Drivers, benefits, and challenges connected to authenticity in DPPs*

Linus Sönnerhed[1,†], Erik Bergström[1], Ulf Seigerroth[1] and Görkem Kılınç Soylu[1]

[1]Jönköping University, School of Engineering, Computer Science and Informatics, P.O. Box 1026, 551 11, Jönköping, Sweden

Abstract

This literature review examines two research questions: *"RQ1: How is authenticity described in the context of product passports across sectors?"* and *"RQ2: What drivers, benefits, and challenges are associated with establishing product passport authenticity?"*. Investigation was conducted via a systematic literature review using a thematic analysis of product passport literature across multiple sectors, including batteries, textiles, and construction. The thematic analysis resulted in the emergence of five themes: regulations, financial, sustainability, product lifecycle, and digital infrastructure. Despite recognition that authenticity is integral to product passport functionality, enabling traceability, transparency, and a circular economy, this necessity faces significant systemic barriers that impede implementation.

The analysis reveals that regulatory ambiguity blocks investment, deferring technological adoption and impeding standardisation, each challenge featuring interconnected dependencies. More fundamentally, the literature shows no shared conceptual foundation for authenticity itself. Definitions vary across industrial sectors: authenticity is conflated with integrity, treated as an extensive attribute list, or implemented either inferentially via traceability or assertively via proofs. Rather than reflecting legitimate sectoral differences, this definitional variation points to broader conceptual confusion about what authenticity means and how it should be verified, implemented, and evaluated. This confusion has cascading consequences. Without conceptual clarity, early adopters create divergent solutions that may impede the creation of digital product passport (DPP) standards and constrain Small and Medium-size Enterprises (SMEs) lacking resources for early adoption. Early solutions may also prove environmentally costly, using energy-intensive digital infrastructures that undermine sustainability goals.

The review concludes that foundational conceptual work of establishing a coherent view of authenticity must accompany the design and implementation of DPPs. Only with an integrated conceptual and empirical grounding can the interconnected and sociotechnical dependencies of DPP authenticity be navigated. Future empirical research should further map how authenticity mechanisms are operationalised within sector-specific workflows, examining sequential decision points and resource constraints across firm sizes.

Keywords

Digital Product Passport, Product Passport, Product Authenticity, Circular Economy, Supply Chain Security, Systematic Literature Review, Thematic Analysis

CEUR-WS.org/Vol-4325/paper28.pdf

1. Introduction

The introduction of the Digital Product Passport (DPP) by the EU is a central effort to improve traceability, transparency and sustainability in supply chains [1] by providing physical products with digital identities [2]. DPPs are expected to provide comprehensive product information such as its origin, environmental impact, and disposal recommendations. Such information may be leveraged to enhance supply chain management, ensure regulatory compliance, and address consumer demand for transparent and reliable product data [3].

Regulations require DPPs to be verifiable in terms of authenticity [1], making it a key component of DPP operationalisation. However, DPP implementation details have yet to be decided [4], which in-

The 12th International Conference on Socio-Technical Perspectives in IS (STPIS'26), September 16–17, 2026, L'Aquila, Italy.

*Contributions: Linus Sönnerhed - Writing and Analysis; Erik Bergström - Analysis and Review; Ulf Seigerroth - Analysis and Review; Görkem Kılınç Soylu - Analysis and Review;

†Corresponding author.

linus.sonnerhed@ju.se (L. Sönnerhed); erik.bergstrom@ju.se (E. Bergström); ulf.seigerroth@ju.se (U. Seigerroth); gorkem.kilinc.soylu@ju.se (G. K. Soylu)

0009-0003-4450-7911 (L. Sönnerhed); 0000-0002-1436-2980 (E. Bergström); 0000-0002-5881-0669 (U. Seigerroth); 0000-0002-7047-0556 (G. K. Soylu)



© 2026 CC-BY logo & © 2026 Copyright for this paper by its author(s). Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

published 2026-11-10

cludes details on establishing DPP authenticity. As DPPs are rolled out across diverse sectors, including batteries, textiles, electronics, furniture, and automobiles [4], understanding how authenticity is conceptualised and perceived across diverse technological, organisational, and regulatory contexts is essential for developing coherent regulatory guidance and supporting future implementation frameworks.

Reviewing previous literature syntheses of DPPs, Wicaksono et al. [5] investigated DPP integration into a circular economy via a systematic literature review. Their work examined technological developments, adoption, and the economic and legal consequences of integrating DPPs into existing supply chains. They further established a conceptual model with underlying technologies and identified data security as crucial. However, while topics such as authentication and access control were discussed, authenticity was not systematically addressed. Zhang et al. [6] conducted a systematic review across several sectors, focusing on technical architecture and enabling technologies, identifying various mechanisms to ensure data security, and presenting Zero-Knowledge Proofs as an implementation option. Their investigation tied authenticity primarily to preventing counterfeiting. Similarly, Fares et al. [7] employed a bibliometric analysis to create a framework of critical product passport adoption aspects, similarly having framed authenticity primarily as counterfeit prevention, a framing also reflected in the state-of-the-art review of material passports in Munaro and Tavares [8] in the construction sector. The literature syntheses suggest a pattern in which cybersecurity and technical aspects receive greater attention, while what DPP authenticity entails in practice remains narrowly framed or underdeveloped.

To develop this area of research and establish the current discourse on ensuring authenticity in digital product passports, this work aims to systematically examine how authenticity is defined or described across sectors, and to establish the range of drivers, benefits, and challenges involved. This may be summarised into addressing two research questions:

- RQ1: How is authenticity described in the context of product passports across sectors?
- RQ2: What drivers, benefits, and challenges are associated with establishing authenticity in product passports?

To achieve the objectives of this paper, we conducted a systematic literature review to examine the descriptions and uses of authenticity in the context of DPPs across sectors, and reviewed the potential drivers, benefits, and challenges of its implementation. Through this systematic examination, we aimed to extend the evidence base necessary for developing coherent regulatory guidance and implementation frameworks, including authenticity across sectors. The remainder of this paper is organised as follows: Section 2 provides background on DPPs and previous work on authenticity. Section 3 describes the research methodology. Section 4 presents the results, while Section 5 discusses the findings. Finally, Section 6 concludes the paper and outlines directions for future work.

2. Background & Related work

2.1. Product Passports

The DPP was introduced as part of EU efforts to support the transition to a circular economy via the European Green Deal [9] and the Circular Economy Action Plan [10]. The push toward a circular economy is expected to counter over-exploitation of resources by using strategies such as reusing, recycling and refurbishing products and their components, thereby maximizing their lifespan [11]. The DPPs are described as digital identities assigned to physical products [2], providing comprehensive product information including product origin, environmental impact and disposal recommendations [1]. Such identities may be assigned either to batch or product series, but may also be assigned on an item-specific basis, dependent on the overall value of the product [4]. One such example includes batteries from the automotive industry, where batteries are one the first sectors requiring regulatory compliance in early 2027 [12]. Other prioritised product groups include textiles, furniture and tyres [1]. While the use of the term DPP applies to several industries, it is not the only term used to describe them, as the implementation for the battery sector is instead termed battery passport [12], and the construction & building materials sector has previously introduced the term material passport [4].

Capelleveen et al. [13] mapped passport variations across sectors while distinguishing them from other adjacent solutions. Their work extracts seven characterising features of product passports, constructing a synthesised definition of passport variations defined below:

> *a material passport (or product passport) is a digital interface composing a certified identity of a single identifiable product by accessing the set of life cycle registrations linked to this object in order to yield insight into the sustainability and circularity characteristics, the circular value estimation, and the circular opportunities for both that product and its underlying components and materials.* ([13], p. 14)

This study will include multiple variations of product passports. The definition provided by Capelleveen et al. [13] will be applied during this review to comprehensively address product passports during the investigation. However, given the primary label provided by the EU is the DPP, we will use DPP and product passports interchangeably. The DPPs have been proposed to contain the following information:

- A unique product identifier [1];
- Product or material properties, including their composition, substances of concern and environmental impact [3, 4];
- Traceability information, such as product origins and its manufacturer [11, 4];
- Usage data, including maintenance, replacement or repair updates [11];
- End-of-life data, such as documentation for appropriate, collection, sorting [11] and disposal [3];

Though this list is likely not comprehensive across sectors, as battery passports are required to contain additional details such as electrochemical performance and durability parameters [12]. In addition to the data requirements regarding the content of product passports, accessing such contents requires use of a data carrier [1], such as a Quick Response (QR) code [14], which is physically present on a product to ensure connection to a product passport [4, 12]. Whether their storage occurs in a centralised or decentralised format is yet to be determined, though a decentralised format is possibly favoured [4].

2.2. Authenticity in Cybersecurity

As discussed by von Solms and van Niekerk [15], general security objectives in both cybersecurity and information security aim to ensure the confidentiality, integrity, and availability of information, forming what is commonly referred to as the CIA triad. Definitions of each of these principles are presented by Kaur et al. [16], defining confidentiality as preventing unauthorised access to data, integrity as ensuring information remains unaltered by unauthorised parties, and availability as maintaining both timely and uninterrupted access to information.

The operationalisation of authenticity from cybersecurity and information security perspectives varies in the literature, as it may be treated as a subset of integrity [15] or as its own, entirely separate principle [17]. Inclusion as a separate principle may be observed in extended frameworks such as CIAAA [16] or the Parkerian Hexad [18].

Standards from the National Institute of Standards and Technology (NIST) present authenticity with different degrees of breadth, either succinctly as *"the property that data originated from its purported source."* [19, p. 2], or as *"the property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator."* [20, p. B-2], in which they closely relate authenticity to authentication. This is in sharp contrast to the definitions found in standards by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC), which present authenticity as *"property that an entity is what it claims to be."* [21, p. 2] with minor formulation variations, in which there is no mention of authentication. Authentication is instead defined as *"provision of assurance that a claimed characteristic of an entity is correct."* [21, p. 2]. As such, there is a difference between authentication and authenticity: authentication focuses

on characteristics and the process of assurance regarding a claim, while authenticity is an intrinsic property which may be assessed.

This review adopts the definitions provided by ISO/IEC 27000 [21] and 270002 [22], as they clearly differentiate between authentication, authenticity, and integrity, thereby providing conceptual clarity during investigation. Further, ISO/IEC standards are international, whereas NIST standards are national. Authenticity in DPP regulations refers to the digital product passport itself [1], making these cybersecurity-related distinctions an important conceptual foundation for analysing how authenticity is addressed across the reviewed product passport literature.

2.3. Authenticity in Product Passports

Product passports must work across diverse product categories with varying physical properties and cost structures [1], creating practical constraints on what authenticity mechanisms are viable. While the QR code is highlighted as a physical-to-digital connector in regulations [12], several alternatives may be considered depending on the required security measures, such as Near Field Connection (NFC) or Radio Frequency Identification (RFID). Highlighted by Byers et al. [23], one alternative is hardware-locked NFC tags with asymmetric cryptography, which offer stronger security than a standard QR code, though they note a QR code may outperform NFC in ease of use. The connection required to anchor the digital identity to its physical counterpart represents another attack vector that must be considered alongside digital security measures, subject to attacks such as duplication or a broken connection [23]. Further, the granularity of DPP assignment for batches, product groups or unique items sets an upper bound on the type of authenticity that can be enforced, as batch-level identifiers cannot technically prevent item-level duplication or substitution. Balanced against enforcing demands of interoperability and scalability [1], the two requirements of physical robustness and digital security must therefore work together seamlessly for consumers to trust a product's authenticity. Regardless of the technological approach chosen, digital product passports remain only as reliable as the data supplied by actors at the source [24].

Achieving authenticity in the context of DPPs therefore requires aligning physical security features with digital security protocols, while relying on the organisational integrity of the actors who input data at the source. Should stakeholders in a product's lifecycle be unable to reliably verify authenticity, the data in the product passport may become suspect [25], potentially undermining the system's ability to support its fundamental goals of increasing traceability, transparency and sustainability [1].

3. Methodology

This study uses a systematic literature review following Kitchenham's [26] methodology to identify, evaluate, and interpret all available research relevant to a particular research question, topic area, or phenomenon of interest. We supplemented this approach with Wohlin's guidelines for backward and forward snowballing [27], which have been highlighted to reduce the risk of missing relevant publications [28]. To further increase transparency, the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) guidelines are used to present the number of results retrieved [29].

3.1. Search Strategy

We conducted preliminary searches to refine the search strategy and identify relevant terminology across disciplines. While early results on authenticity for DPPs were few, search iterations revealed that "product passport" terminology varied significantly across sectors and disciplines. The work of Capelleveen et al. [13] mapping passport variations across sectors while distinguishing them from other adjacent solutions helped establish the scope of this review. This foundation, combined with terminology identified in preliminary searches of related DPP literature, informed the construction of search queries, expanding the sensitivity of the search strategy while maintaining specificity.

To further maintain conceptual clarity, this study adopts the definition of authenticity provided by ISO/IEC 27000 [21, p. 2]: *"the property that an entity is what it claims to be"*. As such, explicit claims of authenticity, as well as the reverse, such as counterfeiting, are included in this review to capture the full authenticity discourse. Multiple relevant synonyms and antonyms for authenticity were identified through preliminary searches and consultation of the Merriam-Webster Dictionary [30]. This synonym and antonym identification was essential, as not all databases included feature-controlled vocabularies or thesauri, necessitating flexible variations in search terms for comprehensive retrieval.

To ensure more comprehensive coverage of literature, multiple databases were queried as suggested by [31]. For this purpose, we selected three databases, ACM, SpringerLink and Scopus, considered adequate due to their broad coverage across multiple sectors and disciplines while avoiding significant overlap. We searched for product passports in both the title and the abstract, requiring the inclusion of authenticity-related terms in any other field to broaden sensitivity while maintaining specificity. The query was then applied to all databases, with database-specific modifications due to differences in query syntax and field limitations. SpringerLink stands out because searches that include abstracts automatically return full-text results. To mitigate potential selection bias and maintain protocol parity, results retrieved from SpringerLink underwent an aggressive, manual title-and-abstract triage stage prior to full-text screening. The collection of queries and their modifications is shown in Table A1 found in Appendix A.

We used the software Rayyan [32] for deduplication and initial title and abstract screening. Following full-text review, we transitioned to Zotero [33] for managing and coding the final literature collection, as it offered enhanced annotation features and metadata organisation.

3.2. Data Identification and Filtering Criteria

We conducted the search in the beginning of 2026. Literature published in journals, conference proceedings or book sections was included, provided the full text was available and in English. Further, all included literature was required to mention a passport variant and explicitly address authenticity or the reverse, alternatively mentioning mechanisms known for implementing authenticity, such as digital signatures [22]. As Kitchenham notes, literature reviews synthesise primary findings, thereby excluding literature that only serves as reviews [26]. To capture earlier discussions of authenticity in product passport contexts, we imposed no restrictions on publication year. A summary of the inclusion and exclusion criteria is shown in Table 1. Grey literature identified during the search or snowballing was included, provided it was available in English and discussed authenticity in the context of product passports.

Table 1
Table describing inclusion and exclusion criteria for scientific literature screening procedure.

Criterion	Details
IC1	Article is a journal, conference, book section or relevant grey literature
IC2	Article is in English
IC3	Article contains mention of a variation of passport
IC4	Article discusses authenticity
EC1	Article is a literature review
EC2	Article is not accessible
EC3	Article fails any of the inclusion criteria

Given the possible embedded nature of authenticity discussions, we applied a generous inclusion threshold during title and abstract screening to capture literature with potential relevance. Following the initial screening, we reviewed full texts of all potentially relevant literature. From the total 550 articles identified from databases, 33 were selected for final inclusion. Using the 33 articles identified from databases, we further conducted one iteration of snowballing, both backwards via screening cited references and forwards via screening the citing literature for the final included articles. To identify further related literature, initially identified and relevant literature reviews were used for one iteration

of backwards snowballing. Literature identified through snowballing was included and excluded using the same criteria as for the database results. Including 36 additional articles, a total of 69 articles were included for this review. The process is visualised in Figure 1.

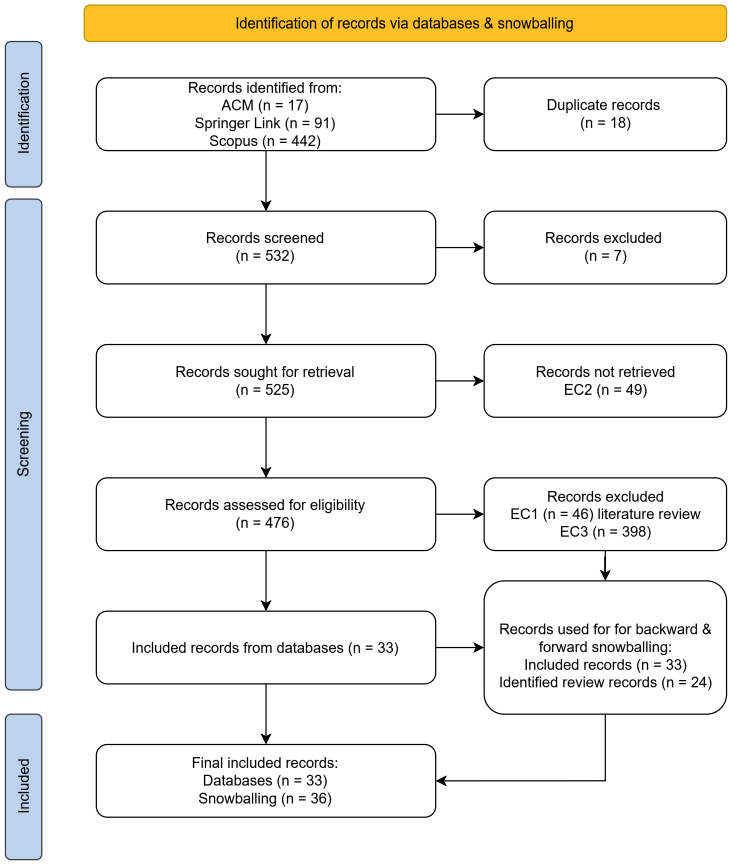


Figure 1: PRISMA diagram presenting review process.

3.3. Thematic Coding

We subjected the final selection of literature to thematic coding using the six-phase approach by Braun and Clarke [34] to identify, analyse, and report patterns, or themes, in the data. The method is widely used for the analysis of qualitative data across disciplines and paradigms [35] deemed appropriate for addressing our research questions. Adhering to the six distinct phases outlined by Braun and Clarke [34] for the analysis, raw data was examined to identify potential patterns. Subsequently, manual analysis of the data was performed to generate initial codes summarising data segments. Data segments in this study were comprised of extracted passages from full-texts, assigned a code based on a core aspect represented. One such example may be the data segment: *"Establishing the authenticity of products prevents economic losses due to counterfeits"*, which may be assigned the preliminary code "economic loss". Preliminary codes were created early in the process with iterative refinement until the creation of a code cookbook. Once preliminary codes were established, they were grouped into broader patterns, referred to as themes, reflecting the data patterns related to the research questions. Upon review, the earlier example of the code "economic loss" was interpreted primarily as a financial concept and therefore falls under a financial theme, grouped with data segments that mention, e.g., economic gain. Data segments may further contain multiple relevant codes for multiple themes, such as the example data segment *"Proof of authenticity created at the beginning of the product lifecycle, which is transferred with ownership change, promotes trust for second-hand sales and traceability."*. This data segment may be associated with the codes "enabler for traceability" and "resale", with implications fitting to both product lifecycle and sustainability themes. As such, thematic coding combined inductive and deductive

elements. Themes were developed iteratively through interpretation of coded data segments, while the analytical lenses of drivers, benefits, and challenges were used to structure the interpretation of the identified themes. Progression through the phases was not linear, but rather an iterative process as findings were refined, recoded and regrouped into new themes. Initial descriptive coding and codebook generation were executed independently by a single primary coder to maintain thematic continuity. Reviewing and defining themes were subsequently conducted through collaborative peer debriefing sessions among all co-authors to explore alternative interpretations, refine theme boundaries, and strengthen the analytical account. The use of this process led to the development of five themes, which are expanded upon in the results and discussion sections.

3.4. Limitations

This study is subject to several distinct limitations. Search scope and linguistic constraints limited the comprehensiveness of the results. We searched three databases, which, while broad, do not capture all relevant literature across disciplines. Including additional databases may have yielded more relevant literature. The restriction of results to English-language publications excluded potentially relevant work in other languages, an issue that may prove severe on continents such as Europe, which are largely multilingual and to which the legislative aspects of the DPP will primarily apply. The terminology surrounding authenticity in product passport contexts is diverse and context-dependent, making some relevant discussions difficult to capture with fixed search terms. Terms such as verification, traceability, or provenance may implicitly address authenticity, depending on the field in which they are used. Finally, some literature was inaccessible, which may have introduced retrieval bias toward open-access or institutional-access publications.

The title and abstract screening proved inefficient for this topic, as discussions of authenticity rarely appear in either; instead, they are embedded in broader analyses of systems or supply chains. This issue was exacerbated by the interdisciplinary nature of the topic, as what constitutes an authenticity discussion in one discipline may be framed differently in another. Consequently, we adopted a more generous initial inclusion for full-text reviews, requiring additional screening effort and limiting the possibilities of including more databases or further iterations of snowballing. Including further snowballing iterations may have yielded additional relevant results. Similarly, forward snowballing the literature reviews may have yielded further results, but would potentially require additional effort as there is less provided context on the content of the source. Generic terminology introduced noise into the results, as terms like “original” or “genuine” often appeared in contexts unrelated to authenticity (e.g., “original research” or “genuine interest”), requiring additional manual filtering.

While the employment of a six-phase approach by Braun and Clarke [34] provides consistency and transparency of methodology, all initial coding was performed by a single researcher, introducing greater risks of confirmation bias or individual interpretation. This may be particularly significant given the transdisciplinary nature of DPPs, as nuances and interpretations are visible to researchers from different backgrounds. While theme development and refinement were collaborative, the employment of multiple independent coders of varied backgrounds would have strengthened analytical rigour and mitigated this limitation.

4. Results

To understand how authenticity operates in the context of product passport literature, we analysed literature across multiple sectors. We first examined how authenticity is defined and conceptualised across sources, then analysed its role through five distinct themes, conceptualised from iterative thematic analysis of the included literature and representing the primary dimensions through which authenticity is conceptualised and discussed across product passport sectors. The final included literature, including sector and contributions is listed in Table B1 in Appendix B.

4.1. Authenticity in Product Passports

Descriptions of authenticity varied significantly across the analysed literature, wherein identified definitions broadly clustered around integrity-oriented, authentication-oriented, and product-oriented uses of authenticity. Lu et al. [36, p. 7] provided a conceptually narrow description: *"Information authenticity means the information pertaining to the correct information source has not undergone improper or unauthorised modification."*, while Wu et al. [24, p. 1] offered a broader conception: *"'Authenticity' means that the information has attributes such as completeness, accuracy, trustworthiness, validity, integrity, faithfulness, originality, meaningfulness, and suitability for a certain purpose"*. This mirrors the broader literature, in which authenticity is employed as a synonym for integrity [37, 38] or, alternatively, as either data authentication [39, 1] or product authentication [40, 41].

This definitional variation reflects the convergence of multiple disciplinary traditions, such as cybersecurity, supply chain management and regulatory practice, each with its own established terminology which was not designed to interoperate. The analysed literature further conflates related but distinct operations: identification (determining what a given product is), verification (confirming claimed characteristics), and assurance that something is genuine (confirming that the product is not counterfeit).

4.2. Authenticity: Drivers, Benefits, and Challenges

These five themes: regulations, financial, sustainability, product lifecycle, and digital infrastructure, were formed by reviewing the analysed literature (see Appendix B in Table B1) through multiple perspectives and formed into themes on the basis of broader constructs. The themes include constructs that may support one another, such as a regulatory driver in one theme serving as a benefit in another. While systemic phenomena cause cascading effects, such as a regulatory mandate (Driver) creating market demand for anti-counterfeiting solutions (Benefit), each data segment was coded based on its primary, localized operational role within that specific subsystem. Within each theme, we applied analytical lenses consisting of drivers, benefits and challenges, defined as follows:

- Drivers - What drives the existence of authenticity in DPPs
- Benefits - What benefits of authenticity exist in the context of DPPs
- Challenges - What inhibits the implementation or use of authenticity in DPPs

The following sections examine each of these five themes in detail.

Regulations

The regulations theme discusses authenticity in the context of regulatory directives.

Regulations from the EU concretely drive requirements for product passports to be verifiable in terms of authenticity [1], a design requirement similarly noted in literature [42]. While this presents obligatory compliance, it also poses challenges regarding clarity on how best to comply. Domskienė and Gaidule [43] highlights from interviews with garment producers in the Baltic Sea Region, that while the recommendations of the European Commission (EC) are recognised as binding, some companies choose to await more precise guidance and support from local legislation as to how the EC recommendations should be implemented. Their interview responses note that a fundamental reorganisation of their systems is required, but due to missing organisational and technological implementation guidelines, it is unclear what actions must be taken. Blockchain-based proposals for establishing authenticity have also been noted to face regulatory issues in cross-border contexts [44], while regulatory gaps surrounding related NFT-based approaches introduce additional implementation uncertainty [45], further emphasising the need for regulatory clarity. Until implementation guidance clarifies these gaps, regulatory drivers for authenticity will remain difficult to translate into practice.

Financial

The financial theme discusses authenticity for economic purposes, such as preventing counterfeit losses or the various costs of implementing authenticity.

From a financial perspective, authenticity is balanced between market opportunity and implementation cost. Market demand for authenticity [23] and a global prevalence of counterfeit products [40, 46, 47] drive anti-counterfeiting measures to address significant losses across industrial sectors [48, 49], noted by [50] to reach trillion-dollar magnitudes. Beyond loss prevention, authenticity is highlighted to strengthen brand protection and supply chain trust between actors [48, 51]. However, actualising these benefits requires substantial investments.

Development and integration of DPPs are noted by Acciai and Pérez-Bou [51] as a particular challenge, due to the financial cost of the technology itself and its adaptation to existing information systems. Hulea et al. [52] further emphasises that initial setup and ongoing maintenance of a DPP system requires significant investments in terms of time and money, requiring technical expertise. They further note this issue is particularly pronounced for small to medium-sized enterprises (SMEs), as they require investments into developing their digital capabilities [52, 53].

Simultaneously, methods which establish authenticity through physical-to-digital connections such as inherent material fingerprinting, require equipment investment such as laboratories as noted by [54] for the purpose of material fingerprinting. This is similarly reflected by [55] wherein specific equipment to identify a given additive material component is required. Similarly, data carrier methods such as QR, NFC or RFID, must balance security levels [23] against implementation cost, as implementations with mechanisms ensuring authenticity may be more costly than those without [48]. Such cost must then further be considered for end-consumers, as there may be an unwillingness to pay potential price premiums introduced by DPPs [56]. This consumer-side financial barrier compounds the implementation costs organisations face, making financial feasibility a decisive factor in determining which authenticity methods organisations adopt.

Sustainability

The sustainability theme discusses authenticity in terms of environmental aspects, such as its role in influencing the goal of reaching a circular economy.

Authenticity for the purpose of sustainability is framed as a fundamental part of the circular economy strategy, addressing consumer confidence in secondary markets and trust that a product is genuinely suitable for strategies such as reuse or recycling. As a driver, authenticity is regarded as an enabler of various r-strategies by providing verifiable evidence of product history and condition [43, 57]. Authenticity further translates into tangible benefits rooted in increased trust, as both consumer and reseller confidence in second-hand products increases [58] and authenticity guarantees can justify premium pricing for sustainably produced goods [51]. However, the promise of trust in sustainability via authenticity may come with an environmental cost as several proposed solutions consume vast amounts of energy [59, 60], instead forming a source of environmental concerns [45]. Ensuring sustainable authenticity by balancing verification rigour against the consumption of its implementation becomes a significant design constraint.

Product Lifecycle

The product lifecycle theme discusses authenticity in the product lifecycle, focusing on aspects such as authenticity as a verification mechanism.

Authenticity in the product lifecycle is proposed to serve dual drivers of safety and traceability. Safety was identified as crucial across several sectors, as failure to establish authenticity can lead to various consequences. Compromised battery-management systems and manipulated battery data may jeopardise safety and increase the risk of thermal runaway [61], counterfeit medication may compromise patient health [49] and ensuring correct material composition [62] or genuineness of safety-relevant additive manufacturing parts depends on ensuring authenticity to meet required standards [55]. This

turns authenticity from a compliance or trust mechanism into a direct safety requirement. Traceability becomes part of establishing this safety, wherein authenticity ensures the reliability of traceability accounts, verifying the steps taken in the supply chain [63, 64, 36] and ensuring accountability [55]. This manifests in several benefits across the product lifecycle, enhancing market transparency [44], supporting informed decision-making for consumers [56] and preventing issues of greenwashing [51]. Further, authenticity may be used for monitoring product stock by establishing the exact number of produced products and protecting intellectual property [55], providing additional benefits beyond safety or compliance.

However, the literature reveals there is a conceptual circularity that complicates authenticity in product lifecycles, as traceability and transparency are simultaneously enabled by and enablers for establishing authenticity [47, 65, 66, 44]. The ability to trace a product's journey can be used to verify its authenticity, yet verifying that history itself requires establishing the authenticity of the steps recorded. As such, authenticity becomes dependent on the mechanism it is meant to reinforce.

Maintaining authenticity across the product lifecycle faces multiple points of failure. Actors involved are forced to depend on each other, as input data is only as trustworthy as the actors themselves [24]. Technically, data carriers and physical identification methods remain vulnerable to destruction, substitution or tampering, breaking the physical-to-digital linking [23, 48]. At the systems level, interoperability gaps between different product passport implementations featuring authenticity may hinder adoption [52, 45, 67].

Achieving authenticity in product lifecycles becomes a blend of technological solutions, reliability between human actors and interoperable systems designed to withstand tampering, forming a sociotechnical combination that is difficult to guarantee across a given supply chain.

Digital Infrastructure

The digital infrastructure theme primarily discusses the aspects of product passport technology.

Digital infrastructure forms a two-sided coin in the context of authenticity, as there are various provided pathways to achieve authenticity, but each provides their own set of challenges. The availability of proposed technologies such as Decentralized Identifiers (DIDs) [23, 42], Verifiable Credentials (VCs) [68] and blockchain systems [62, 37] form various data layer solutions which may or may not be combined [52]. The direct physical-to-digital linking provide similarly myriad pathways, such as intrinsic physical identification methods [54, 49] or data carriers (QR, RFID, NFC) [69, 23, 48] each providing authenticity at different security and cost levels. However, the diversity creates additional challenges, as technical competence [52], digital maturity [45] and organisational readiness [43, 45] vary across sectors and companies of varying size.

Further, navigating the various options of implementation becomes an issue of gauging adoption complexity [52, 37], their interoperability [67, 44] and their overall scalability [52, 37]. Such implementation complexity was further noted by Antsipava et al. [70] as difficulties understanding an underlying technology may pose a hindrance for establishing trust in authenticity disclosures for end-consumers. Thus, while technological diversity enables customisation to different security and cost requirements, the same diversity requires companies to navigate complex technical trade-offs among capability, feasibility, and compatibility, as well as adoption barriers stemming from consumer comprehension. This makes the selection of technology for authenticity itself a strategic challenge rather than a straightforward decision.

Result Summary

Across these five themes, authenticity emerges not as a single problem but as a collection of interconnected socio-technical constraints. Regulations drive authenticity adoption, yet lack of guidance creates financial uncertainty about which solutions to adopt. Meanwhile, technological barriers to interoperability compound regulatory compliance challenges and actor-dependency vulnerabilities embedded in the product lifecycle. Thus, addressing authenticity in product passports requires not

solving each theme independently, but recognizing how constraints are related across domains. The themes, codes and lenses are summarised in Table 2 below.

Table 2
Table describing themes and associated sub-themes, grouped by categories of drivers, benefits and challenges.

Theme	Drivers	Benefits	Challenges
Regulations	EU authenticity requirement [1, 71]	(Authenticity benefits of regulations are fundamentally for the purpose of having authenticity, considered in this analysis as not bringing additional benefits)	Lack of regulations or standards for regulatory compliance [23, 24, 51, 41, 66, 59, 44, 43, 72, 45, 63, 25, 73, 53, 4, 74]
Financial	Prevention of counterfeit products [40, 46, 75, 69, 50, 76, 48, 51, 55, 49, 41, 66, 56, 59, 44, 68, 58, 72, 52, 77, 78, 79, 67, 62, 71, 80, 25, 81, 82, 83, 84, 53, 4] Market demand for authenticity [23, 36]	Prevention of counterfeit financial loss [50, 49, 62] Brand protection [51, 78, 79]	Implementation cost for a given solution [51, 49, 54, 44, 43, 72, 36, 52, 62, 85, 25, 83, 53, 74] Cost of maintenance for a given solution [24, 37, 51, 75, 43, 52, 67, 62, 25, 83] Introduction of DPP increases product pricing [56, 83]
Sustainability	Facilitating R-Strategies, including resale, reuse and remanufacture [40, 75, 23, 42, 24, 37, 61, 48, 86, 51, 41, 56, 60, 58, 43, 72, 87, 36, 57, 45, 62, 80, 25, 82, 83, 84]	Justification of higher pricing for sustainably produced products [51, 56, 60, 83]	Solutions with environmental drawbacks, such as large energy consumption [59, 44, 60, 45]
Product Lifecycle	Product safety verification across the lifecycle [40, 61, 88, 86, 55, 49, 72, 52, 78, 79, 62, 81, 84] End-to-end traceability of products and materials [75, 42, 89, 90, 69, 24, 37, 38, 61, 76, 55, 41, 65, 66, 56, 54, 44, 60, 68, 43, 72, 87, 36, 52, 85, 91, 63, 80, 64, 25, 73, 92, 93, 84, 94]	Inventory management of products [65] Passport operator accountability [75, 89, 90, 37, 68, 87, 67, 95, 63, 73, 96, 93, 97, 94] Enabling transparency in the supply chain [75, 47, 42, 90, 24, 37, 38, 76, 48, 51, 98, 41, 65, 56, 59, 39, 44, 60, 68, 72, 45, 95, 73, 92, 93, 94, 74] Enabling informed decision-making [42, 48, 51, 56, 25, 73] Protection of intellectual property rights [55]	Risk of false sustainability claims (greenwashing) [51] Reliance on actors for authenticity [24, 99] Interoperability between DPP technologies [41, 44, 87, 67, 45, 25]
Digital Infrastructure	Availability of authenticity solutions, e.g. blockchain, NFT, DIDs, VCs, NFC & RFID [40, 46, 47, 75, 23, 42, 89, 90, 69, 24, 37, 38, 61, 50, 88, 76, 48, 86, 51, 55, 49, 98, 41, 65, 56, 54, 70, 59, 39, 60, 44, 68, 43, 72, 87, 36, 52, 4, 77, 78, 79, 67, 57, 45, 95, 62, 71, 85, 63, 80, 64, 1, 25, 73, 81, 82, 92, 96, 93, 97, 84]	(Authenticity benefits of digital infrastructure are fundamentally for the purpose of having authenticity, considered in this analysis as not bringing additional benefits)	Lack of technological competence [51, 43, 52, 45, 85, 25, 53] Organisational readiness to adopt product passports [51, 41, 44, 43, 45] Complexity of solution implementation [42, 51, 66, 43, 62, 53, 70] Solution scalability limitations [47, 75, 90, 37, 51, 87, 45, 95, 62, 25, 82] Resilience of physical-to-digital connections [46, 23, 48, 72, 83]

5. Discussion

The following discussion interprets the identified patterns in relation to established socio-technical perspectives, while retaining the themes developed through the analysis. In particular, work-system thinking supports the interpretation of conceptual and operational fragmentation, socio-technical systems engineering informs the analysis of cascading implementation dependencies, and contextual inquiry informs the proposed investigation of situated organisational workflows [100, 101, 102].

5.1. The Use of Authenticity

In response to the first research question, *"RQ1: how is authenticity described in the context of product passports across sectors?"*, the analysed literature reveals significant definitional variation, as the broader discourse reflects differences in how sectors prioritise and operationalise authenticity.

This variation has multiple sources. One source is the convergence of multiple disciplines, including cybersecurity, supply chain management and regulatory practice, each with established terminology that was not designed to interoperate. This disciplinary diversity means authenticity lacks a unified operational meaning across product passport contexts. The definitional variation highlighted in the results reflects this convergence, ranging from operationally narrow definitions, such as that provided by Lu et al. [36], to an expansive list of attributes as observed in Wu et al. [24]. Compared to the definitions given in ISO/IEC standards, neither aligns consistently. This variation obscures rather than clarifies what authenticity means operationally.

It is worth noting that the breadth of definitions, such as the one provided by [24], may instead reflect contextual differences in how authenticity is operationalised across sectors, wherein it may reasonably encompass broader data quality concerns, or, in other contexts, be applied more narrowly. However, the literature does not make these contextual distinctions explicit, treating both broader and narrower conceptions as if they are alternative versions of the same concept, rather than acknowledging that operational contexts may require different scopes of assurance. A clearer approach may be to represent the larger scopes with multiple security aspects, rather than combining concepts such as data veracity and integrity, to more accurately contextualise and describe use. Such distinctions may also support greater clarity and comparability across future security research.

Further, the literature employs "product authentication" or "data authentication", often conflating identification (proving what a given product is), verification (confirming claimed characteristics) and assurance of something being genuine (confirming the product is not counterfeit). These operations are fundamentally different, and make it further unclear as to what the term means. This is compounded by a gap in international standards and field practice. Despite clear definitional guidance from ISO/IEC, which distinguishes authenticity (the property that an entity is what it claims to be) from authentication (the provision of assurance that a claimed characteristic is correct), the analysed literature predominantly adopts alternative definitions or conflates these distinct concepts. This gap suggests that either the standards are insufficiently specific for product passport contexts, or that practitioners are unaware of or unable to adopt standardised definitions within their operational constraints.

This difficulty can also be interpreted through Alter's work-system perspective, which views human participants and technical components as an integrated system rather than treating information systems solely as technical configurations. From this perspective, the definitional variation identified here also reflects difficulties in reconciling system conceptualisations with operational realities [100].

5.2. Authenticity Across Literature

The second research question asked *"RQ2: What drivers, benefits, and challenges are associated with establishing authenticity in product passports?"*. Through five themes, the results reveal a paradox: while authenticity is increasingly recognized as integral to product passport functionality, its implementation reveals significant structural tensions between what is required, what is technically feasible, and what stakeholders can practically achieve.

5.2.1. Drivers and Benefits of Authenticity Across Sectors

Authenticity in product passports is driven by a convergence of regulations, market demand, and support for core passport functionality. While regulatory requirements establish the foundational imperative for authenticity implementation, authenticity is further valued as an enabler of genuine traceability through supply chains, verification of product safety, and support for circular economy practices. These drivers generate interconnected benefits: authenticity enables transparency and accountability across supply chains, supporting informed decision-making among stakeholders. It further prevents counterfeiting, reducing associated losses and protecting brand integrity. This counterfeiting prevention, combined with enhanced supply chain visibility, builds stakeholder trust, enabling premium pricing for high-quality, sustainably produced goods. This convergence of drivers and benefits suggests that authenticity is not peripheral to product passport systems, but rather integral to their foundational purpose.

5.2.2. Interdependency Constraints

The implementation of authenticity reveals clear cascading dependencies, wherein regulatory ambiguity prevents financial commitment, financial uncertainty defers technological adoption, deferred adoption prevents standardisation, and absent standardisation fragments interoperability. Each domain's constraints enable or block others, forming a sociotechnical coordination challenge that cannot be solved by optimising domains independently.

This systematic tension manifests clearly in the regulations theme, which reveals a gap in current policy design. While regulations create drivers for authenticity, they lack surrounding guidance on implementation specificity. While the EU requirement for verifiable authenticity is clear, our analysis shows that companies interpret it differently due to a lack of guidelines. This imposes an implementation burden on regulated entities, including all actors within the EU market and those seeking to interact with it.

The gap has several cascading effects across other themes. The financial theme reveals that unclear regulatory requirements prevent companies from making confident investments in specific technologies. Instead, companies defer adoption until guidance clarifies which solutions satisfy regulatory requirements. This forms a collective action problem, as without early adopters demonstrating viable approaches, policymakers lack evidence to formulate specific guidance. While authenticity may justify premium pricing, consumer willingness to absorb these costs remains uncertain, weakening incentives for early adoption even where regulatory direction is clear. Simultaneously, the digital infrastructure theme shows that, even with proposed implementations and early adopters, the solutions may not be interoperable, potentially introducing traceability gaps and failing to uphold regulatory compliance. Further, cost and technical competence remain significant barriers for SMEs, which may need to develop expertise before making investment decisions regarding authenticity solutions. Furthermore, if cost assessments fail to account for the sustainability impacts of different authenticity methods, as revealed in the sustainability theme, early adoption may paradoxically lead to environmentally compromised solutions with unnecessarily high energy consumption.

Ideally, regulatory guidance would precede large-scale technology development, reducing financial uncertainty and creating space for interoperable solutions. However, practical reality is inverted, wherein implementation requirements are already upon the industry while standardised approaches remain undefined. Cost structures locked in by early adoption may create interoperability challenges that constrain later participants, while entrenched solutions become costly to replace. The race between deployment and standardisation means that which solutions win will depend less on their technical merit than on which actors can afford to move first.

These coordination failures are further complicated by how authenticity itself is conceptualised across literature. An apparent circularity emerges within the product lifecycle theme, as traceability is used to verify authenticity while confidence in traceability itself depends on prior assurance of authenticity. Existing approaches conflate two different forms of authenticity. One is treated as inferential, wherein a product is authentic because its traceability record appears legitimate, suggesting it followed a

claimed supply chain path. The other treats authenticity in an assertive manner, in which a product is authentic due to inherent properties proven by e.g. material fingerprints, verifying it independently of the historical record. Traceability asks where something came from and authenticity asks whether this is the genuine entity. Rather than representing competing alternatives, object-level proof and provenance assurance provide complementary forms of evidence: the former supports confidence in the entity, while the latter supports confidence in its recorded history. When literature proposes "traceability establishes authenticity" or conversely that "authenticity is required for traceability", these statements operate in different contexts. The apparent circularity emerges as actors attempt to use a tool designed for one purpose (historical verification) to serve another (product- or material-level proof). This mismatch becomes acute when recognizing that a perfectly documented trace of counterfeit goods is still counterfeit, and traceability alone cannot guarantee authenticity. As such, a reframing is necessary. Rather than expecting traceability to establish authenticity, authenticity mechanisms should establish object-level confidence, with traceability serving as a separate function for accountability and compliance.

Collectively, these constraints form a cascading dependency structure, wherein regulatory ambiguity creates financial uncertainty, financial uncertainty delays technological adoption, delayed adoption hinders standardisation, and absent standardisation fragments interoperability. These dependencies also reflect a broader socio-technical systems engineering problem: technical and organisational elements cannot be developed independently when system functionality and use depend upon both. The coordination barriers identified here therefore extend beyond the selection of authenticity mechanisms to the alignment of regulatory guidance, organisational readiness, work practices, and technical infrastructure [101].

5.2.3. Gaps in Current Approaches

These conceptual and coordination limitations reveal consequential gaps in how authenticity is currently framed as a research problem. Authenticity requirements remain under-specified at the operationalisation level. Literature includes several benefits enabled by authenticity, such as preventing counterfeit loss, improving transparency and enabling informed decision making, but provides limited characterisation of how authenticity functions across diverse organisational contexts. Even stakeholder-engaged research may capture functional requirements without fully specifying implementation realities, as a solution that is technically or economically viable in one supply chain may prove impractical in another, particularly across the divide between large enterprises and SMEs.

Further, feasibility assessments remain incomplete in scope. Current evaluations rarely consider organisational readiness, differential burdens across firm sizes, sustainability implications of energy-intensive solutions, or how early design choices constrain future options. Organisations may rationally adopt solutions that are financially feasible in the short term while creating downstream constraints, such as vendor lock-in, data incompatibility or established workflows that limit future flexibility.

In addition, several solutions are designed around assumed rather than demonstrated functions. The gap between inferential and assertive authenticity reveals this directly, as current product passport designs treat traceability as the primary authenticity mechanism, positioning historical verification to solve what is fundamentally an object-level proof problem. This constitutes a mismatch between the evidentiary function of a process history and the object-level property it is expected to establish: a supply-chain record may support provenance assurance, but it cannot independently demonstrate material genuineness. This suggests that authenticity is frequently approached through theoretically plausible indicators rather than explicit consideration of what object-level authenticity requires operationally. Addressing these gaps requires research that integrates understanding of operationalisation realities, fuller cost accounting and how multiple authenticity mechanisms can function as complementary elements in a coherent system.

These gaps reinforce one another. Under-specified authenticity requirements complicate feasibility assessments, while solutions built around assumed rather than demonstrated functions risk validating technically coherent but operationally inadequate approaches. Addressing any one of these issues in

isolation therefore risks producing solutions that appear effective conceptually but fail in practice.

5.2.4. Future Research

As such, various directions for future research emerge. The coherent conceptualisation of authenticity in DPP literature forms a foundational requirement for future work on DPP authenticity, as interconnected challenges cannot be addressed without established groundwork. Once such conceptual foundations are established, future research should map how authenticity mechanisms are operationalised within sector-specific workflows, examining the sequential decision points organisations face when adopting product passports. This may include investigating which technical capabilities companies must develop in-house or outsource, how organisational readiness, such as technical competence, data infrastructure maturity and supply chain integration, varies across firm sizes, or how early technology choices constrain or enable later pivots. Such mapping would inform implementation roadmaps that account for differential starting points, enabling SMEs to adapt solutions proportionate to their resources while larger enterprises plan for scale. Without such empirical understanding, policy guidance risks prescribing technically sound solutions that are organisationally infeasible for significant portions of regulated entities.

In addition, studies examining the sustainability footprint of authenticity mechanisms should develop cost-benefit frameworks that account for lifecycle environmental impacts alongside financial feasibility. This research must quantify energy consumption at each stage (implementation, operation, end-of-life), which mechanisms impose disproportionate environmental burdens, and how environmental costs shift when scaling from pilot to industry-wide deployment. Current adoption decisions made without this information may lock supply chains into solutions that are financially feasible in the short term, but environmentally costly at scale. Such frameworks would enable policymakers to set environmental guardrails alongside authenticity requirements, preventing a scenario where regulatory compliance inadvertently increases supply chain emissions.

Likewise, future work should also investigate how authenticity information is communicated to different stakeholder groups throughout the product lifecycle. While numerous technical mechanisms have been proposed to establish authenticity, less attention has been paid to how authenticity claims are interpreted and evaluated by end users. Questions remain regarding the level of knowledge required to understand authenticity disclosures, how trust is established in secondary markets, and whether authenticity mechanisms remain meaningful as products change ownership over time. Understanding how users interpret authenticity signals may prove as important as establishing authenticity itself, because technically robust solutions provide limited value if stakeholders cannot confidently assess or act on the information presented.

Further, research into enterprise architecture frameworks for product passports could focus on developing reference implementation patterns that guide organisations through integrating authenticity mechanisms into their existing systems. Rather than prescribing a single architectural approach, this research may document how authenticity verification can be operationalised across different organisational contexts, examining decision points, integration requirements and adaptation patterns for enterprises of varying sizes and supply chain complexity. This would enable organisations to follow established patterns rather than designing solutions from scratch, reducing the resource burden that currently defers adoption. Such workflow mapping should be context-sensitive, recognising that organisational actors' understandings and capacities are context-dependent rather than uniform across firms and sectors [102].

Collectively, these research directions address the operationalisation gap, the cost-accounting gap and the coordination gap identified above, while remaining grounded in challenges companies face when implementing authenticity in product passport systems.

6. Conclusions

This literature review examined two research questions: *"RQ1: How is authenticity described in the context of product passports across sectors?"* and *"RQ2: What drivers, benefits, and challenges are associated with establishing authenticity in product passports?"*. Through thematic analysis, five themes emerged: regulations, financial, sustainability, product lifecycle, and digital infrastructure. The review reveals tensions between the recognised importance of authenticity and the practical difficulties of implementing it.

Authenticity is presented across the literature as integral to product passport functionality, enabling traceability, transparency and circular economy practices, and is required by emerging EU regulations. However, the analysis suggests a mismatch between this recognised necessity and the systemic barriers to implementation, wherein findings suggest that authenticity cannot be addressed solely through technical mechanisms, as implementation depends equally on organisational, regulatory, and lifecycle considerations. Regulations drive authenticity, yet implementation guidance remains unclear, creating interconnected and cascading sociotechnical dependencies across themes. While regulatory mandates and market pressures create a powerful social driver for DPP implementation, the organisational capacities and technical infrastructures across supply chains do not yet align. Regulatory ambiguity continues to stall financial investment, which in turn defers technological adoption and fragments ecosystem-wide interoperability.

Amplifying the cascading coordination failure is an underlying and more fundamental issue: definitional variation across sectors, such as conflating authenticity with integrity or treating it as an extensive list of attributes. This is similarly observed in the variation with which it may be implemented, either treated inferentially via traceability or assertively via proofs. The definitional variation suggests that there is no shared conceptual foundation for what authenticity in product passports means or requires. Rather than reflecting legitimate sectoral differences, this variation points to broader conceptual confusion about authenticity itself, extending to how it should be verified, implemented, and evaluated.

Given these interconnected barriers and underlying conceptual confusion, addressing authenticity in product passports requires attention to foundational conceptual work before and alongside regulatory and technical solutions. The lack of shared understanding about what authenticity is undermines both implementation efforts and future security research in product passport contexts. Without conceptual clarity, early adopters create incomplete, divergent solutions that may influence the creation of DPP standards, thereby fragmenting the ecosystem and constraining smaller firms that may lack the resources to develop early adopter approaches. In addition, early solutions may prove an environmental detriment, using energy-intensive and costly digital infrastructures, potentially sabotaging the very goal of sustainability that the DPP pursues.

Acknowledgments

We gratefully acknowledge the financial support provided by the Knowledge Foundation (KKS) through the project *Digital Product Passport Systems for Sustainability (PASS4Sustainability)*, reference number 20240094.

Declaration on Generative AI

During the preparation of this work, the author(s) used Claude Haiku 4.5, Grammarly in order to: Grammar and spelling check, Paraphrase and reword, Peer review simulation. While Rayyan includes AI features, these were not utilized. After using these tools & services, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

Appendix A

Table A1
Queries applied to databases with database-specific modifications due to differences in query syntax and field limitations.

Source	Query-string
ACM	Title:(("Digital Product Passport*" OR "Battery Passport*" OR "Battery Identity Global Passport*" OR "Material* Passport*" OR "Product Circularity Data Sheet*" OR "Resource* Passport*" OR "Digital Lifecycle Passport*" OR "Building Passport*" OR "Building Renovation Passport*" OR "Building Logbook*" OR "C2C Passport*" OR "Cradle to Cradle Passport*" OR "Circularity Passport*" OR "Nutrient* Certificate*" OR "Product* Passport*" OR "Recycling Passport*" OR "Resource Identity Tag*" OR "Technical Passport for Equipment*" OR "Workwear Passport*")) OR Abstract:(("Digital Product Passport*" OR "Battery Passport*" OR "Battery Identity Global Passport*" OR "Material* Passport*" OR "Product Circularity Data Sheet*" OR "Resource* Passport*" OR "Digital Lifecycle Passport*" OR "Building Passport*" OR "Building Renovation Passport*" OR "Building Logbook*" OR "C2C Passport*" OR "Cradle to Cradle Passport*" OR "Circularity Passport*" OR "Nutrient* Certificate*" OR "Product* Passport*" OR "Recycling Passport*" OR "Resource Identity Tag*" OR "Technical Passport for Equipment*" OR "Workwear Passport*")) OR Keyword:(("Digital Product Passport*" OR "Battery Passport*" OR "Battery Identity Global Passport*" OR "Material* Passport*" OR "Product Circularity Data Sheet*" OR "Resource* Passport*" OR "Digital Lifecycle Passport*" OR "Building Passport*" OR "Building Renovation Passport*" OR "Building Logbook*" OR "C2C Passport*" OR "Cradle to Cradle Passport*" OR "Circularity Passport*" OR "Nutrient* Certificate*" OR "Product* Passport*" OR "Recycling Passport*" OR "Resource Identity Tag*" OR "Technical Passport for Equipment*" OR "Workwear Passport*")) AND AllField:((authentic* OR genuine* OR counterfeit* OR fake* OR imitation* OR fals* OR forge* OR original* OR legitimate* OR illegitimate*))
Springer Link	("Digital Product Passport*" OR "Battery Passport*" OR "Battery Identity Global Passport*" OR "Material* Passport*" OR "Product Circularity Data Sheet*" OR "Resource* Passport*" OR "Digital Lifecycle Passport*" OR "Building Passport*" OR "Building Renovation Passport*" OR "Building Logbook*" OR "C2C Passport*" OR "Cradle to Cradle Passport*" OR "Circularity Passport*" OR "Nutrient* Certificate*" OR "Product* Passport*" OR "Recycling Passport*" OR "Resource Identity Tag*" OR "Technical Passport for Equipment*" OR "Workwear Passport*") AND (authentic* OR genuine* OR counterfeit* OR fake* OR imitation* OR fals* OR forge* OR original* OR legitimate* OR illegitimate*)
Scopus	TITLE-ABS-KEY ("Digital Product Passport*" OR "Battery Passport*" OR "Battery Identity Global Passport*" OR "Material* Passport*" OR "Product Circularity Data Sheet*" OR "Resource* Passport*" OR "Digital Lifecycle Passport*" OR "Building Passport*" OR "Building Renovation Passport*" OR "Building Logbook*" OR "C2C Passport*" OR "Cradle to Cradle Passport*" OR "Circularity Passport*" OR "Nutrient* Certificate*" OR "Product* Passport*" OR "Recycling Passport*" OR "Resource Identity Tag*" OR "Technical Passport for Equipment*" OR "Workwear Passport*") AND ALL (authentic* OR genuine* OR counterfeit* OR fake* OR imitation* OR fals* OR forge* OR original* OR legitimate* OR illegitimate*)

Appendix B

Table B1: Description of citation, associated sector, and briefly presenting their topic.

Citation	Sector	Topic
[40]	Batteries	Securing battery management systems via e.g. PUFs and signatures
[46]	Supply chain	Investigates challenges of identifiers in DPPs in Supply Chains
[47]	Automotive industry Wine	Proposes hybrid blockchain-based DPPs with an authenticated viewer
[75]	IoT Supply Chain	Proposes various IoT Supply Chain security measures
[23]	Construction	Evaluates various identifier and data carrier combinations for DPPs in construction
[42]	Footwear	Proposes Decentralized Identifiers as the foundation for DPPs combined with data spaces
[89]	Electric Vehicles Luxury Industry	Advocates for distributed ledger technologies for battery passports
[90]	Supply Chain	Sharing DPP data by managing data sharing policies using Zero-Trust Architecture
[69]	Supply Chain	Discusses valueflows modelling of DPPs
[24]	Construction	Proposes blockchain combined with NFTs for construction waste-material
[37]	Batteries	Proposes blockchain and smart contracts for battery passports
[38]	Construction Real estate	Proposes blockchain in construction as a product passport
[61]	Batteries	Discusses secure data acquisition for battery management systems for battery passports
[50]	General	Proposes scanning fingerprints of material for DPPs
[88]	General	Discusses a predecessor to DPPs and how it may be applied
[76]	General	Discusses blockchain as an enabler for DPPs
[48]	Textiles	Discusses the RAIN RFID as a data carrier option for DPPs
[86]	Batteries	Discusses secure battery management system architecture linked to battery passports
[51]	Textiles Food	Discusses DPPs in textile sector supply chains
[55]	Additive Manufacturing	Examines the use of microstructural fingerprints in additively manufactured components
[49]	General	Investigates the use of ionogels for anti-counterfeiting tags with application for DPPs
[98]	Mechatronics	Investigates DPP integration into sustainable mechatronics design
[41]	General	Presents a sustainability oriented digital architecture
[99]	Plastics	Presents a case study on plastics production related to DPPs
[65]	Manufacturing	Evaluates Web3 technologies in shared manufacturing
[66]	Textiles	Discusses traceability in the textile industry
[56]	Textiles	Investigates consumer attitudes in relation to DPPs
[54]	Mining	Discussing the CERA 4in1 Standards for and their applicability for DPPs
[70]	General	Investigates whether blockchain-based disclosures affect trust
[59]	General	Interviews actors to investigate the impact of DPPs

Table B1: Description of citation, associated sector, and briefly presenting their topic.

Citation	Sector	Topic
[39]	Supply Chain	Proposes data notarization via hybrid Distributed Ledger Technologies
[60]	Hydrogen	Outlining the DPP design requirements for a green hydrogen market
[44]	Batteries	Explores the key benefits of battery circularity
[68]	General	Investigates DIDs and VCs as DPP identity solutions
[58]	General	Compiles interviews, workshops and legal demands to formulate the core aspects of the DPP
[43]	Textiles	Interviews experts to form an overview of technological challenges
[72]	Batteries	Investigating a battery passport using PUFs
[87]	General	Explores decentralised DPPs with asset administration shells
[36]	Construction Waste	Explores waste-material passports in cross-jurisdictional trading
[52]	General	Investigates implementing the DPP via Hyperledger Fabric
[4]	General	Discusses the regulatory evolution, necessity and perspectives on DPPs
[77]	General	Discusses inclusion of RAIN tag scanning in mobile devices
[78]	General	Discusses RAIN tags for enabling DPPs
[79]	General	Presents an implementation of DPPs via a hybrid blockchain architecture
[67]	General	Explores DIDs as a means of accessing DPPs
[57]	General	Presents a framework for DPPs with a proposed blockchain implementation
[45]	Architecture engineering construction (AEC)	Explores digital twins using NFTs with applicability for material passports
[95]	Batteries	Proposes a blockchain-based framework for DPP implementation
[62]	General	Investigates DPP implementation via blockchain for enabling a reverse supply chain
[74]	Textiles Cosmetics	Explores the potential of DPPs to promote innovation and circularity in the fashion and cosmetics sectors
[71]	General	Presents DPPs and discusses RAIN tags as an implementation measure
[85]	Textiles	Discusses DPPs in the context of the textiles sector
[91]	Batteries	Discusses the implications of the battery passport
[63]	General	Explores the requirements, characteristics and a potential implementation for DPPs
[80]	General	Discusses perceived benefits and architectures for implementing DPPs
[64]	General	Presents a novel signature scheme with application for authenticated material passports
[1]	General	The EU regulations presenting general DPP contents
[25]	General	Explores the integration of blockchain into DPPs to facilitate information transparency
[73]	Plastics	Investigates the use of DPPs to overcome information asymmetry in plastics value chains

Table B1: Description of citation, associated sector, and briefly presenting their topic.

Citation	Sector	Topic
[81]	Batteries	Discusses cryptographic co-processors in BMSs with battery passports as an implementation solution
[82]	Batteries	Proposes RFID for the implementation of battery passports
[92]	General	Proposes the use of LLMs and blockchain for the creation of verifiable DPP records
[96]	General	Discusses the current state of the DPP in the context of social and environmental sustainability
[93]	General	Presents a hybrid DLT approach for the creation of DPPs
[97]	Energy Sector	Discusses data sharing trust in the energy sector
[83]	Textile, electronics, battery	Investigating the benefits and barriers to the use of DPPs across stakeholders
[84]	General	Investigates DPP related initiatives
[53]	General	Investigates DPP costs and benefits for SMEs
[94]	Raw material supply chain	Presentation of system architecture model developed within the MaDiTraCe project

References

[1] Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 establishing a framework for the setting of ecodesign requirements for sustainable products, amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and repealing Directive 2009/125/EC (Text with EEA relevance), 2024. URL: http://data.europa.eu/eli/reg/2024/1781/oj, legislative Body: EP, CONSIL.

[2] K. Voulgaridis, T. Lagkas, C. M. Angelopoulos, A.-A. A. Boulogeorgos, V. Argyriou, P. Sarigiannidis, Digital product passports as enablers of digital circular economy: a framework based on technological perspective, Telecommunication Systems 85 (2024) 699–715. URL: https://doi.org/10.1007/s11235-024-01104-x. doi:10.1007/s11235-024-01104-x.

[3] E. Union, EU's Digital Product Passport: Advancing transparency and sustainability | EU Retail Platform, 2025. URL: https://transition-pathways.europa.eu/retail/policy/eus-digital-product-passport-advancing-transparency-and-sustainability, (visited on 2026-06-10).

[4] T. Götz, H. Berg, M. Jansen, T. Adisorn, D. Cembrero, S. Markkanen, T. Chowdhury, Digital product passport : the ticket to achieving a climate neutral and circular European economy? (2022). URL: https://epub.wupperinst.org/frontdoor/index/index/docId/8049.

[5] H. Wicaksono, A. Mengistu, A. Bashyal, T. Fekete, Digital Product Passport (DPP) technological advancement and adoption framework: A systematic literature review, Procedia Comput. Sci. 253 (2025) 2980–2989. doi:10.1016/j.procs.2025.02.022.

[6] Z. Zhang, J. Gu, R. Li, W. Lian, C. Ma, J. Tian, Bridging digital and green transitions: A literature review of digital product passport systems, Renewable and Sustainable Energy Reviews 228 (2026). doi:10.1016/j.rser.2025.116600.

[7] N. Fares, M. S. Islam, S. K. Jauhar, B. Kucukaltan, Towards an International Digital Product Passport: The New Paradigm of a Worldwide Circular Economy, Circular Economy and Sustainability 5 (2025) 5475–5495. URL: https://doi.org/10.1007/s43615-025-00690-5. doi:10.1007/s43615-025-00690-5.

[8] M. Munaro, S. Tavares, Materials passport's review: challenges and opportunities toward a circular economy building sector, Built Environment Project and Asset Management 11 (2021) 767–782. doi:10.1108/BEPAM-02-2020-0027.

[9] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS The European Green Deal, 2019. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52019DC0640.

[10] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A new Circular Economy Action Plan For a cleaner and more competitive Europe, 2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0098.

[11] C. Plociennik, M. Pourjafarian, S. Saleh, T. Hagedorn, A. d. Carmo Precci Lopes, M. Vogelgesang, J. Baehr, B. Kellerer, M. Jansen, H. Berg, M. Ruskowski, L. Schebek, A. Ciroth, Requirements for a digital product passport to boost the circular economy, INFORMATIK 2022, 2022. doi:10.18420/inf2022_127.

[12] 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 (Text with EEA relevance), 2023. URL: http://data.europa.eu/eli/reg/2023/1542/oj, legislative Body: EP, CONSIL.

[13] G. Capelleveen, D. Vegter, M. Olthaar, J. Hillegersberg, The anatomy of a passport for the circular economy: A conceptual definition, vision and structured literature review, Resources, Conservation & Recycling Advances 17 (2023). doi:10.1016/j.rcradv.2023.200131.

[14] P. K. F. Wan, S. Jiang, Enabling a dynamic information flow in digital product passports during product use phase: A literature review and proposed framework, Sustainable Production and Consumption 54 (2025) 362–374. doi:10.1016/j.spc.2025.01.014.

[15] R. von Solms, J. van Niekerk, From information security to cyber security, Computers & Security 38 (2013) 97–102. doi:10.1016/j.cose.2013.04.004.

[16] G. Kaur, Z. Habibi Lashkari, A. Habibi Lashkari, Introduction to Cybersecurity, in: G. Kaur, Z. Habibi Lashkari, A. Habibi Lashkari (Eds.), Understanding Cybersecurity Management in FinTech: Challenges, Strategies, and Trends, Springer International Publishing, Cham, 2021, pp. 17–34. doi:10.1007/978-3-030-79915-1_2.

[17] B. Sangchoolie, P. Folkesson, P. Kleberger, J. Vinter, Analysis of Cybersecurity Mechanisms with respect to Dependability and Security Attributes, in: 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), 2020, pp. 94–101. doi:10.1109/DSN-W50199.2020.00027, iSSN: 2325-6664.

[18] R. C. Reid, A. H. Gilbert, Using the parkerian hexad to introduce security in an information literacy class, in: 2010 Information Security Curriculum Development Conference, InfoSecCD '10, Association for Computing Machinery, New York, NY, USA, 2010, p. 45–47. URL: https://dl.acm.org/doi/10.1145/1940941.1940953. doi:10.1145/1940941.1940953.

[19] M. Dworkin, Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication, Technical Report NIST Special Publication (SP) 800-38B, National Institute of Standards and Technology, 2016. URL: https://csrc.nist.gov/pubs/sp/800/38/b/upd1/final. doi:10.6028/NIST.SP.800-38B.

[20] Joint Task Force Transformation Initiative, Managing Information Security Risk: Organization, Mission, and Information System View, Technical Report NIST Special Publication (SP) 800-39, National Institute of Standards and Technology, 2011. URL: https://csrc.nist.gov/pubs/sp/800/39/final. doi:10.6028/NIST.SP.800-39.

[21] ISO/IEC 27000, Information technology – Security techniques – Information security management systems – Overview and vocabulary, 2018.

[22] ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls, 2022.

[23] B. S. Byers, P. Emmenegger, J. J. Hunhevicz, D. Schumm, F. Heisel, D. M. Hall, C. De Wolf, Decentralized phygital identifier systems for digital passports in circular construction: a design science evaluation, Construction Innovation (2025) 1–35. doi:10.1108/CI-02-2025-0074.

[24] L. Wu, W. Lu, Z. Peng, C. Webster, A blockchain non-fungible token-enabled 'passport' for construction waste material cross-jurisdictional trading, Automation in Construction 149 (2023) 104783. doi:10.1016/j.autcon.2023.104783.

[25] A. Saleheen, S. Afrid, Potential of decentralised blockchains for the digital product passport : Need for traceability and transparency in textile industries, Master's thesis, University of Borås, 2023. URL: https://urn.kb.se/resolve?urn=urn:nbn:se:hb:diva-30585.

[26] B. Kitchenham, S. Charters, Guidelines for performing Systematic Literature Reviews in Software Engineering, EBSE Technical Report EBSE-2007-01, Technical Report, Keele University and Durham University, 2007.

[27] C. Wohlin, Guidelines for snowballing in systematic literature studies and a replication in software engineering, in: Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering, EASE '14, Association for Computing Machinery, New York, NY, USA, 2014, pp. 1–10. doi:10.1145/2601248.2601268.

[28] E. Mourão, J. F. Pimentel, L. Murta, M. Kalinowski, E. Mendes, C. Wohlin, On the performance of hybrid search strategies for systematic literature reviews in software engineering, Information and Software Technology 123 (2020) 106294. doi:10.1016/j.infsof.2020.106294.

[29] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, R. Chou, J. Glanville, J. M. Grimshaw, A. Hróbjartsson, M. M. Lalu, T. Li, E. W. Loder, E. Mayo-Wilson, S. McDonald, L. A. McGuinness, L. A. Stewart, J. Thomas, A. C. Tricco, V. A. Welch, P. Whiting, D. Moher, The PRISMA 2020 statement: an updated guideline for reporting systematic reviews, BMJ (2021) n71. doi:10.1136/bmj.n71.

[30] Merriam-Webster, Merriam-Webster, 2026. URL: https://www.merriam-webster.com/, (visited on 2026-06-10).

[31] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, M. Khalil, Lessons from applying the systematic literature review process within the software engineering domain, Journal of Systems and Software 80 (2007). doi:10.1016/j.jss.2006.07.009.
[32] Rayyan, AI-Powered Systematic Review & Literature Review Platform, 2026. URL: https://www.rayyan.ai/, (visited on 2026-06-10).
[33] Zotero, Zotero | Your personal research assistant, 2026. URL: https://www.zotero.org/, (visited on 2026-06-10).
[34] V. Braun, V. Clarke, Using thematic analysis in psychology, Qualitative Research in Psychology 3 (2006) 77–101. doi:10.1191/1478088706qp063oa.
[35] S. K. Ahmed, R. A. Mohammed, A. J. Nashwan, R. H. Ibrahim, A. Q. Abdalla, B. M. M. Ameen, R. M. Khdhir, Using thematic analysis in qualitative research, Journal of Medicine, Surgery, and Public Health 6 (2025) 100198. doi:10.1016/j.glmedi.2025.100198.
[36] W. Lu, Z. Peng, C. Webster, L. Wu, Developing a construction waste material 'passport' for cross-jurisdictional trading, Journal of Cleaner Production 414 (2023) 137509. doi:10.1016/j.jclepro.2023.137509.
[37] S. Yılmaz, İ. Kösesoy, A blockchain-based framework to sustainable ev battery recycling and tracking, Electronics 14 (2025). doi:10.3390/electronics14244854.
[38] J. Bronckers, Digital Building Logbook—The Mother Use Case for Blockchain in Real Estate, in: A. Jreisat, M. Mili (Eds.), Blockchain in Real Estate: Theoretical Advances and New Empirical Applications, Springer Nature, Singapore, 2024, pp. 207–232. doi:10.1007/978-981-99-8533-3_11.
[39] D. Tortola, C. Felicioli, A. Canciani, F. Severino, Scalable Data Notarization Leveraging Hybrid DLTs, in: 2024 32nd International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2024, pp. 20–25. doi:10.1109/WETICE64632.2024.00013.
[40] L. Crocetti, R. Di Rienzo, A. Verani, F. Baronti, R. Roncella, R. Saletti, A Novel and Robust Security Approach for Authentication, Integrity, and Confidentiality of Lithium-ion Battery Management Systems, in: 2023 IEEE 3rd International Conference on Industrial Electronics for Sustainable Energy Systems (IESES), 2023, pp. 1–6. doi:10.1109/IESES53571.2023.10253728.
[41] A. Naraločnik, Artificial Intelligence and Blockchain-Driven Circular Platforms: Fostering Green Innovation and Sustainable Consumer Behavior in High-Value Resale, Sustainability 17 (2025). doi:10.3390/su172411224.
[42] C. Sousa, R. Ferreira, P. Pinto, C. Pereira, R. Rebelo, Digital Product Passport Architecture for Boosting Circularity in Footwear Industry, Procedia Computer Science 239 (2024) 1560–1567. doi:10.1016/j.procs.2024.06.331.
[43] J. Domskienė, E. Gaidule, An overview of technological challenges in implementing the digital product passport in the textile and clothing industry, AUTEX Research Journal 24 (2024). doi:10.1515/aut-2024-0002.
[44] M. Ebrahimi, K. Chirumalla, A. Fattouh, Enabling Battery Circularity with Blockchain Technology: An Exploratory Study of Key Benefits, in: H. Mizuyama, E. Morinaga, T. Nonaka, T. Kaihara, G. von Cieminski, D. Romero (Eds.), Advances in Production Management Systems. Cyber-Physical-Human Production Systems: Human-AI Collaboration and Beyond, Springer Nature Switzerland, Cham, 2026, pp. 402–416. doi:10.1007/978-3-032-03546-2_27.
[45] H. Naderi, A. Shojaei, Digital twin non-fungible token (DT-NFT): Enabling data ownership in the AEC industry, Automation in Construction 168 (2024) 105777. doi:10.1016/j.autcon.2024.105777.
[46] D. Palm, N. Kuenster, F. Dorka, M. Buecheler, Architectures And Systems For Identifying Assets In Circular Supply Chains Using Digital Product Passports And The Asset Administration Shell (2024) 898–905. URL: https://repo.uni-hannover.de/handle/123456789/17909. doi:10.15488/17776, book Title: Proceedings of the Conference on Production Systems and Logistics: CPSL 2024.
[47] D. Tortola, C. Felicioli, A. Canciani, F. Severino, Authenticated data visualization for hybrid blockchain-based digital product passports, Computer Communications 236 (2025) 108110. doi:10.1016/j.comcom.2025.108110.

[48] P. Ugale, M. Brewster, Unlocking Circularity in Textiles Through a RAIN-Enabled Automated Framework, IEEE Journal of Radio Frequency Identification 9 (2025) 919–936. doi:10.1109/JRFID.2025.3636554.

[49] S. I. C. J. Palma, E. Ramou, A. C. A. Roque, Random and unpredictable optical textures in biobased self-assembled ionogels for dynamic anti-counterfeiting tags, Communications Materials 6 (2025) 208. doi:10.1038/s43246-025-00940-x.

[50] W. Berchtold, M. Steinebach, Securing Product Identity With Digital Fingerprinting, IST International Surface Technology 18 (2025) 46–47. doi:10.1007/s35724-025-1712-9.

[51] E. Acciai, S. Pérez-Bou, Exploring the role of digital product passports for supply chain traceability in the "made in italy" textile sector, Asia Pacific Journal of Marketing and Logistics 38 (2026) 916–932. URL: https://www.sciencedirect.com/science/article/pii/S1355585525001480. doi:10.1108/APJML-03-2025-0371.

[52] M. Hulea, R. Miron, V. Muresan, Digital Product Passport Implementation Based on Multi-Blockchain Approach with Decentralized Identifier Provider, Applied Sciences 14 (2024). doi:10.3390/app14114874.

[53] C. Bernier, A. Dao, M. Gupta, K. Kocia, M. Le, A. Schneider, A study on DPP costs and benefits for SMEs, Technical Report, CIRPASS Consortium, 2024. URL: https://cirpassproject.eu/wp-content/uploads/2024/03/CIRPASS-A-study-on-DPP-costs-and-benefits-for-SMEs-v1.0-1.pdf.

[54] T. Nowaz, P. Fernandez, L. Foerster, M. Tost, D. Monfort Climent, S. Olmos Betin, F. Melcher, Navigating the Mining Industry Challenges: An Introduction to the CERA 4in1 Standards, BHM Berg- und Hüttenmännische Monatshefte 170 (2025) 108–115. doi:10.1007/s00501-025-01556-x.

[55] K. Gupta, K. Poka, A. Ulbricht, A. Waske, Identification and authentication of additively manufactured components using their microstructural fingerprint, Materials & Design 254 (2025) 113986. doi:10.1016/j.matdes.2025.113986.

[56] R. Zhao, C. Liu, Consumer Acceptance of Digital Product Passports: The Roles of Technological Awareness and Value Orientations, Sustainability 17 (2025). doi:10.3390/su172310878.

[57] S. Nowacki, G. M. Sisik, C. M. Angelopoulos, Digital Product Passports: Use Cases Framework and Technical Architecture Using DLT and Smart Contracts, in: 2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT), 2023, pp. 373–380. doi:10.1109/DCOSS-IoT58021.2023.00067, iSSN: 2325-2944.

[58] M. R. N. King, P. D. Timms, S. Mountney, A proposed universal definition of a Digital Product Passport Ecosystem (DPPE): Worldviews, discrete capabilities, stakeholder requirements and concerns, Journal of Cleaner Production 384 (2023) 135538. doi:10.1016/j.jclepro.2022.135538.

[59] F.-A. Kemmner, H. Legenvre, A.-P. Hameri, Sharing data to implement the circular economy: the case of digital product passports, Industrial Management & Data Systems 125 (2025) 2854–2873. doi:10.1108/IMDS-04-2024-0403.

[60] P. Heeß, J. Rockstuhl, M.-F. Körner, J. Strüker, Enhancing trust in global supply chains: Conceptualizing Digital Product Passports for a low-carbon hydrogen market, Electronic Markets 34 (2024) 10. doi:10.1007/s12525-024-00690-7.

[61] F. Basic, C. Seifert, C. Steger, R. Kofler, Secure Data Acquisition for Battery Management Systems, in: 2023 26th Euromicro Conference on Digital System Design (DSD), 2023, pp. 553–560. doi:10.1109/DSD60849.2023.00082, iSSN: 2771-2508.

[62] H. Xia, J. Li, Q. Jan Li, J. Milisavljevic-Syed, K. Salonitis, Integrating blockchain with digital product passports for managing reverse supply chain, Transportation Research Part E: Logistics and Transportation Review 202 (2025) 104336. doi:10.1016/j.tre.2025.104336.

[63] D. S. Guth-Orlowski, The digital product passport and its technical implementation, 2023. URL: https://medium.com/@susi.guth/the-digital-product-passport-and-its-technical-implementation-efdd09a4ed75, (visited on 2026-06-10).

[64] D. Roio, A. Ibrisevic, A. D'Intino, Reflow: Zero Knowledge Multi Party Signatures with Application to Distributed Authentication, 2021. doi:10.48550/arXiv.2105.14527. arXiv:2105.14527.

[65] P. Stuckmann-Blumenstein, L. Krämer, D. Bons, P. Keitzl, E. Burov, Shared Manufacturing, in: W. Prinz, D. Trauth (Eds.), Tokenizing the Future: A Guide to Web3 and the Metaverse, Springer Nature Switzerland, Cham, 2025, pp. 385–398. doi:10.1007/978-3-031-91405-8_25.

[66] L. Borsacchi, Certification Standards and Ecolabelling for Sustainability and Traceability in the Textile Supply Chain, in: W. Ozuem, S. Ranfagni, C. Millman (Eds.), Sustainable Digital Marketing for Fashion and Luxury Brands: Theory and Practice, Springer Nature Switzerland, Cham, 2025, pp. 675–697. doi:10.1007/978-3-031-82467-8_28.

[67] D. S. Guth-Orlowski, Accessing Digital Product Passports with Decentralized Identifiers (DIDs), 2023. URL: https://medium.com/spherity/accessing-digital-product-passports-with-decentralized-identifiers-dids-175ca455cee3, (visited on 2026-06-10).

[68] I. I. García, F. D. Muñoz-Escoí, J. A. Aroca, F. J. F.-B. Peñuela, Digital Product Passport Management with Decentralised Identifiers and Verifiable Credentials, 2024. doi:10.48550/arXiv.2410.15758. arXiv:2410.15758.

[69] D. Roio, A. Burns, S. Bocconi, Implementing a Digital Product Passport to Support the Open-Source Hardware Community, in: M. Moritz, T. Redlich, S. Buxbaum-Conradi, J. P. Wulfsberg (Eds.), Global collaboration, local production: Fab City als Modell für Kreislaufwirtschaft und nachhaltige Entwicklung, Springer Fachmedien, Wiesbaden, 2024, pp. 101–113. doi:10.1007/978-3-658-44114-2_8.

[70] D. Antsipava, E. A. van Reijmersdal, J. Strycharz, G. van Noort, Can Blockchain-Based Authenticity Disclosures Increase Consumer Trust in Online Advertising?, Journal of Advertising 55 (2026) 156–183. URL: https://doi.org/10.1080/00913367.2025.2510233. doi:10.1080/00913367.2025.2510233.

[71] J. Dossett, What is a Digital Product Passport and How Does It Affect Me?, 2024. URL: https://www.impinj.com/library/blog/what-is-a-digital-product-passport, (visited on 2026-06-10).

[72] J. Blümke, H.-J. Hof, Authentic Batteries: A Concept for a Battery Pass Based on PUF-enabled Certificates, in: The Sixteenth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2022), Zenodo, 2022. doi:10.5281/zenodo.7457486.

[73] H. Berg, R. Kulinna, C. Stöcker, S. Guth-Orlowski, R. Thiermann, N. Porepp, Overcoming information asymmetry in the plastics value chain with digital product passports : how decentralised identifiers and verifiable credentials can enable a circular economy for plastics, Working Paper, Wuppertal Institut für Klima, Umwelt, Energie, Wuppertal, 2022. URL: https://nbn-resolving.org/urn:nbn:de:bsz:wup4-opus-79405. doi:10.48506/opus-7940.

[74] B. Becchi, I. D'Adamo, S. Di Leo, M. Gastaldi, C. Grosso, C. Trusiani, Integrating knowledge management and digital product passports to foster sustainable and collaborative ecosystems, Journal of Knowledge Management 30 (2026) 214–241. doi:10.1108/JKM-10-2025-1512.

[75] D. Kasimatis, I. Politis, N. Pitropakis, P. Papadopoulos, W. J. Buchanan, Decentralized Device Identity: PUF-Driven Soulbound Token Verification for IoT Supply Chain Security, IEEE Transactions on Consumer Electronics 72 (2026) 332–341. doi:10.1109/TCE.2025.3642921.

[76] N. Williams, Transparency and Technology: How to Transform to Sustainability by Applying Blockchain Technology, in: P. Wollmann, R. Püringer (Eds.), Transforming Public and Private Sector Organizations: Implementing Sustainable Purpose, Travelling Organization and Connectivity for Resilience, Springer International Publishing, Cham, 2022, pp. 345–357. doi:10.1007/978-3-031-06904-8_19.

[77] C. Fusaro, Enabling a new wave of innovation: RAIN in mobile handsets, 2024. URL: https://therainalliance.org/enabling-a-new-wave-of-innovation-rain-rfid-in-mobile-handsets/, (visited on 2026-06-10).

[78] T. R. Alliance, Enhancing Circularity With RAIN-Enabled Digital Product Passports, 2024. URL: https://therainalliance.org/wp-content/uploads/2024/08/RAIN_Alliance_DPP_Position_Paper_9-18-24.pdf, (visited on 2026-06-10).

[79] A. Canciani, C. Felicioli, F. Severino, D. Tortola, Enhancing Supply Chain Transparency through Blockchain Product Passports, in: 2024 IEEE International Conference on Pervasive Computing

and Communications Workshops and other Affiliated Events (PerCom Workshops), 2024, pp. 751–756. doi:10.1109/PerComWorkshops59983.2024.10502429, iSSN: 2766-8576.

[80] J. Hazan, P.-F. Marteau, M. Merenda, P. N. Hurstel, F. Montagnon, The case for native Digital Product Passport tokenization, Joint Report, Boston Consulting Group & Arianee, 2023. URL: https://web-assets.bcg.com/67/d2/b56ba814487198e87b533255161f/bcgxarianee-digital-product-passport-vf.pdf, (visited on 2026-06-10).

[81] L. Crocetti, L. Montemaggi, R. Di Rienzo, F. Baronti, R. Roncella, R. Saletti, On the Necessity, Security Requirements and Performance Requirements of Digital Signature Co-processors in Li-ion BMSs, in: 2023 IEEE 2nd Industrial Electronics Society Annual On-Line Conference (ONCON), 2023, pp. 1–6. doi:10.1109/ONCON60463.2023.10430543.

[82] F. Scherr, F. Basic, P. Eder, C. Steger, R. Kofler, Next-Generation Battery Management Systems: Integrating RFID for Battery Passport Applications, in: 2024 IEEE International Conference on RFID Technology and Applications (RFID-TA), 2024, pp. 137–140. doi:10.1109/RFID-TA64374.2024.10965188, iSSN: 2836-3574.

[83] T. Wautelet, A.-C. Ayed, D2.2 Exploring possible Digital Product Passport (DPP) use cases in battery, electronics and textile value chains, Technical Report, CIRPASS Consortium, 2024. doi:10.5281/zenodo.10974901.

[84] SLR, CEA, Polimi, D3.1 Annex: DPP Related Initiatives, Technical Report, CIRPASS Consortium, 2024. URL: https://cirpassproject.eu/wp-content/uploads/2024/02/CIRPASS-D3.1-Annex-V8.pdf.

[85] Ultimate Guide to Digital Product Passport for Textiles, 2025. URL: https://thetextilethinktank.org/ultimate-guide-to-digital-product-passport-for-textiles/, (visited on 2026-06-10).

[86] F. Basic, C. R. Laube, P. Stratznig, C. Steger, R. Kofler, Wireless BMS Architecture for Secure Readout in Vehicle and Second life Applications, in: 2023 8th International Conference on Smart and Sustainable Technologies (SpliTech), 2023, pp. 1–6. doi:10.23919/SpliTech58164.2023.10193573.

[87] S. de Diego, I. Gutiérrez-Aguero, Decentralized Digital Product Passport Building Blocks for Enhancing Supply Chain Sovereignty and Circular Economy Practices, IEEE Access 13 (2025) 137973–137985. doi:10.1109/ACCESS.2025.3594826.

[88] S. Balakrichenan, Smart City Standardization in France: The Case of Proxi-Produit Project to the DPP Policy, in: L. Anthopoulos (Ed.), Smart City Standardization: A Global Perspective, Springer Nature Switzerland, Cham, 2025, pp. 217–233. doi:10.1007/978-3-031-95959-2_12.

[89] C. Vestergaard, H. A. Bobosha, K. Langfeldt, Distributed Ledger Technology: Beyond the Hype, in: C. Vestergaard (Ed.), Blockchain for International Security: The Potential of Distributed Ledger Technology for Nonproliferation and Export Controls, Springer International Publishing, Cham, 2021, pp. 7–22. doi:10.1007/978-3-030-86240-4_2.

[90] F. Stodt, P. Ruf, C. Reich, F. Theoleyre, Distributed zero trust architecture based on policy negotiation secured by DPP in blockchain, Annals of Telecommunications 80 (2025) 1053–1070. doi:10.1007/s12243-025-01124-x.

[91] The global battery alliance battery passport: giving an identity to the EV's most important component, Technical Report, Global Battery Alliance, 2020. URL: https://www.globalbattery.org/media/publications/wef-gba-battery-passport-overview-2021.pdf, (visited on 2026-06-10).

[92] D. Rohrschneider, M. Pehlke, U. Handmann, M. Jansen, LLM-based JSON Mapping and Blockchain Integration for Digital Product Passports, Digital Business 6 (2026) 100167. doi:10.1016/j.digbus.2026.100167.

[93] A. Canciani, C. Felicioli, A. Lisi, F. Severino, Hybrid DLT as a data layer for real-time, data-intensive applications, 2023. doi:10.48550/arXiv.2304.07165. arXiv:2304.07165.

[94] R. Abdallah, D. Şahinel, O. A. Adarve, D. Montfort, Enhancing Digital Product Passports with Material Fingerprinting and Decentralized Non-Conformity Signals: Application to Critical Raw Materials, Procedia Computer Science 277 (2026) 1051–1060. doi:10.1016/j.procs.2026.02.145.

[95] R. Kannappan, J. Hatin, E. Bertin, N. Crespi, Enhancing Digital Product Passport Through Decentralized Digital Twins, in: 2025 12th IFIP International Conference on New Technologies,

Mobility and Security (NTMS), 2025, pp. 300–308. doi:10.1109/NTMS65597.2025.11076730, iSSN: 2157-4960.

[96] L. Panza, G. Bruno, F. Lombardi, Integrating Absolute Sustainability and Social Sustainability in the Digital Product Passport to Promote Industry 5.0, Sustainability 15 (2023). doi:10.3390/su151612552.

[97] T. Zwede, M. Ehaus, M. Babel, P. Heeß, L. Schick, M.-F. Körner, J. Strüker, Designing and implementing the trust diamond for verifiable and privacy-preserving data sharing: engineering energy flexibility provision, Energy Informatics 8 (2025) 143. doi:10.1186/s42162-025-00603-8.

[98] M. Hammadi, S. Merschak, T. M. L. Diallo, P. Hehenberger, CEF-DPP: A Circular Economy Framework Integrating Digital Product Passport for Improving Circularity of Sustainable Mechatronics Design, Circular Economy and Sustainability 5 (2025) 3431–3463. doi:10.1007/s43615-025-00550-2.

[99] T. Rumetshofer, K. Straka, J. Fischer, How the Digital Product Passport Can Lead the Plastics Industry towards a Circular Economy—A Case Study from Bottle Caps to Frisbees, Polymers 16 (2024). doi:10.3390/polym16101420.

[100] S. Alter, Sociotechnical systems through a work system lens: A possible path for reconciling system conceptualizations, business realities, and humanist values in is development, volume 1374, 2015.

[101] G. Baxter, I. Sommerville, Socio-technical systems: From design methods to systems engineering, Interacting with Computers 23 (2011) 4–17. URL: https://www.sciencedirect.com/science/article/pii/S0953543810000652. doi:https://doi.org/10.1016/j.intcom.2010.07.003.

[102] R. Glanville, D. Griffiths, P. Baron, P. Bednar, C. E. Welch, Contextual inquiry and socio-technical practice, Kybernetes 43 (2014) 1310–1318. URL: https://www.emerald.com/k/article-pdf/43/9-10/1310/1800521/k-07-2014-0156.pdf. doi:10.1108/K-07-2014-0156.