 401 response and denied access to the data, see Figure 11.



No access to remote data: Request failed with status code 401

Figure 11: Example of error message, when data is requested without associated offer or permission

When access to the requested data is given, the data is provided in the structure of the ontology as described in the previous chapters, see Figure 12.



Battery Detailed Information

```
▼ object {29}
    _id : [illegible]
    batteryIDDMCCode : [illegible]
  ▼ hasElectrochemicalProperties {5}
    ▼ internalResistanceProperties {1}
        _id : [illegible]
    ▼ voltageProperties {1}
        _id : [illegible]
    ▼ batteryPowerProperties {1}
        _id : [illegible]
    ▼ temperatureProperties {1}
        _id : [illegible]
      _id : [illegible]
  ▼ hasPhysicalDimensionsProperties {1}
      _id : [illegible]
  ▼ hasCellChemistryProperties {8}
    ▼ cathodeActiveMaterials [1]
        0 : null
    ▼ recycledContentActiveMaterials [1]
        0 : null
    ▼ anodeActiveMaterials [1]
        0 : null
    ▼ cathodeCompositionOther [1]
        0 : null
    ▼ anodeCompositionOther [1]
        0 : null
    ▼ electrolyteComposition [1]
        0 : null
    ▼ declarationOfConformity {1}
        _id : [illegible]
```

Figure 12: Providing of the requested data according to the standardised ontology.

6 Conclusions and recommendations

6.1 Conclusions

While the basics of a battery passport seem simple enough, various considerations would cause passport architectures to quickly become complex. For example, there are many different stakeholders that have different rights and duties regarding various battery data. Also, many changes need to be accommodated for over time, such as changes in legislation, business opportunities, owners and other stakeholders, the kinds of data that may or must be stored, the ways in which the quality of the passport data is monitored and controlled, etc.

One of the major problems is the flexibility that battery passports need to exhibit, e.g., in terms of functionality and configurations. While the (architecture of the) battery passport that we have used in our experiments is working, it is also way too simple for supporting the necessary flexibility.

Thus, we have considered what a simple, functional architecture for a battery passport (IT component) might look like that we expect can be used to realize the required flexibility. In this architecture, the flexibility is achieved by having every function implemented by a particular script (and policies for various configurations and preferences) and requiring that there be a 'script management script' to control that flexibility.

Research question

Our main research question was as follows

Can battery passports be technologically viably used in the mobility domain (Electric Vehicle, including heavy mobile machinery) and grid-battery industry?

We can answer this question positively. All technologies are available and implementable. The relevant data models are known and available. Challenges remain integration and scalability. We have also identified the key role of a battery-passport service provider.

Sub-questions

1. Is sufficient harmonization of battery-passport data possible between manufacturers?

We suspect a positive answer. Even though only two battery manufacturers (ELEO and Cleantron) were involved, there was sufficient guidance from the European regulations and the Battery Pass project to assure interoperability of battery-passport data between the manufacturers. Our demo showed “happy flows” for all relevant data exchanges.

2. Can the integrity and provenance of battery passport data be sufficiently guaranteed?

This question is for further study, see also the recommendations.

3. Is there an access control model for battery passport data that would be acceptable to all relevant stakeholders, for managing confidentiality, regulatory access to data, ownership (control, possession), and transfer of ownership, and such?

We suspect a positive answer. The access model of our demo assures that data can only be accessed when there is an offer by the data owner for this data.

4. Can the questions above answered positively, such that they also comply to the applicable European regulation?

The data model and ontology used in our demo was compliant to the European regulation on battery passports. A full legal analysis is for further study.

5. Can the questions above answered positively, such that the battery passport adds relevant value to battery+BMS products in terms of money and environment?

The immediate business case for battery passports is compliance to European regulation, and avoidance of associated non-compliance penalties. We suspect that the exchange of battery-passport data has positive business value for all involved roles. However, this is again for further study.

6.2 Recommendations

As we have seen, battery passports need to be very flexible, not only to accommodate legally or otherwise required data and functions, but also to accommodate for changes in such functionality and data, the ownership of the battery, the passport for that battery, and possibly also particular data concerning the battery or its passport. Also, during the lifetime of a battery, an ever-increasing number of parties will need to fulfil particular roles, such as authorized representatives, importers, distributors, fulfilment service providers, etc. We recommend:

- Creating and maintaining an inventory of battery passport functions, that not only specifies functions and roles, but also states what (if anything) it contributes to the compliance of such a passport with various regulations.
- Creating and maintaining an inventory of associated processes, e.g., for the governance, management, maintenance and innovation of battery passports. These are needed for further scalability (more participants, more batteries, ...) and higher technology-readiness levels (now TRL5).
- This project did not cover how a battery passport deals with attacks by malicious actors, as such we recommend further research into this topic to ensure the battery passport system can be trustworthy. This would include both physical security (e.g. integrity of QR codes on batteries) and IT/cyber security (confidentiality, integrity, accessibility).

We expect such inventories to facilitate the further development of a pervasively useable battery passport architecture and validate it.

ICT, Strategy & Policy

Anna van Buerenplein 1
2595 DA Den Haag
www.tno.nl

TNO innovation for life