ISSN 2616-7433 Vol. 7, Issue 6: 1-6, DOI: 10.25236/FSST.2025.070601

A Brief Analysis of the Path of Promoting Digital Passports through Electronic Information Products

Hongliang Zhao[1], Pinghe Zhang[2,*]

[1]*China Electronics Standardization Institute, Beijing, China*
[2]*Education & Examination Center of Ministry of Industry and Information Technology, Beijing, China*
**Corresponding author: 18511336623@163.com*

Abstract: *With the increasing global resource constraints and environmental protection requirements, "Digital Product Passport" (DPP), as a key tool for tracing product information throughout its life cycle, is becoming an important tool for promoting the greening, compliance and sustainable development of electronic information products. Based on the concept of digital passport and international practice, this paper analyzes the three major challenges faced in promoting the digital passport of electronic information products, namely technical standards, data security and business models, and proposes corresponding promotion paths.*

Keywords: *Digital Passport, Electronic Information Products, Sustainable Development*

1. Introduction

The life cycle of electronic information products (including smartphones, tablets, PCs, smart wearable devices, etc.) is complex, involving multiple links such as material mining, manufacturing, circulation, use and recycling. Traditional labels, barcodes or QR codes only record limited information and are difficult to meet the in-depth needs of green manufacturing, compliance management and circular economy. Digital passports enable online access to the entire chain of data such as product material sources, production processes, performance parameters, energy efficiency indicators, maintenance history, recycling status, etc. through a unified identification and information platform, providing regulators, enterprises and consumers with a transparent and traceable digital "product ID card".

2. Necessity of promoting "digital passport"

With the profound adjustment of the global trade pattern and the rise of the green transformation wave, the full life cycle management of electronic information products has become an international consensus[1]. As a data carrier that integrates supply chain transparency, compliance certification and circular economy elements, the Digital Product Passport (DPP) is receiving high attention from policy promotion and industrial pilot projects in major economies such as the European Union and the United States.

2.1 International perspective: regulation-driven and data governance

(1) EU Green New Deal and circular economy requirements. The Sustainable Product Ecodesign Regulation (ESPR) adopted in 2023 clearly stated that by 2030, heavy and light electronic and electrical products must be equipped with digital passports to enable online verification of product composition, carbon footprint, maintenance and recycling information, and promote the circular economy transformation of the European market. At the same time, the EU Battery Regulation stipulates that from 2027, all power batteries (including removable batteries used in smart terminals) must be accompanied by detailed digital passports, recording the entire chain data from raw materials to recycling, and providing technical support for ecological compliance and cross-border supervision.

(2) Global data governance and cross-border mutual recognition requirements. Digital passports advocate a "decentralized trust" mechanism based on distributed ledgers, which can be interconnected with regulatory systems in the EU, the United States and other places to form a multilateral mutual recognition framework and reduce repeated testing and audit costs. In future WTO or regional free trade agreements, digital passports are also expected to become part of the new "green trade" standard, helping

ISSN 2616-7433 Vol. 7, Issue 6: 1-6, DOI: 10.25236/FSST.2025.070601

Chinese manufacturers gain greater voice in international negotiations.

2.2 Industry practice perspective: management upgrade and business innovation

(1) Supply chain transparency and risk control. DPP standardizes the management of key data of products from raw material procurement, parts manufacturing, whole machine assembly to maintenance and recycling, enabling enterprises to monitor supply chain risks in real time and respond quickly to quality and safety incidents. In response to common mineral conflicts and environmental violations in the electronics industry, enterprises can use digital passport data to proactively disclose ESG (environmental, social and governance) information to enhance brand credibility and investor confidence.

(2) Extend product life cycle and circular business model. By recording maintenance history, material recyclability, disassembly guidance and other information, DPP provides a technical foundation for "product as a service" (PaaS) and "remanufacturing" business models, helping enterprises upgrade from "sell-out" to "lease + recycling" and tap secondary value. Practical cases show that early pilot smartphone and laptop manufacturers tracked battery health and parts replacement records through digital passports, increasing the average service life of equipment by 15%-20%, significantly reducing after-sales costs and the amount of electronic waste generated.

(3) Accelerate compliance certification and market access. The unified data format and open query interface enable enterprises to complete the preparation of multiple domestic and international compliance certification materials such as 3C, energy efficiency, and environmental protection at one time, reducing the cumbersome document docking and manual work. Many multinational e-commerce platforms have announced that they will give priority to recommending products with digital passports and connect to internal rating systems to facilitate consumers to quickly retrieve product sustainability indicators and increase the market premium of products with passports.

3. Core elements of the digital passport for electronic products

3.1 Unique identification and data link

Every electronic information product is given a globally unique digital identification (such as a QR code, RFID tag or NFC chip) when it leaves the factory. This identification is not only a static mark, but also a dynamic "ID card" with data throughout the product life cycle[2].

(1) Identification generation and implantation: In the manufacturing process, a globally unique serial number is generated through a security key and written into a physical carrier (QR code printing, RFID/NFC chip burning) to ensure that it can be consistently identified from the production line to the end user.

(2) Data collection and synchronization: Whenever a product goes through production, quality inspection, logistics, sales, maintenance, recycling and other links, on-site scanning or remote reading and writing can automatically trigger data synchronization with the cloud platform to record production batches, logistics tracks, sales channels, maintenance history, user reviews and other information.

(3) Real-time traceability and service: Users or regulatory entities can instantly call the cloud database by scanning the identification to obtain the complete information of the product, and realize value-added services such as authenticity verification, anti-counterfeiting management, intelligent warranty reminders, and recall warnings.

3.2 Standardized data model

To achieve cross-enterprise and cross-border collaborative circulation and back-end processing, the information fields stored in the digital passport must be uniformly defined and formatted[3].

3.2.1 Core field classification

(1) Material composition: device model, main raw materials (plastic, metal, semiconductor), environmentally friendly hazardous substance content (such as RoHS test results);

(2) Energy efficiency parameters: power consumption, standby power consumption, conversion efficiency, energy efficiency level certification (such as ENERGY STAR, EU energy efficiency label);

(3) Origin: manufacturing place, supplier name, production batch and date;

ISSN 2616-7433 Vol. 7, Issue 6: 1-6, DOI: 10.25236/FSST.2025.070601

(4) Compliance certification: safety certification (CE, FCC, CCC), industry standard compliance declaration;

(5) Maintenance records: after-sales service outlets, maintenance time, cause of failure, parts replacement record;

(6) Recycling destination: scrap date, disassembly site, recycling method, final disposal record.

3.2.2 Data format and interface

Use extensible markup languages such as JSON-LD and XML, and formulate field dictionaries based on international standards (such as GS1 and IEC 62402); provide multiple data interfaces such as RESTful API, OData, MQTT, etc., and be compatible with various ERP, MES, WMS, blockchain nodes and other systems to achieve "semantic intercommunication and pluggable interfaces".

3.3 Secure and reliable data infrastructure

In order to ensure that key information in digital passports will not be tampered with and can be safely shared among multiple parties (manufacturers, distributors, regulatory authorities, recycling companies, etc.), it is necessary to build a highly available, traceable, and permission-controllable data base.

(1) Distributed ledger and immutability: Based on blockchain (public chain/consortium chain) or distributed ledger technology, key pipeline operations (production, certification, logistics node chain, maintenance chain, recycling chain) are written into the chain ledger, and consensus mechanism and chain structure are used to prevent any single point tampering;

(2) Permission management and privacy protection: Through hierarchical access control (RBAC/ABAC), the minimum necessary permissions are assigned to different roles; sensitive business data (such as supplier prices, internal test reports) are encrypted for storage and transmission, combined with homomorphic encryption or zero-knowledge proof technology to achieve "verifiable buyers without leaking secrets" secure sharing;

(3) High availability and audit traceability: Multi-node deployment, data redundant backup and automatic fault switching to ensure 24-hour online; At the same time, the audit logs of all read and write operations are recorded, and once a security incident or compliance audit occurs, detailed off-chain and on-chain dual traceability reports can be provided.

4. International Typical Practices

Europe has piloted digital passports and promoted them in stages; built cross-departmental and cross-industry public service platforms; encouraged ecological partners to jointly maintain data quality, etc.

(1) EU "Digital Product Passport" pilot. The EU Circular Economy Action Plan proposes to implement digital passport requirements for key electronic and electrical equipment by 2026, and has carried out pilots in the fields of mobile phones and white goods, collecting product recyclability and environmental footprint data through a unified portal.

(2) German battery passport. For lithium batteries, Germany has required that all battery products be accompanied by digital passports from 2027 to record chemical composition, battery life, recycling information, etc., to provide data support for battery recycling and secondary use.

5. Three major challenges currently faced

5.1 Lack of technical standards and interoperability

Although the concept of digital passports is increasingly recognized, there are still obvious gaps in the technical standards, which directly affect the seamless collaboration and large-scale application between systems.

5.1.1 Standards have not yet been unified

Standard formulation is lagging: At present, there is no unified international standard for "digital passports for electronic information products" at home and abroad. The industry is mainly based on pilot specifications or self-developed solutions by enterprises, which lack authority and replicability.

ISSN 2616-7433 Vol. 7, Issue 6: 1-6, DOI: 10.25236/FSST.2025.070601

Risk of standard conflict: Different departments and regions may act in their own way. For example, the quality inspection department, environmental protection department and customs are independent of each other, and their standard requirements are different, resulting in the need to maintain multiple sets of data models for the same product, increasing duplication of work.

5.1.2 Fragmentation of data formats and interfaces

Difficulty in multi-platform collaboration: The interfaces of regulatory systems (such as customs, quality inspection), enterprise ERP/MES, third-party certification and maintenance platforms are different, the calling methods and data field names are not unified, and cross-system docking requires a lot of adaptation and development.

Chaotic version management: With the continuous iteration of business, the interface version is frequently updated, but there is a lack of a unified version release and decommissioning mechanism. The compatibility of the old system with the new interface is not guaranteed, and data loss or confusion is prone to occur.

5.1.3 Lack of interoperability testing

Lack of a unified testing framework: There is no IoT interoperability testing laboratory or certification agency, and it is impossible to perform integration testing and interconnection certification on digital passport platforms of different manufacturers.

Insufficient demonstration applications: The industry pilot cases are scattered, and there is a lack of comprehensive demonstration applications covering the entire process from production, circulation to recycling, and it is impossible to form a "reference implementation" for standardized reuse.

5.2 Data security and privacy protection

The digital passport of electronic products involves a large amount of corporate secrets and user privacy. While pursuing transparency and traceability, we must be cautious to prevent data leakage and abuse risks.

5.2.1 Balance of commercial sensitive information

Core process and formula: Data such as production process parameters, supplier list, cost structure, etc. are crucial to corporate competitiveness. If they are fully disclosed, they will weaken market advantages.

Hierarchical authorization management: It is necessary to introduce fine-grained permission control, and assign "visible field sets" and "writable field sets" to different roles (government supervision, brand owners, channel merchants, and users) to achieve "differentiated sharing and minimum exposure".

5.2.2 Platform and network security protection

Single point risk of centralized platform: If the digital passport platform adopts a centralized architecture, once it is attacked by DDoS, SQL injection or internal abuse, a large amount of product information on the entire network will be affected.

Dynamic security monitoring: In addition to conventional firewalls, intrusion detection systems (IDS/IPS), and WAF (Web application firewall), it is also necessary to introduce security behavior analysis (UEBA), vulnerability scanning, and red-blue confrontation drills to ensure timely detection and response to threats.

5.2.3 Data encryption in transmission and storage

End-to-end encryption: From product scanning devices, mobile apps, ERP systems to cloud databases, data links must be fully encrypted (TLS, VPN) to prevent man-in-the-middle attacks.

Static data encryption: Sensitive fields stored in databases and distributed ledgers are encrypted at the field level or table space level, and combined with key management services (KMS), to ensure that even if the storage medium is stolen, the data cannot be directly read.

5.3 Enterprise cost and operation model transformation

The construction of the digital passport system involves multiple investments in identification hardware, software platform, personnel training, etc., and small and medium-sized enterprises are

ISSN 2616-7433 Vol. 7, Issue 6: 1-6, DOI: 10.25236/FSST.2025.070601

particularly under great pressure; at the same time, the business value model behind it is still in the exploration stage.

5.3.1 High initial deployment costs

Hardware investment: Bulk purchase of QR code/RFID/NFC tags and labeling equipment updates require one-time capital expenditures; if you want to cover the entire production line, you also need to configure hardware such as barcode scanners and mobile terminals.

Software and operation and maintenance: Developing or subscribing to a cloud management platform, integrating internal systems such as ERP, MES, and WMS, and continuously performing functional iterations and security maintenance all constitute continuous operating costs.

5.3.2 Feasibility challenges for small and medium-sized enterprises

Technical thresholds and human resource training: Enterprises that lack a digital foundation need to train employees, reshape processes, and hire or outsource professional teams to increase labor costs.

Insufficient scale effect: For enterprises with small production capacity and few product categories, it is difficult to quickly balance investment and benefits, and the customer unit price is low and the payback cycle is long, resulting in low enthusiasm.

5.3.3 Exploration of business models and value-added services

Precise maintenance and extended warranty services: By connecting to the after-sales system, customized maintenance reminders, remote fault diagnosis and other value-added services are provided based on digital passport data; data analysis and operation teams need to be built.

Second-hand transactions and refurbishment incentives: In the second-hand market, digital passports can be used to verify authenticity and usage history to enhance trust; companies can cooperate with recyclers to establish a "trade-in" points or cash rebate mechanism.

Green recycling and traceability incentives: In combination with environmental protection and carbon neutrality policies, green points or tax incentives are issued to users or channels who actively participate in recycling and correctly return old machines; for companies, it is necessary to build a recycling data docking, logistics tracking and incentive redemption platform.

6. Suggestions on promotion paths

(1) Accelerating the construction of the standard system. It is necessary to formulate technical specifications for issuing digital passports for electronic information products, covering data models, identification rules, interface protocols, security requirements, etc. In addition, industry associations, standardization organizations and leading enterprises should be promoted to jointly create industry-level demonstration standards.

(2) Building a unified and reliable public service platform. It is necessary to build a digital passport platform to provide basic services such as identity registration, data link, inquiry and verification. The platform should adopt distributed architecture, blockchain bottom layer, multi-layer encryption and permission management mechanism to ensure security and high availability.

(3) Implementing phased pilots and step-by-step incentives. We should select key areas such as smart phones, laptops and wearable devices to carry out pilot projects to form replicable experiences. Financial subsidies or tax incentives should also be given to enterprises that are the first to deploy digital passports and meet data quality requirements.

(4) Promoting market-oriented applications and ecological construction. It is necessary to support e-commerce platforms, after-sales service providers and recycling enterprises to access the same passport system, and carry out accurate maintenance, remanufacturing and material recycling services based on passport data. Financial institutions should also be guided to provide innovative credit products such as Supply Chain Finance and Recovery Financing based on digital passport data for enterprises to reduce operating costs.

7. Conclusion

The digital passport of electronic information products is an important tool for improving product life

ISSN 2616-7433 Vol. 7, Issue 6: 1-6, DOI: 10.25236/FSST.2025.070601

cycle management, increasing resource recycling and enhancing industry competitiveness. We should learn from international advanced experience, improve standards and platform construction as soon as possible, cultivate a business ecosystem through phased pilots and policy incentives, give full play to the supporting role of digital passports in green manufacturing, compliance supervision and circular economy, and help the high-quality and sustainable development of the electronic information industry.

References

[1] Hulea M, Miron R, Muresan V. Digital Product Passport Implementation Based On Multi-Blockchain Approach With Decentralized Identifier Provider[J]. Applied Sciences, 2024, 14(11): 4874.
[2] Langley D J, Rosca E, Angelopoulos M, Et Al. Orchestrating A Smart Circular Economy: Guiding Principles For Digital Product Passports[J]. Journal of Business Research, 2023, 169: 114259.
[3] Voulgaridis K, Lagkas T, Angelopoulos C M, Et Al. Digital Product Passports As Enablers Of Digital Circular Economy: A Framework Based On Technological Perspective[J]. Telecommunication Systems, 2024, 85: 699-715.