Poster Presentation - Authenticity in Digital Product Passports

Linus Sönnerhed

Abstract

Digital Product Passports (DPPs) aim to enhance supply chain traceability and sustainability [1]. While literature recognises cybersecurity as essential, it predominantly addresses confidentiality, integrity, and availability [2], overlooking authenticity, the property of being genuine. The focus on implementing authenticity in DPPs is proposed to offer distinct benefits: preventing counterfeits, which annually cause large financial losses [3], preventing unsafe commodities, including safety-compromised vehicle batteries [4], and strengthening the traceability and sustainability offerings of the DPP [5].

While the benefits of authenticity for DPPs are conceptually established, realising these benefits in practice remains unclear. Multiple approaches to authenticity verification exist, ranging from cryptographic data signatures [6] to physical data carrier security (e.g. QR, NFC, RFID) [6, 7, 8]. Such propositions often provide partial solutions, e.g., utilising cryptographic signatures, but failing to account for maintaining a reliable link between the physical product and its digital counterpart [9]. Further, propositions have yet to be empirically tested in real-world supply chain contexts, requiring additional research to assess their usability and practical costs from different actor- and role-based perspectives as well as sector-specific constraints. This requires identifying stakeholders and understanding their needs, use cases, and limitations regarding authenticity in DPPs.

This research investigates: *how can authenticity in DPPs be realised in practice?* To answer this, the research identifies which actors and roles shape DPP authenticity application and what constraints and requirements they face across sectors. Further, candidate authenticity verification approaches are identified at both the data-layer, including cryptographic mechanisms, and the product-layer, such as data carrier security measures. The results of both studies serve to inform the design of a DPP structure integrating authenticity verification approaches. Such a design can then be cyclically evaluated and iteratively improved for feasibility, usability, and cost, based on the feedback of DPP ecosystem actors.

This research will provide empirical evidence on the practical viability of authenticity for DPPs. By identifying actor requirements and real-world constraints, the findings support the design of DPP systems that balance security, usability, and cost, enabling policymakers to mandate authenticity mechanisms that industries can feasibly implement. This bridges the gap between DPP aspiration and market adoption, enabling supply chain traceability and sustainability goals at scale.

References

[1] M. Hulea, R. Miron, and V. Muresan. "Digital product passport implementation based on multi-blockchain approach with decentralized identifier provider". In: *Appl Sci* 14 (2024). DOI: 10.3390/app14114874. URL: https://doi.org/10.3390/app14114874.

[2] M. Jansen et al. "Stop guessing in the dark: Identified requirements for digital product passport systems". In: *Systems* 11 (2023). DOI: 10.3390/systems11030123. URL: https://doi.org/10.3390/systems11030123.

[3] M. R. Carro-Temboury et al. "An optical authentication system based on imaging of excitation-selected lanthanide luminescence". In: *Sci. Adv.* 4 (2018). DOI: 10.1126/sciadv.1701384. URL: https://doi.org/10.1126/sciadv.1701384.

[4] K. Gupta et al. "Identification and authentication of additively manufactured components using their microstructural fingerprint". English. In: *Materials and Design* 254 (2025). ISSN: 02641275 (ISSN); 9781856174978 (ISBN). DOI: 10.1016/j.matdes.2025.113986. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-105004077170&doi=10.1016%2Fj.matdes.2025.113986&partnerID=40&md5=f1bad206913efa08f6b3c42cd0eb40d1.

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

[6] Domenico Tortola et al. "Authenticated data visualization for hybrid blockchain-based digital product passports". In: *Computer Communications* 236 (Apr. 2025), p. 108110. ISSN: 0140-3664. DOI: 10.1016/j.comcom.2025.108110. URL: https://www.sciencedirect.com/science/article/pii/S0140366425000672 (visited on 04/28/2026).

[7] T. Götz et al. "Digital Product Passport: the Ticket to Achieving a Climate Neutral and Circular European Economy?" undefined. In: *Digital Product Passport: The Ticket to Achieving a Climate Neutral and Circular European Economy?* (2022). URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85144882929&partnerID=40&md5=ca3081bec5bc00c87efde53f3934d937.

[8] P. Ugale and M. Brewster. "Unlocking Circularity in Textiles Through a RAIN-Enabled Automated Framework". English. In: *IEEE Journal of Radio Frequency Identification* 9 (2025), pp. 919–936. DOI: 10.1109/JRFID.2025.3636554. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-105023307365&doi=10.1109%2FJRFID.2025.3636554&partnerID=40&md5=7d2c1b29d7af0ccf7966817fca433c68.

[9] Santiago de Diego and Iván Gutiérrez-Aguero. "Decentralized Digital Product Passport Building Blocks for Enhancing Supply Chain Sovereignty and Circular Economy Practices". In: *IEEE Access* 13 (2025), pp. 137973–137985. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2025.3594826. URL: https://ieeexplore.ieee.org/abstract/document/11106427 (visited on 05/05/2026).