EVS38
Göteborg, Sweden, June 15-18, 2025

Battery Passport - Challenges in Transitioning from Regulation to Implementation

Avedis Dadikozyan [1], Subhajeet Rath[1], Erwin Somers[2], Sjoerd Rongen[2], Wenzel Prochazka[4], Henk Jan Bergveld[3] and Erik Hoedemaekers[1]

[1] *TNO, Dept. of Powertrains, Helmond, Netherlands (avedis.dadikozyan@tno.nl)*

[2] *TNO, Dept. of Data Ecosystems, Eindhoven, Netherlands*

[3] *NXP Semiconductors, Eindhoven, Netherlands*

[4] *NXP Semiconductors, Gratkorn, Austria*

Executive Summary

This paper explores the transition from regulatory intent to practical implementation of the EU-mandated battery passport. Key challenges include the realization of a decentralized, interoperable data architecture, the secure collection and synchronization of BMS lifecycle data, and the standardization of battery state estimation algorithms. We present a functional demonstrator developed through the GTD-E project and extended in SeBaPaD, which integrates a digital product passport (DPP), embedded BMS hardware with secure elements, and validated algorithms for key metrics such as State-of-Health and round-trip efficiency. The system leverages semantic data models, data sovereignty principles, and edge/cloud computation to generate trusted passport data across the battery lifecycle. This work highlights the technical feasibility of a regulation-compliant battery passport while identifying open challenges in data governance, trust, and scalability.

Keywords: digital battery passport, battery algorithms, digital passport interoperability, data security.

1 Introduction

Building a sustainable battery economy demands more than innovation in chemistry and engineering. It requires full transparency across every stage of a battery's life, from raw material sourcing to end-of-life management. In 2023, the European Parliament adopted the Battery Regulation (EU) 2023/1542 [1], mandating the creation of a "battery passport" — a digital record containing essential data about a battery's materials, usage, repair, and end-of-life management. The battery passport is expected to support circular economy goals by ensuring responsible sourcing and enabling second-life use. However, the implementation of the battery passport is not straightforward - it requires robust data reporting, a reliable system architecture, comprehensive security, and coordinated collaboration throughout the industry.

Recent efforts, including the publication of the DIN DKE SPEC 99100:2025-02 [2], have laid important foundational frameworks for defining the key data attributes, data formats, and security protocols that must be captured across a battery's lifecycle. Organizations like TNO and NXP are playing vital roles in the technical realization of the Battery Passport. TNO is focusing on data architecture, battery parameter estimation, and semantic alignment [3, 4, 5], while NXP is concentrating on designing secure Battery Management Systems (BMS) hardware and ensuring robust data protection. However, significant gaps

remain between regulatory goals and technical readiness. In particular, while the DIN document provides valuable direction on what data needs to be captured, it offers limited guidance on how to securely generate, collect, validate, and synchronize this data within real-world systems.

This paper explores three key technological pillars that require attention to achieve a fully functional battery passport: (1) the design of interoperable digital passport architecture that respect data sovereignty and allows for scalable, multi-stakeholder collaboration; (2) secure data collection and synchronization through BMS hardware enhancements, including the integration of secure elements; and (3) standardization and optimization of algorithms needed to compute passport-relevant battery parameters, such as State-of-Health (SoH) and round-trip efficiency. We present a practical demonstrator that integrates these elements, combining secure BMS data capture, real-time cloud synchronization, and semantic data harmonization to meet emerging regulatory requirements.

The remainder of this paper is structured as follows. Section 2 discusses the software architecture of the digital battery passport. Section 3 addresses secure data collection mechanisms on the BMS and synchronization with external systems, along with the need for standardizing BMS algorithms in line with passport data requirements. Section 4 describes the development of a working battery passport demonstrator. Finally, Section 5 summarizes the conclusions and outlines future directions, including areas where current guidelines require further extension to fully support compliant and practical battery passport implementations.

2 Digital Passport Architecture

Though we have experimented with data-space architectures and results so far are promising, more work is needed to ensure these work for both static (e.g. manufacturing date) and dynamic data (e.g. number of charging cycles), as well as public access (for all), restricted access (for e.g. customs agents) and granted access (for specific parties, such as the owner).

In Figure 1 an overview of the various aspects of the battery passport and access to that are presented. Specifically, it shows how the QR code on the battery should reference to the publicly accessible data, as well as the data to which access is restricted. To provide this specific access, a data sharing infrastructure is needed, which gives a requester of data access to the actual battery passport as provided by the responsible Economic Operator and containing data for various audiences with differing access. All while falling under the EU Battery Regulation [1].

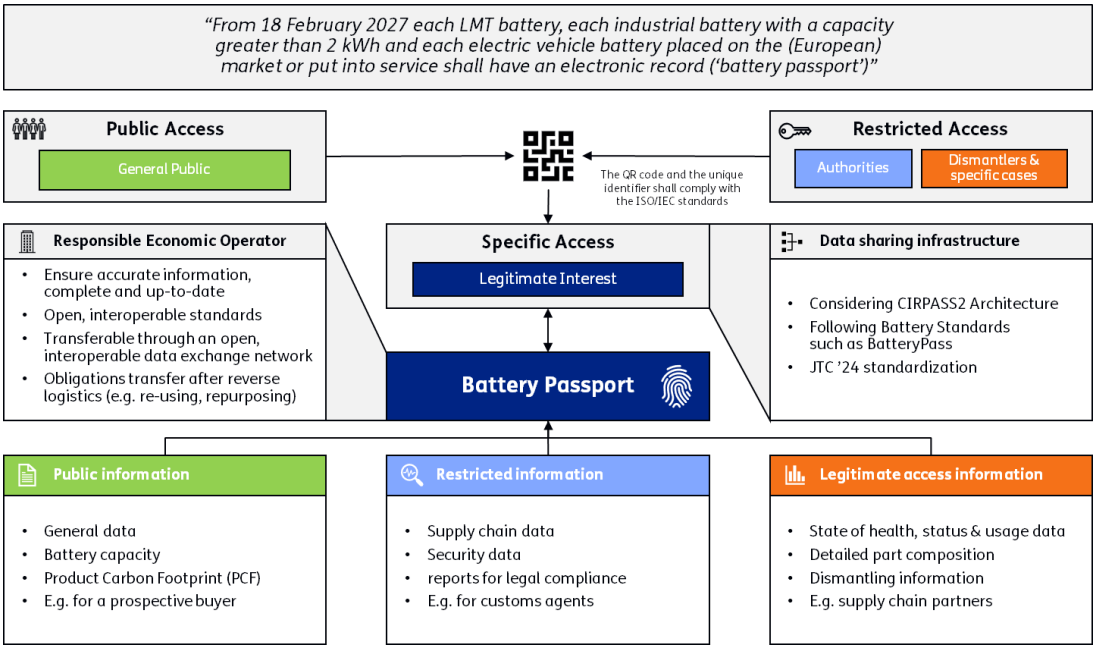


Figure 1: Digital Passport Architecture Overview.

2.1 Architecture and Data Sovereignty

In our battery passport implementation, we make use of the data-space design as described by the International data-spaces Association (IDSA) in the data-space Reference Architecture Model (IDS-RAM) [7]. IDS-RAM provides a modular framework that integrates existing technologies and standards to create an interoperable system where participants retain full control over their data. This means that organizations are able to decide how, when, and with whom they share their data—ensuring that no one misuses or improperly distributes sensitive information. This concept of data sovereignty is particularly important in the context of digital passports, as it ensures that battery manufacturers, users, and other stakeholders can safely exchange information without compromising their control. For example, when a manufacturer produces a battery, they can control who sees their battery's specifications, and they can restrict access to sensitive data, such as performance data, to certain parties (like certified repair centers or regulators). The system ensures that this data is always under their control, even if it is shared across multiple organizations. This architecture aligns with the requirements set out in DIN 77010 [7, 8, 9], which aims to standardize how this information should be structured and exchanged to ensure transparency and compliance with European regulations.

While this architecture provides a solid foundation, there are still challenges in scaling and applying it across diverse industry contexts. The architecture supports authorized data access and shared understanding of data semantics, but practical implementation, particularly concerning interoperability and data sharing across multiple, varied systems, remains an area requiring further refinement. As the EU Battery Regulation demands not only accessibility and portability but also protection and provenance of battery-related data, ensuring these elements in a real-world system requires additional technical and regulatory alignment [10].

2.2 Semantic Interoperability and Vocabulary Hubs

For DPPs to work effectively, interoperability is crucial. This involves not just technical compatibility but also ensuring a shared understanding of the data's meaning across different stakeholders. This is where semantic interoperability comes into play. In line with DIN 77010's guidelines for consistent data interpretation, the battery passport data-space utilizes vocabulary hubs. These hubs serve as collaborative spaces where communities of practice define and maintain semantic models. This enables translation and alignment of ontologies, ensuring that data from diverse sources—ranging from manufacturers to recyclers—can be understood consistently and without loss of meaning.

Nevertheless, the establishment of common semantic standards remains a work in progress. While the vocabulary hubs provide a promising foundation for standardizing data interpretations and facilitate the re-use of existing data models, broad adoption across a diverse and evolving industry landscape will require ongoing collaboration and agreement. Effective interoperability hinges not only on shared definitions but also on the continued development of dynamic, flexible models that can accommodate emerging data needs [9].

2.3 Data Trustworthiness and Integrity

Trust in the data exchanged within the battery passport data-space is essential, yet it remains one of the more complex issues to address. Static data—such as specifications, manuals, and repair or recycling instructions—tends to be more straightforward in terms of trust. It is provided by certified participants, inherently carrying the trust of the originating party (e.g. the car manufacturer). Dynamic data, such as that generated by Battery Management Systems (BMS) as the car is being used by a consumer, presents a more nuanced challenge. The reason is that here there are more incentives to alter the data, as well as more opportunities for various actors to interact with the data. As such, additional layers increasing trust must be implemented.

A key aspect of this trust-building process is the onboarding of the BMS into the system. This allows the BMS, and thus battery to authenticate itself and proof that the data on the battery state being written originates from the actual BMS. Furthermore, because the data from the BMS is updated frequently, it must be securely transmitted for integration into the DPP. Cryptographic signing of this data ensures its integrity, providing a level of assurance about the accuracy and authenticity of the information being shared.

While these mechanisms for securing dynamic data are essential, there is still room for improvement. Trust in BMS data can be further bolstered by establishing more robust, standardized methods for data onboarding, signing, and verification that are adaptable to a wide range of BMS technologies. Furthermore, the use of secure communication channels is a key part of ensuring that data is reliably transmitted and protected across the ecosystem [10].

Finally, it may be necessary to include certain non-IT processes and checks to again increase the trust in data. For example, a garage could perform a physical measurement on the battery health and check if this is within the expected range given the reported number of charge cycles. These processes are currently out of scope of legislation, as well as most digital product passport implementations, and may only become urgently relevant when the first cases of battery-passport-related fraud have surfaced.

2.4 Identity, Certification, and SSI Integration

To facilitate trust and ensure scalable identity management, the battery passport implementation incorporates Self-Sovereign Identity (SSI) concepts. Certification authorities issue credentials for both human and machine participants, which are stored in decentralized digital wallets. These credentials are integral to authentication and authorization processes within the data-space. Similarly, certified services—such as those responsible for onboarding batteries or aggregating BMS data—are critical for maintaining the integrity of the system.

The integration of SSI and certification into the data-space-based implementation provides a reliable method for ensuring that only authorized entities can access and interact with the battery passport data. While this approach supports the scalability of the system, challenges remain in terms of standardizing and adopting these methods across the industry. The role of certification authorities and the reliability of digital wallets are critical factors that will determine the success of this system in real-world applications. Ensuring that these certifications are universally recognized and accepted is an ongoing process that requires continued attention to industry best practices and regulatory requirements [7]. Fortunately, these developments aren't only driven by DPPs, and for example the currently ongoing EiDAS2.0 developments provide a foundation to build this DPP identification system onto [11].

3 Battery Management System

The Battery Management System (BMS) is a critical component for monitoring and managing a battery's health, performance, and safety. It collects a range of data, including cell voltages, temperatures, currents, and safety metrics, while also estimating key internal states like State-of-Health (SoH). These estimations are based on algorithms designed to predict the battery's condition, but differences between these algorithms can create challenges in ensuring consistent service, repair, and accurate residual value assessments, especially in the context of second-life applications. Furthermore, as the EU and other regulatory bodies push for circular economy initiatives, the BMS is expected to store and report additional lifecycle data for the battery passport. This makes it essential for BMS systems to support secure data collection, synchronization, and computation of relevant parameters that meet regulatory standards, ensuring data integrity throughout the battery's life cycle.

In this section, we explore two key aspects of the BMS's role in supporting the battery passport: (1) the secure collection and synchronization of lifecycle data, which is essential for data integrity and privacy, and (2) the standardization of BMS algorithms needed to ensure the accuracy and consistency of the data required by the battery passport regulation. Both areas are crucial for enabling the battery passport to function as intended, providing transparent, reliable, and secure data across the battery's lifecycle.

3.1 Secure BMS Data Collection & Synchronization

Due to the mandatory introduction of the battery passport, the BMS needs to include additional functionality to allow detailed tracking and reporting of battery lifecycle data. Suppose this data is reported in certain time intervals. In that case, the data may be used to track personal use of applications powered by the battery, like being home in case of home storage, or daily driving distance, or driving style in case of vehicle batteries. Therefore, the required sharing of this battery lifecycle data should be secure and compliant with the data privacy regulations in place. Currently, implemented security mechanisms included in BMS fall short in fully preventing unauthorized tampering with BMS data, where unauthorized persons or entities can make changes to BMS data. Moreover, the EU Battery Regulation asks for access to the BMS software to replace or update it when the battery might be used in a different application as a second-life system. This means that the functional BMS software and the data storage need separation to persist during and after the software change, as the battery still needs to be identifiable with its unique ID and previous life cycle data. NXP recommends physical separation into a secure storage device and a functional BMS device with memory for the functional software itself to meet these requirements.

With these security features in place for tracking and storage, it's crucial to address the risk of upstream data manipulation. For instance, if modules are exchanged or measurement devices are tampered with to falsely present higher residual value to potential buyers, this could compromise the integrity of the data. To mitigate this risk, it is necessary to prevent the use of uncertified parts during battery repairs or

re-purposing. The physical security of the battery system extends beyond the BMS hardware, requiring robust authentication and verification mechanisms for both the BMS and other components within the battery system. These mechanisms help ensure the integrity of the battery's lifecycle data and protect against fraudulent activities. However, further exploration is needed to determine how identification and verification methods can effectively prevent unauthorized access to the battery, especially in cases of physical tampering.

By adding a secure element, such as the NXP NCJ37x [12], to the BMS main controller, which includes a battery-passport applet as firmware on it, most of the complex passport-related tasks can be dealt with, without the need to change the BMS or MCU architecture. It will also allow to use of the same BMS hardware design in countries with and without legal requirements, as the part can be a populated or unpopulated slot, without the need to change the hardware security modules on the main BMU (Battery Management Unit). As a result, the authenticity of the battery is ensured, and data access to and from the BMS occurs in a secure manner. Even when the BMS itself does not have a direct connection to the database in the cloud, encrypted packages can be served to other transmission pathways.

3.2 BMS Algorithm Standardization

The EU Battery Regulation mandates the reporting of critical performance indicators, such as State-of-Health (SoH) and round-trip efficiency, through the battery passport. These indicators are central to assessing a battery's residual value, repurposing potential, and environmental impact. However, the regulation does not yet specify how these parameters should be calculated, leaving a significant gap between compliance goals and technical implementation. Without harmonized algorithms, there is a risk of inconsistency across battery manufacturers and BMS suppliers, which could undermine the passport's credibility, comparability, and effectiveness in real-world scenarios.

Currently, BMS developers use proprietary or heuristic methods to estimate SoH and efficiency, which vary in complexity, accuracy, and data requirements. These variations create challenges in comparing batteries across manufacturers or use cases, and in verifying claims related to degradation or energy performance. This fragmentation also limits the development of transparent second-life markets, where traceable and standardized lifecycle metrics are essential for assessing the condition and value of used batteries.

To address this gap, several initiatives, including Battery2Life, BASE, and the SeBaPaD project [13, 14, 15], are working toward reference algorithms and validation frameworks. TNO, in particular, has developed and tested prototype algorithms for round-trip efficiency and energy-efficiency fade estimation in its Battery-in-the-Loop (BiL) environment. These algorithms were applied in the GTD-E demonstrator [16] and are now being refined and deployed in a dedicated hardware-integrated module as part of SeBaPaD. By subjecting these models to rigorous, repeatable testing under controlled conditions, the project aims to generate empirical evidence for regulatory alignment and establish technical foundations for standardization.

The envisioned outcome is not a single mandated algorithm, but rather a set of validated, well-documented reference methods that can be adopted, compared, or audited across platforms. These would offer regulators, OEMs, and third parties a common framework for interpreting key battery metrics and for verifying compliance with digital passport obligations.

In the absence of immediate top-down standardization, TNO's contributions aim to bridge the transition period, demonstrating how trusted, transparent, and adaptable estimation methods can be deployed today while laying the groundwork for industry-wide consensus tomorrow.

4 Battery Passport Demonstrator

In the GTD-E project [16], a basic battery passport demonstrator has been developed based on the dataspace concepts mentioned above. TNO and NXP are now extending this in the SeBaPaD project [15] with improvements in the areas of DPP, security, and BMS algorithms. The SeBaPaD approach is conceptually presented in Figure 2. The developments in this project will bring together the various technologies previously discussed. These iterative developments allow us to experience which parts of the battery passport are already quite mature, such as the semantic model or basic data sharing infrastructure, and which parts require more work to be robust and scalable enough for wide-scale adoption.

4.1 Digital Product Passport

The digital battery passport demonstrator realizes in practice the architectural foundations outlined in Section 2, combining decentralized data control, semantic interoperability, and secure data exchange

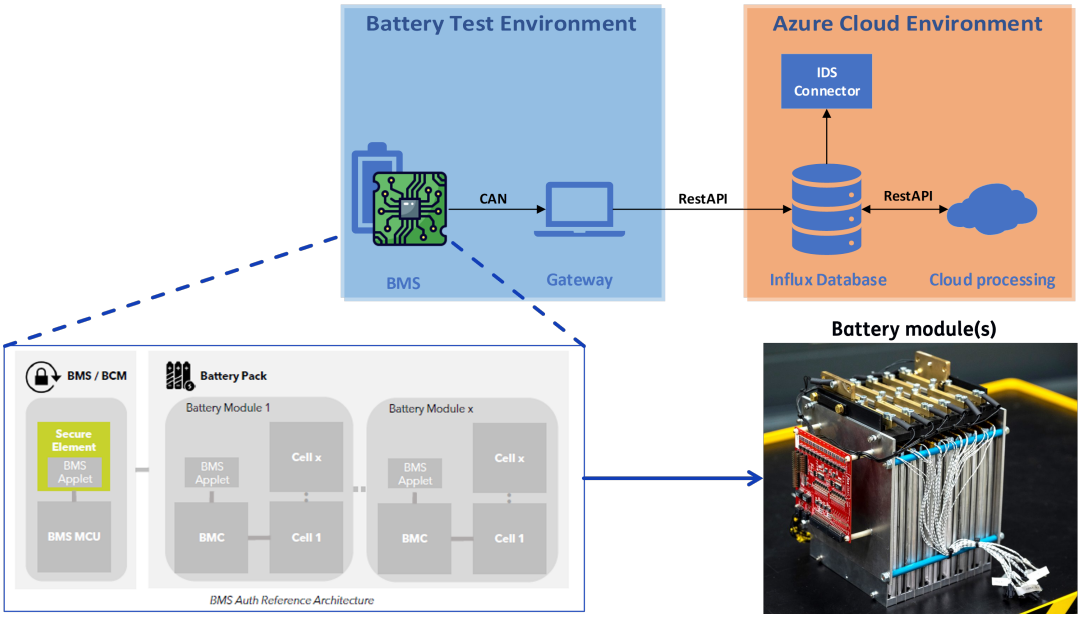


Figure 2: SeBaPaD conceptual approach.

within a distributed data space. This implementation aligns with the EU Battery Regulation's expectations for privacy-preserving, multi-stakeholder collaboration while remaining scalable and technically robust.

To address data sovereignty as discussed in Section 2.1, the demonstrator adopts a federated architecture based on the Data Spaces Support Centre blueprint. Each stakeholder—battery manufacturer, owner, and service provider—retains and manages their respective segments of passport data. Information is shared only when explicitly permitted through machine-readable usage contracts, ensuring that all access is traceable and governed by pre-agreed policies. No centralized data pool is used, and control always resides with the data provider.

In line with semantic interoperability principles (Section 2.2), the demonstrator uses a standardized data model, referred to as the battery passport profile. This model, based on semantic web technologies and harmonized with ongoing European initiatives such as BatteryPass, allows all parties to interpret and exchange data, such as identity, manufacturing, usage, and service events, consistently and without ambiguity. Public and private data layers are clearly defined, enabling differentiated access via mechanisms like QR codes or secure APIs, depending on the requester's role.

To uphold data integrity and trustworthiness (Section 2.3), the demonstrator integrates cryptographic signatures for all passport entries, allowing their origin and authenticity to be verified. Additionally, a secure element embedded in the battery pack stores key passport data—such as unique ID and lifecycle indicators, in tamper-proof form. This ensures that even when offline, the battery can provide authenticated data to authorized actors, e.g, during shipping or recycling.

A simplified overview of this implementation is illustrated in Figure X, which shows the roles of the main actors, their data control points, and the secure data-sharing interfaces linking them. The system design integrates OpenAPI-based connectors, ODRL-based policy enforcement, and secure element hardware to realize a distributed yet cohesive passport framework.

The demonstrator validates that the abstract concepts presented in Section 2 can be translated into a functioning, regulation-aligned system. At the same time, it reveals ongoing challenges, such as managing multi-level linked data and evolving authorization logic for hierarchical datasets. These insights inform future work and highlight the importance of combining technical innovation with careful attention to governance, legal compliance, and industry alignment.

4.2 Battery Management System

4.2.1 BMS Hardware

The BMS hardware platform in the demonstrator is based on a high-voltage reference design developed by NXP for stationary energy storage [17]. It comprises a Battery Management Unit (BMU), Cell Monitoring Units (CMUs), and a Battery Junction Box (BJB), interconnected via NXP's third-generation TPL protocol, as depicted in Figure 3. This architecture supports voltages up to 1500 V and long cabling distances, suitable for industrial applications.

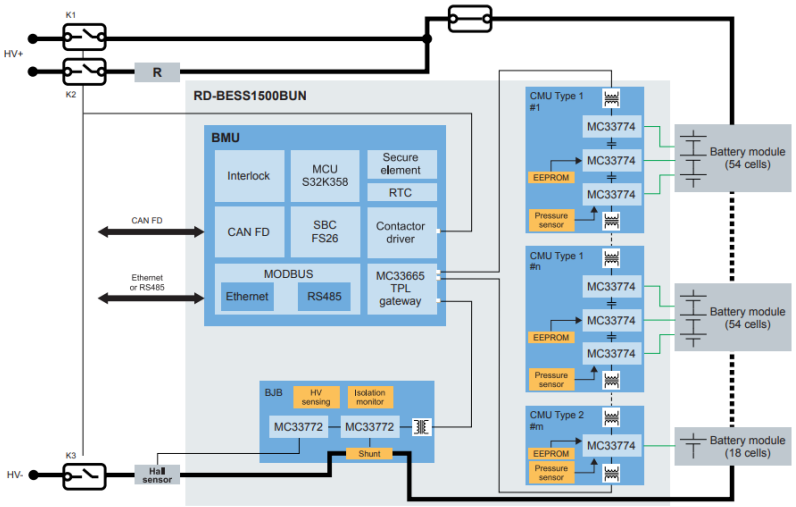


Figure 3: Battery Management System reference design [17].

The BMU integrates the S32K358 microcontroller, featuring dual Arm® Cortex®-M7 cores with ASIL D safety compliance, and a discrete NCJ37x secure element. The secure element provides hardware-based cryptographic operations, tamper-resistant data storage, and NFC access, enabling secure and persistent passport data availability even when the battery is offline. This component hosts a battery passport applet and is central to data integrity and traceability requirements under the EU regulation.

A custom battery module has been developed as part of the ongoing SeBaPaD project to integrate and evaluate the full BMS and passport architecture. This module is being subjected to climate chamber testing, providing controlled conditions for temperature, current, and voltage to assess system behavior and algorithm reliability across a broad operational envelope. This setup offers an essential validation environment to ensure robustness and reproducibility of both hardware and software components.

4.2.2 BMS Algorithms

The demonstrator implements modular BMS algorithms to estimate key parameters required for the digital battery passport, including State-of-Health (SoH) and round-trip efficiency. These values are essential for lifecycle tracking, second-life qualification, and environmental compliance.

In the GTD-E project, TNO developed a dedicated algorithm to compute round-trip efficiency, including its evolution over time, referred to as State-of-Health of Round-Trip Efficiency (SoH_RTE). The algorithm was embedded into the BMS software and validated through Battery-in-the-Loop (BiL) testing, as reported in the D3.4.1 BMS Validation Report [18]. It operates using a hybrid edge/cloud model: the BMS computes high-frequency short-term efficiency locally, while long-term SoH_RTE is derived in the cloud based on aggregated intervals. Figure 4 illustrates the algorithm's performance for two battery modules, showing strong agreement between embedded BMS outputs and values stored via cloud calculation in the battery passport system.

This edge/cloud architecture enables resource-efficient operation while maintaining regulatory-quality reporting. It allows the BMS to leverage fast internal measurements while outsourcing computationally intensive tasks to scalable cloud infrastructure. However, the implementation also highlighted several practical and security-related challenges.

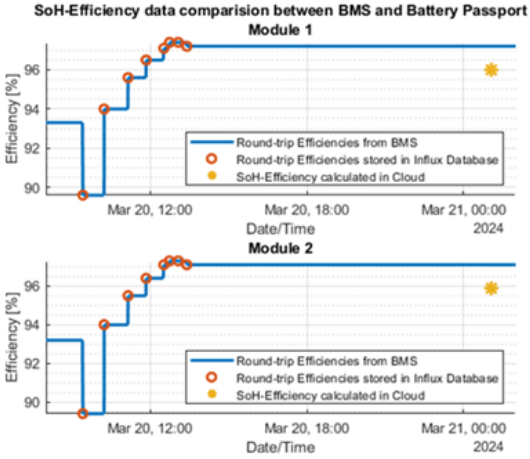


Figure 4: Comparison of round-trip efficiency data calculated on the BMS and in the cloud for two battery modules [4].

From a local perspective, integrating third-party diagnostics into existing BMS firmware imposes strict constraints on memory footprint and CPU load. At the system level, ensuring secure and efficient communication to the cloud via RestAPI requires robust interface design, reliable network connectivity, and tamper-resistant data handling. Moreover, managing cloud costs and minimizing data transfer overhead remain important concerns, particularly in volume deployments.

As part of the ongoing SeBaPaD project, the demonstrator continues to serve as a practical testbed for deploying and refining these algorithms under real-world conditions. This includes assessing long-term behavior during climate chamber testing of a custom battery module, providing further validation for the technical readiness of SoH_RTE tracking in battery passport contexts.

5 Conclusion

This paper presented a functional demonstrator that translates the European Battery Regulation into a working system through a secure, interoperable, and semantically aligned battery passport implementation. It combines three core components: a decentralized data-sharing infrastructure based on data-space principles, secure lifecycle data acquisition through embedded BMS hardware, and modular algorithms for passport-relevant state estimation. Together, these elements represent a cohesive and regulation-aligned architecture, validated through the GTD-E project and currently extended under the SeBaPaD initiative.

The demonstrator showcases a federated digital product passport architecture in which stakeholders maintain control over their respective datasets via standardized interfaces and policy-enforced access contracts. The use of semantic web technologies ensures that data is both machine-readable and interoperable across systems and domains. Secure elements integrated at the battery pack level provide tamper-resistant storage and authentication, supporting data integrity even in offline or second-life scenarios.

On the algorithmic side, the demonstrator includes embedded and cloud-based estimators for State-of-Health (SoH) and round-trip efficiency. These are implemented using a hybrid edge/cloud model that enables high-frequency local computation and long-term aggregation in the cloud. Validated using a Battery-in-the-Loop testbed and environmental chamber testing, the algorithms demonstrate both technical feasibility and alignment with regulatory use cases, such as residual value assessment and repurposing eligibility.

Importantly, this work highlights the necessity of close collaboration across disciplines, spanning embedded systems, cloud architecture, data governance, battery diagnostics, and regulatory analysis. The composition of the author team itself reflects this interdisciplinary nature, integrating expertise from semiconductor design, data ecosystems, and battery system engineering. As future deployments scale toward industry-wide adoption, such collaboration will remain essential. Continued cross-sector engagement is needed not only to address remaining technical challenges but also to align operational practices with evolving European regulatory frameworks.

References

[1] Regulation (EU) 2023/1542 of the European Parliament and of the Council concerning batteries and waste batteries, 2023. Available online: https://eur-lex.europa.eu/eli/reg/2023/1542/oj. EU Battery Regulation.

[2] DIN DKE SPEC 99100:2025-02, *Battery Passport Content Guidance*, 2025.

[3] Netherlands Organisation for Applied Scientific Research (TNO), *Towards future-proof battery passports,* Report No. R10003, 2024.

[4] E. Hoedemaekers, S. Rongen, S. Wilkins, *Next Generation Battery Packs Ready for the Battery Passport*, JSAE 2023, Yokohama, Japan.

[5] C. Beckers, E. Hoedemaekers, A. Dağkılıç, H. Bergveld, *Round-Trip Energy Efficiency and Energy-Efficiency Fade Estimation for Battery Passport,* 2023 IEEE Vehicle Power and Propulsion Conference (VPPC) Artikel 10403325 Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/VPPC60535.2023.10403325

[6] Data Spaces Support Centre, "Data Spaces Blueprint v2.0" [Online]. Available: https://dssc.eu/space/BVE2/1071251457/Data+Spaces+Blueprint+v2.0+-+Home

[7] International Data Spaces Association, "Understanding the IDS Reference Architecture Model," [Online]. Available: https://internationaldataspaces.org/understanding-the-idsa-reference-architecture-model/

[8] DIN 77010, Data Interoperability Framework for Digital Product Passports*, Deutsches Institut für Normung, 2023.

[9] StandICT.eu, "A Landscape of Standards for the Digital Product Passport," [Online]. Available: https://standict.eu/digital-product-passport-standards-report

[10] Rizos, V., and Urban, P., "Implementing the EU Digital Battery Passport," CEPS In-Depth Analysis, March 2024. [Online]. Available: https://circulareconomy.europa.eu/platform/sites/default/files/2024-03/1qp5rxiZ-CEPS-InDepthAnalysis-2024-05_Implementing-the-EU-digital-battery-passport.pdf

[11] European Commission *eIDAS regulation,* Available: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

[12] NXP Semiconductors. "NCJ37x Automotive-Grade Secure Element." NXP, https://www.nxp.com/products/NCJ37x. Accessed April 21, 2025.

[13] Battery2Life Project. Battery Passport and Digital Lifecycle Management. Available online: https://battery2life.eu (accessed April 21, 2025).

[14] BASE Project – Battery Passport and Algorithms for Second-Life Evaluation. Funded by the European Commission. Available online: https://cordis.europa.eu/project/id/101103419 (accessed April 21, 2025).

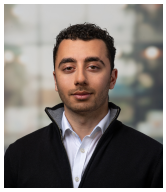
[15] TNO, "SeBaPaD: Secure Battery Passport Demonstrator," TNO, 2025. Available online: https://www.tno.nl/en/sustainable/mobility-logistics/batteries/secure-battery-passport-demonstrator/ (accessed April 21, 2025).

[16] TNO, "GTD-E Project: Towards a Green Transport Delta – Electrification," TNO. Available online: https://www.tno.nl/en/sustainable/mobility-logistics/batteries/gtde/ (accessed April 21, 2025).

[17] NXP Semiconductors, "RD-BESS1500BUN: Battery Management System Reference Design for 1500V BESS Applications," [Online]. Available: https://www.nxp.com/design/design-center/development-boards-and-designs/RD-BESS1500BUN (accessed April 21, 2025).

[18] E. Hoedemaekers, F. Hoekstra, C. Beckers, S. Rath, “D3.4.1 BMS Validation Report,” Internal Report No. 1001723, Green Transport Delta – Electrification (GTD-E), TNO, November 7, 2024.

Presenter Biography



Ir. Avedis Agop Dadikozyan is a research scientist at TNO (Netherlands Organisation for Applied Scientific Research), specializing in automotive and maritime powertrain electrification. He holds an MSc in Automotive Technology from Eindhoven University of Technology. His expertise includes battery system modelling, energy management strategies, and battery diagnostics. At TNO, he contributes to the development of model-based tools and software solutions for electric powertrains and is actively involved in national and European innovation projects on sustainable mobility.