

ENHANCING SUPPLY CHAIN SECURITY THROUGH PHYSICALLY UNCLONABLE AUTHENTICATION

SHAIMURAT AIBAR¹–PÉTER TAMÁS²

Abstract: Global supply chains are facing increasing challenges related to product counterfeiting, grey-market diversion, compliance with international sanctions, and the fulfilment of sustainability requirements. Conventional identification and tracking technologies, such as barcodes, RFID, and Real-Time Locating Systems (RTLS), effectively support logistics operations; however, they have limited capability to verify the authenticity of physical products and detect tampering. This paper presents the operating principles of NanoSign technology and investigates its potential applications across various logistics domains. The study compares NanoSign with currently applied tracking technologies and examines its applicability in sanction compliance, Digital Product Passports, ESG compliance, pharmaceutical logistics, and the authentication of high-value products. The comparative analysis suggests that NanoSign is not intended to replace existing tracking systems but to complement them with a physically unclonable authentication layer that can significantly enhance supply chain security and transparency. Finally, the paper discusses the current limitations of the technology and outlines potential directions for future research.

Keywords: supply chain security, unclonable authentication, NanoSign

1. INTRODUCTION

Although Radio Frequency Identification (RFID) and QR-based tracking are widely used, they still suffer from a major weakness: the gap between the physical object and its digital record. Most current systems protect the data, but not the item itself. A QR code can be copied without any difficulty, and an RFID tag can be cloned or even physically moved from one package to another. These vulnerabilities have reduced trust in conventional smart labels and highlighted the need for authentication methods that rely on the physical properties of the material itself, rather than on easily duplicated digital identifiers. In response to these systemic failures, SMark Technology Zrt. and NanoSign Holding Zrt. presented a solution that bridges the gap between nanoscale physics and digital traceability [1, 2]. According to the manufacturer, the NanoSign system is not merely a label, but a comprehensive verification ecosystem designed to establish an immutable link. The technology's efficiency lies in its three-component architecture, which ensures that security is embedded at every level of the product's journey:

- The NanoSign Marker
- Encrypted QR code
- Unique Serial Number (USN)

¹ MSc student, University of Miskolc, Institute of Logistics, Hungary
aibar.shaimurat@student.uni-miskolc.hu

² University prof., University of Miskolc, Institute of Logistics, Hungary
peter.tamas@uni-miskolc.hu

The NanoSign marker is a 0.9x0.9 mm nanoscale security marking. Unlike traditional optical tags, this marker consists of a stochastic (random) pattern of over 15,000 unique elements (pixels). This pattern functions as an Optical Physical Unclonable Function (PUF).

A defining characteristic of the NanoSign system is its dual-tier verification process. As it stated by the company, on the front line, a dedicated mobile application allows authorized personnel to track the geolocation and time-stamp of every scan, providing real-time visibility into the movement of high-risk goods [2]. Building upon the author's Scientific Student Conference (TDK) thesis defended at the University of Miskolc under the supervision of Prof. Dr. Tamás Péter [3], this paper investigates the implementation of the NanoSign system within high-security logistics. By analysing real-world applications, such as battery passports and sanction compliance, this work demonstrates that NanoSign represents a necessary evolution in protecting global trade integrity.

1.1. Research methodology and evaluation framework

This study conducts an exploratory qualitative comparative analysis to evaluate the integration potential of an emerging optical Physically Unclonable Function (PUF) technology (NanoSign) within modern supply chain security and tracking architectures. Because NanoSign represents an early-stage technology currently lacking independent peer-reviewed benchmarks, its technical capabilities are modelled using a hybrid baseline: theoretical performance boundaries established in foundational optical PUF literature combined with primary hardware specifications provided by the technology developer [1, 2].

To ensure objective evaluation alongside mature tracking technologies (Barcodes, Passive/Active RFID, BLE, and UWB), all technologies are evaluated through a unified supply chain identification and security framework based on peer-reviewed literature published over the past decade.

A primary methodological challenge in comparing these technologies lies in their distinct core operational objectives. The first one being tracking and localization technologies (RFID, BLE, UWB), designed for continuous spatial monitoring and real-time inventory flow. The second is our object – forensic authentication technologies (NanoSign, optical PUFs), designed primarily for physical anti-counterfeiting, tamper evidence, and deterministic physical identity verification.

Despite these functional divergences, both categories intersect at the critical operational mandate of supply chain integrity: verifying item identity, origin, and state. Therefore, the comparative matrix evaluates all technologies across five core, quantifiable dimensions:

- Data capacity
- Read Range
- RF/EM Immunity: signal resilience against electromagnetic interference, metallic reflection, and fluid absorption
- Physical Cloning Risk
- Unit Cost

Rather than asserting empirical equivalence, this methodology uses first-principles physical analysis to map NanoSign's theoretical capabilities onto specific supply chain use cases.

2. DETAILED DESCRIPTION OF THE CHARACTERISTICS OF THE OPTICAL PUF TECHNOLOGY

2.1. Description of the optical PUF and its operation

The structural and functional superiority of nanomaterials is derived from their unique physicochemical properties, which emerge specifically at the nanoscale [4]. As particles decrease in size, a much higher percentage of their atoms reside on the surface, leading to heightened chemical reactivity and unique surface plasmon resonance – a phenomenon essential for developing high-sensitivity optical sensors. Furthermore, the transition from bulk materials to the nanoscale triggers quantum confinement effects, where the electronic and optical properties of a substance become dependent on its physical dimensions rather than its chemical composition alone.

In the specialized field of anti-counterfeiting, these characteristics provide a versatile and robust platform for security. Quantum dots (QDs), for instance, utilize size-dependent emission to provide precise colour tunability and exceptional photostability. Unlike traditional dyes, QDs do not fade easily and can be engineered to emit specific wavelengths under targeted excitation. This level of control allows for the creation of sophisticated PUFs. By leveraging stimuli-responsive mechanisms, these nanomaterials can be integrated into electrophoretic displays or hidden markers that are virtually hard to replicate using conventional manufacturing, as their optical signature is tied to the precise, stochastic arrangement of individual nanoparticles [4].

To understand NanoSign, one must first understand how modern science views the manufacturing process. In any technological process, whether creating microchips or printing labels, there are always microscopic, uncontrollable deviations. In microelectronics, these are referred to as “process variations” [5].

The structural integrity of the NanoSign system is predicated on the transition from deterministic engineering to entropy-driven stochastic distribution [4]. By utilizing high-precision nanotechnology fabrication techniques, each individual label is endowed with a unique physical architecture that is not designed in the traditional sense but rather emerges through controlled chaotic processes at the molecular level. On a footprint of only 0.9 x 0.9 mm, the system integrates over 15,000 discrete nanoscale elements [1]. This high degree of information density creates an Optical PUF, where the specific spatial arrangement of the nanoparticles serves as a biological-style unique fingerprint. Because these patterns are the result of stochastic variance during production, they reside beyond the reach of exact replication, even the original manufacturer, using the same equipment and parameters, face major challenges to recreate an identical atomic configuration once the initial marker has been set (Fig. 1).



Figure 1. NanoSign label [1]

Furthermore, the security of the NanoSign marker is reinforced by its mechanical relationship with its substrate. According to the developer, the use of specialized destructive security paper ensures that the nanostructure is not merely sitting on the surface but is strongly bonded to the material's fibres. From a material science perspective, this creates a bond where any attempt to physically relocate or remove the label induces structural failure [6]. The scale of the identifier effectively removes the human element from the threat model; the dimensions are so small that manual intervention is physically hard. Any attempt to compromise the system requires high-resolution nanolithography and multi-million dollar imaging inventory [6].

2.2 Description of the main feature of the optical PUF

Having learned that the marker is unique, a sceptic might ask a reasonable question: "Alright, it is unique. But if I have an ultra-powerful microscope, can I study its structure and simply recreate an exact copy?". This is exactly where the PUF concept reveals its greatest strength – the power of chaos. As noted earlier, PUFs are based on fundamental randomness [4]. The difference between "knowing what it looks like" and "being able to make it" becomes an insurmountable chasm at the nanoscale.

The high resistance against physical and digital cloning of NanoSign markers relies on the physical properties of Optical PUFs [4]. Due to the stochastic nature of the nanostructure fabrication process, the spatial distribution of the nanoparticles (15,000 pixels within a 0.9×0.9 mm area) is practically constrained from being deterministically controlled or reproduced, even by utilizing deterministic high-precision manufacturing or advanced microscopy [5].

If the structure of the marker cannot be read like a standard barcode, then how can a customs inspector, a logistics manager, or an end consumer verify the authenticity of the product? The principles of this mechanism has described in Majzoobi's scientific paper as the Challenge-Response architecture [5]. The process can be described in 3 phases (Fig. 2).

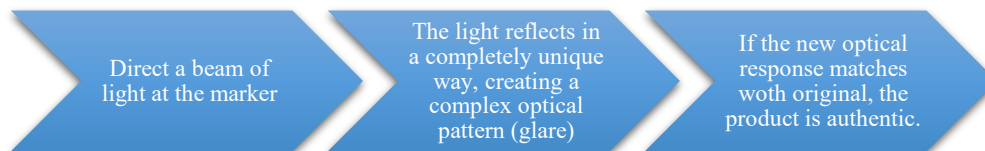


Figure 2. The Challenge-Response process of identifying

Majzoobi's article places significant emphasis on the fact that secure systems must be protected against physical tampering at the hardware level [5]. NanoSign solves this problem by turning the marker itself into a fragile ecosystem. According to the manufacturer, the NanoSign marker is not applied to standard glossy sticker paper, but to specialized destructive security paper, to prevent physical transfer attacks [1, 2]. Theoretically, any mechanical stress (e.g., peeling attempt) or chemical exposition disrupts the structural integrity of the substrate, altering the relative sub-micron alignment of the constituent pixels. During the Challenge-Response verification, even a fractional spatial shift distorts the response signal, resulting in an immediate authentication failure [5]. The application will

immediately flag the physical tampering. Thus, the NanoSign marker becomes an inseparable physical component of its packaging, one that can only perish along with the packaging itself.

3. EXPLORATION AND COMPARISON OF TRACKING SYSTEMS

Serving as the foundational catalyst in the evolution of tracking systems, barcodes remain the predominant mechanism for encoding machine-readable data across commercial goods and services. This technological democratization has placed data-extraction capabilities directly into the hands of billions of users globally. Today, almost every packaged commodity is tagged with at least one barcode, predominantly adhering to standard formats such as European Article Number (EAN) or Universal Product Code (UPC) [7].

Within the framework of modern supply chain management, methodologies for monitoring assets and inventory are fundamentally categorized into two distinct objects: discrete and continuous tracking [8]. The selection of a specific approach defines the level of operational transparency and determines the technological infrastructure required for implementation.

Discrete tracking is characterized as an event-driven monitoring model [8]. In this configuration, an object is identified exclusively as it reaches specific nodes or checkpoints within the logistics network. This method functions as a periodic observation process. The observer gains visibility into the status and location of goods only at certain intervals, leaving the state of the shipment unknown during the transitions between reading points. Despite these data gaps, discrete tracking remains the prevailing standard in global logistics due to its scalability and cost-efficiency [8].

Continuous tracking is designed to provide real-time visibility across the entire supply chain. This methodology allows for the instantaneous localization of shipments and the monitoring of environmental variables at any given moment. Continuous tracking is indispensable for high-value or highly sensitive cargo, where any deviation from the planned route or condition requires immediate intervention.

RFID represents a sophisticated branch of Automatic Identification and Data Capture (AIDC) technology [9]. It utilizes electromagnetic fields to identify and monitor objects without requiring physical contact or a direct line of sight. The technical efficiency of an RFID system depends on the seamless interaction between three core elements: the RFID tag (transponder), the RFID reader (interrogator), and the backend middleware or software.

Security and privacy issues are one of the most important concerns and constraints. Modern counterfeiters now possess the equipment necessary to replicate visual markers with alarming precision. Most traditional methods are “overt”, meaning they are visible and easily scannable, making them easy targets for duplication.

Table I demonstrates that unprotected tags are vulnerable to eavesdropping, spoofing and cloning. Attacks can happen at any point: either in transmission, or while providing service, or at software/middleware level (delivery of virus to compromise middleware and backend systems) [8].

The transition to Real-Time Locating System (RTLS) represents a move toward a “persistent data stream”. Unlike passive RFID, which requires a tag to pass within a short range of a reader to be energized and identified, RTLS provides continuous, instant location information. Throughout the 2000s and 2010s, RTLS technology evolved from expensive, hard-wired infrastructure to flexible, multi-modal systems [10].

Table I.
RFID attacks [7]

System level	Threat type	Description
Physical level	Tag destruction	Permanently disabling a tag by removing it, destroying it, or using unauthorized “kill” commands.
	Signal blocking	Using shielding (like metal foil) or electronic jamming to hide the tag from the reader.
Communication level	Eavesdropping	Unauthorized devices “listening” to the radio signals between a tag and a reader to steal data.
	Relay attacks	Intercepting a signal and sending it to a different location to trick the system into verifying a far-away tag.
Application level	Cloning	Creating an exact electronic copy of a legitimate tag to simulate its identity.
	Spoofing	Impersonating a real tag to gain access or privileges without creating a physical copy.
System level	Data corruption	Introducing fake tags into the system to cause software errors or crash the reader's database.
	Privacy risks	Unauthorized tracking of items/people, leading to industrial espionage or loss of privacy.

Despite the rapid development of RTLS and its growing adoption in logistics, manufacturing, and industrial automation, these technologies still face several structural limitations. One of the most significant challenges is the high cost of ownership, which includes both capital expenditures (CAPEX) and operational expenditures (OPEX). The initial investment required for RTLS infrastructure (anchors, servers, network cabling, and installation) can be substantial, especially in large facilities [11]. Other critical concerns include the complexity of system maintenance and cybersecurity, which create a continuous operational burden and the risk of coordinate falsification or facilitating theft by misleading location data.

To address these limitations, a comparative evaluation of conventional tracking and authentication mechanisms is required. Tables below summarize the structural, operational, and security parameters across primary identification frameworks (Barcodes, Passive/Active RFID, UWB, BLE) in comparison with optical PUF technology (NanoSign). While tracking technologies differ fundamentally in their underlying physics and data structures, comparing them provides a strategic baseline to evaluate how emerging optical physically unclonable function (PUF) markers, such as NanoSign, integrate into modern supply chain security. To ensure scientific rigor and eliminate subjectivity, qualitative metrics were assigned based on standardized physical parameters and literature-based performance bounds. Each technology is evaluated against quantifiable operational thresholds defined before analysis.

Data capacity for tracking technologies was categorized into discrete tiers – Low (<4 KB), Moderate (4KB–100 KB or equivalent hybrid payloads), and High (> 100 KB) – based on accessible payload sizes documented in industry standards and academic literature. While conventional electronic and optical tags rely solely on digital memory bits, NanoSign require a dual-layer capacity assessment. Although there are no precise figures available, the structure of NanoSign, comprising a QR code, an USN and the label itself, suggests that the marker can store up to several KB of information, which is the reason it is classified Moderate (Table II).

Table II.
Comparative analysis of tracking technologies in logistics

Tracking technology	Operational mechanism	Data capacity	Read range	Key advantage	Main technical limitations	Source
Barcode (1D/2D, QR)	Optical scanning of parallel lines or stochastic patterns representing digital data	Low (8 bits to 4 KB)	Centimetres to few meters	Inexpensive; universal standards; easy implementation via smartphones	Requires line-of-sight; orientation dependent; scans one item at a time; easily damaged	[7, 12]
RFID (Passive, Active)	Radio wave propagation (far-field) for data transfer	Moderate (up to 72 KB)	Centimetres to 15 meters	Bulk scanning without line-of-sight; automated verification; durable/rugged labels	Signal attenuation in metallic environments; high initial infrastructure cost	[8, 13]
UWB	Time of Flight measurement using short-duration, broad spectrum radio pulses	High data rates over short ranges (up to 850 KB)	Up to 200 meters	Highest precision; minimal interference; deterministic data	Highest infrastructure cost; requires dense anchor deployment and synchronization	[10, 11, 14, 15, 16]
BLE	Signal strength or Angle of Arrival using radio beacons	Moderate (up to 100 KB)	Up to 100 meters	Energy efficient; compatible with smart devices; low-cost beacons	Probabilistic accuracy (1–5m); requires battery power for tags; range affected by obstacles	[10, 11, 15, 16]
NanoSign (According to the developer)	Optical Physical Unclonable Function utilizing nano-level stochastic elements	Moderate (combined marker)	Proximity/contact	Physically improbable to reproduce; low cost; forensic authentication; tamper-evident; physically hard to replicate	Requires specific reader app or specialized sensing; manual/individual verification	[1, 2]

As the comparison table shows, the examined tracking and labelling technologies share several common strengths and limitations, even though their underlying mechanisms differ significantly. For example, both RFID and BLE offer a moderate information capacity within individual tags or labels. In this context, “moderate” indicates that the amount of data they

can store is fully sufficient for typical warehouse operations and supply-chain workflows. These two technologies are also united by their low cost, which makes them accessible for large-scale deployments. As a result, RFID and BLE remain the most widely adopted solutions for everyday tracking and labelling tasks in logistics. However, when operations require high-precision localization, mainstream technologies become insufficient. In such cases, UWB stands out as the preferred option.

Within this comparison, NanoSign occupies a unique position. It combines several advantages typically found across different technologies while avoiding many of their weaknesses.

This comparison positions NanoSign as a promising candidate for future logistics applications, particularly in areas where both traceability and protection against counterfeiting are essential. By bridging the gap between digital tracking and physical authentication, according to the developer, NanoSign offers a hybrid approach that could significantly strengthen the next generation of labelling and tracking systems.

The qualitative ratings for interference susceptibility (RF/electromagnetic immunity and physical line-of-sight sensitivity) in Table III evaluate how resilient each technology signal is when encountering physical barriers (line-of-sight blockage), metallic surfaces, liquids, and electromagnetic (EM) noise common in industrial logistics environments.

- High: Technology fails or experiences severe signal attenuation when subjected to direct line-of-sight blockage, metallic reflection, or liquid absorption;
- Moderate: Technology experiences moderate packet loss or range reduction under non-line-of-sight or multi-path interference conditions, but relies on frequency hopping or anti-collision protocols to maintain connectivity;
- Low / Very Low: Technology exhibits high immunity to environmental attenuation and narrow-band noise due to high penetration capabilities, ultra-wide spectral spreading, or localized optical verification.

For barcodes, optical signals cannot penetrate dirt or dust. Damaged, smudged, or occluded tags result in a very high read failure rate [7, 12]. Ultra-high frequency RFID (860–960 MHz) is notoriously susceptible to the liquids (which absorb RF energy) and metallic surfaces (which reflect signals, cause detuning of the tag antenna, and create multipath destructive interference) [13]. BLE operates in the crowded 2.4 GHz band alongside Wi-Fi and Zigbee. While it suffers from attenuation through human bodies and metal walls, it mitigates interference [16]. And for UWB, its massive bandwidth gives it exceptional immunity to multi-path fading and narrow-band interference. According to the developer, NanoSign’s design and the tag’s specific features, it is immune to RF or metal interference, as it operates within the spectral range. But it does require optical contact with the reader to read the nanostructure, similar to a barcode (Table III).

The physical cloning risk assesses the susceptibility of a tracking marker or tag to visual duplication, electronic payload extraction, or physical spoofing without specialized cryptographic keys or hardware protection. Barcodes store deterministic, plain-text data visually [7]. Anyone with a high-resolution camera or scanner can capture, replicate, and print identical duplicates in seconds. Standard RFID tags transmit static identifiers over unencrypted radio channels [8]. Attackers can easily read the EPC memory using handheld readers and clone it onto inexpensive programmable tags or software emulators [8]. BLE and UWB have the same moderate rating (Table III) since both tags can be physically duplicated,

but only if an attacker gains access to the credential or device firmware [15]. And the very low rating for a NanoSign has been explained earlier in the paper.

Unit cost represents the marginal cost of producing and deploying a single physical tag or marker (excluding infrastructure and reader equipment):

- Very Low (<\$0.01-\$0.05): Paper, film, or ink-based passive tags manufactured via scalable printing processes (e.g., standard 1D/2D barcodes).
- Low (\$0.05-\$0.50): Silicon-based passive tags requiring micro-antennas (e.g., standard passive UHF RFID labels).
- Moderate (\$1.00-\$10.00): Battery-assisted passive, active radio tags, or complex transceiver nodes requiring onboard memory and power sources (e.g., active RFID, BLE beacons [11]).
- High (>\$10.00): High-precision RF transceivers, impulse-radio nodes, or localized real-time location hardware (e.g., UWB tags [16]).

Since the price of each tag varies by manufacturer or depends on the complexity of the tag itself, average figures from publicly available sources were used to estimate the price per unit. NanoSign is categorized as Low to moderate. Although it utilizes advanced optical physical unclonable functions (PUFs), its fabrication relies on the stochastic self-assembly of nanoparticles deposited onto tamper-evident paper substrates rather than silicon microchip manufacturing [1, 2]. Because the microscopic security pattern is intrinsically generated during chemical deposition rather than digitally programmed, the per-unit production cost scales similarly to specialized printed security labels rather than electronic tags (Table III).

Table III.
Extended analysis of tracking technologies in logistics

Tracking technology	RF/EM immunity	Physical line-of-sight sensitivity	Physical cloning risk	Unit cost	Logistics applications	Source
Barcode (1D/2D, QR)	Non-RF	High	High	Very low	Retail checkouts; warehouse inventory recording; package labelling.	[7, 12]
RFID (Passive, Active)	High susceptibility	Low	High	Low to moderate	Warehouse inventory; pallet-level tracking; apparel supply chain; automated dock doors	[8, 13]
UWB	Low	Low	Moderate	High	Forklift safety; crane positioning; high-precision asset tracking; station-level assembly	[10, 11, 14, 15, 16]
BLE	Moderate	Moderate	Moderate	Low to moderate	IoT sensors for condition tracking (temperature, speed); pallet and yard tracking; asset search	[10, 11, 15, 16]
NanoSign	Very Low	High	Very low	Low to moderate	High-risk cargo; pharmaceuticals; sanctioned goods; Battery Passports; luxury goods	[1, 2]

The extended comparison table highlights a defining characteristic of the NanoSign system: it is the only technology among contemporary tracking and labelling solutions that simultaneously demonstrates very low susceptibility to tampering and low unit cost. This combination is exceptionally rare in the logistics sector, where systems typically achieve one of these advantages at the expense of the other.

NanoSign's position in the comparison therefore appears not only distinctive but also strategically significant. For companies that prioritize both security and cost-efficiency, NanoSign offers a unique value proposition. Its microstructure provides a level of tamper resistance that conventional digital identifiers cannot match, while its production and deployment costs remain comparable to those of mainstream labelling technologies.

It's important to note that Nanosign doesn't aim to compete with existing tracking systems, but rather serves as a powerful complement. It can also function as a standalone system. For example, RFID could be responsible for warehouse automation, while Nanosign provides legal authentication and counterfeit protection at customs or at the customer's premises.

Having examined its technical characteristics, cost profile, and security properties, we can now outline the practical implications of these findings. With a solid understanding of NanoSign's strengths and operational potential, the next chapter will focus on exploring concrete application areas within the logistics sector.

4. EXPLORATION OF NANOSIGN'S FIELDS OF APPLICATION

In the context of fast-moving consumer goods (FMCG) or low-value commodities, traditional identification methods such as standard QR codes or passive RFID remain the most cost-effective solutions [17]. For these categories, the primary logistical objective is volume throughput and basic inventory management, rather than strict anti-counterfeiting. The findings presented by Balkema (2023) provide direct empirical support for this argument. In his study on the adoption barriers of tracking technologies in the food industry, he demonstrates that the primary difficulties arise precisely in product categories with very low profit margins. Even a minimal increase in unit cost [17].

Table IV.
Technological applicability matrix based on Asset Risk and Monitoring Demands

Asset value/risk	Low monitoring requirements	High monitoring requirements
High	Anti-counterfeit focus - Target goods: luxury items, high-end apparel, fashion. - Deployment logic: discrete tracking is sufficient. NanoSign serves as a solution against digital cloning.	Critical asset protection - Target goods: aerospace components (AOG), pharmaceuticals, critical legal documents. - Deployment logic: high liability risks justify NanoSign integration to prevent catastrophic counterfeit consequences.
Low	Commodity retail - Target goods: fast-moving consumer goods (FMCG), groceries. - Deployment logic: low-margin constraints make NanoSign economically unviable; barcodes or passive RFID remain optimal.	Bulk logistics - Target goods: construction materials, raw commodities, heavy industrial supplies. - Deployment logic: emphasis is on mass movement/volume tracking; standard barcode or RFID solutions are sufficient.

Balkema's analysis is particularly relevant because it focuses on RFID, a technology that is widely considered inexpensive and mature. Despite the low cost of individual RFID tags, the author emphasizes that the total cost of ownership remains substantial. Beyond the tag itself, companies must invest in readers, antennas, integration software, and ongoing maintenance of the infrastructure [17]. These findings are directly applicable to NanoSign as well. Although NanoSign markers are inexpensive to produce, the system still requires specialized scanning equipment, secure data storage, and periodic verification processes. As Balkema notes, even small additional costs can become prohibitive when applied to millions of low-value items moving through the supply chain (Table IV).

This leads to an important conclusion that NanoSign is not designed for mass-market consumer goods, and its deployment in such contexts would not be economically justified.

4.1. Regulatory compliance and sanctioned goods tracking

One of the most critical challenges facing international logistics is ensuring compliance with international trade restrictions and embargoes. Standard tracking systems often fail to provide sufficient visibility, making it frequently improbable to identify the product securely during high-risk export operations or to verify its true end destination.

A recent and highly relevant example illustrating the consequences of insufficient end-user verification is the 2026 sanctions-enforcement case in Latvia. According to official reporting, the Latvian Prosecutor's Office secured an 11-year prison sentence against an Azerbaijani national for exporting dozens of Starlink Mini Kits and other dual-use items, including weapons components and ballistic measurement devices, to the Russian military in violation of EU sanctions. The total value of the exported goods was estimated at approximately €200,000. The case is notable not only for the severity of the penalty but also for the underlying mechanism of the violation: the goods were diverted through intermediaries and re-exported to a prohibited end-user, demonstrating a complete breakdown in end-user verification and supply-chain transparency [18].

This case underscores the structural weaknesses that persist in many international supply chains. Even when exporters comply with documentation requirements, the absence of reliable, tamper-proof tracking mechanisms allows sanctioned goods to be redirected to unauthorized recipients. The Latvian prosecution highlights how traditional documentation and digital identifiers fail to prevent route manipulation, identity masking, and post-export diversion – all of which are central challenges in embargo enforcement.

A system such as NanoSign, which links each physical item to a non-copiable marker and records geolocated scan events, directly addresses the vulnerabilities exposed in this case [1, 2]. If such a system had been in place, any deviation from the declared route or any attempt to transfer the goods to unauthorized intermediaries would have triggered an immediate alert, creating an evidentiary trail for customs and enforcement authorities.

Crucially, this system automates compliance verification. The location of the scan must correspond with the origin of the GPS signal and the recipient or delivery address stated on the official product documents. In instances where there is a geographic discrepancy between these signals that exceeds a predefined threshold, the system flags the shipment, indicating that a more thorough follow-up check is necessary for the sanctioned products. By integrating NanoSign, the system not only assists customs authorities upon check-ups but also empowers law-abiding traders, exporters, and freighters to guarantee they meet sanction standards and can objectively prove their good faith [2].

4.2. ESG communication and Digital Product Passports

As environmental sustainability transitions from a corporate social responsibility (CSR) initiative to a strict regulatory requirement, supply chain transparency has become the cornerstone of ESG (Environmental, social, and governance) compliance. Regulatory bodies worldwide are implementing stringent frameworks to combat so-called “greenwashing” – the deceptive practice of marketing products as environmentally friendly without verifiable evidence.

The Volkswagen emissions scandal (widely known as Dieselgate) remains the most significant case of corporate environmental deception ever recorded. The scandal became public in September 2015, when the U.S. Environmental Protection Agency (EPA) and the California Air Resources Board (CARB) announced that Volkswagen had intentionally installed “defeat devices” in its diesel vehicles. These software systems were designed to detect when a car was undergoing laboratory emissions testing and temporarily reduce nitrogen oxide (NOx) emissions to legal levels. During normal driving, however, the vehicles emitted up to 40 times the permitted NOx limits [19].

The scandal also caused severe reputational damage for the company. This loss of confidence extended beyond Volkswagen’s customer base and triggered broader doubts about other companies promoting their “green innovations” and reduced-emission technologies. The Volkswagen case demonstrates that compliance with sustainability standards is not merely a formal reporting exercise but a critical factor with significant financial and reputational consequences when violated. As shown in the chart presented by Barth et al. (2022), investor trust collapsed to unprecedented levels, resulting in some of the largest shareholder losses recorded in the sector [19].

The severe financial and reputational consequences of data manipulation are best illustrated by the Volkswagen “Dieselgate scandal”, which resulted in over \$35 billion in fines. By implementing NanoSign as a physical “trust anchor”, manufacturers can provide forensic-level proof of compliance, making the falsification of environmental data (whether in emissions or battery lifecycles) highly arduous.

Central to this new regulatory landscape is the European Union’s initiative to mandate Digital Product Passports (DPPs), particularly within the rapidly expanding Electric Vehicle (EV) battery sector. The core objective of a battery passport is to trace the lifecycle of the asset – from the ethical extraction of raw materials (such as lithium and cobalt) to its manufacturing, deployment, and eventual recycling. As reported in European Union Journal, “Battery Passports will become mandatory in the European Union from 18 February 2027 under the EU Battery Regulation (EU) 2023/1542. From that point, manufacturers placing EV and in-scope industrial batteries on the EU market must be able to provide ongoing, verifiable lifecycle data – not just one-off reports [20].

However, a critical vulnerability exists within the DPP framework is the “Digital-to-Physical Gap”. If the digital passport is highly secure (e.g., blockchain-based) but the physical label connecting the asset to the ledger can be easily removed, copied, or attached to a counterfeit or unethically sourced battery, the entire system’s integrity collapses.

NanoSign addresses this structural flaw by acting as an irreproducible cryptographic anchor for ESG claims. By applying a physically unique NanoSign marker to the battery casing or high-value components, manufacturers ensure an immutable link between the physical object and its digital twin [1, 2]. Because the NanoSign system provides authentically verifiable tracking of the product’s journey, it serves as a robust mechanism to

support transparent corporate operations and align with regulatory guidelines, such as those established by the Hungarian Competition Authority (GVH). Consequently, stakeholders across the circular economy can verify not only the location of the battery but its absolute provenance, ensuring that environmental claims are backed by objective, real-time data.

4.3. Pharmaceuticals and high-risk chemicals

While the financial implications of supply chain fraud are immense, the infiltration of counterfeit goods into highly regulated sectors such as pharmaceuticals, biotechnology, and chemical logistics poses a direct threat to public safety.

According to data from the World Health Organization (WHO), the illicit trade in pharmaceuticals is estimated to be valued between \$200 billion and \$431 billion annually. With approximately 10% of medications globally identified as counterfeit, this issue affects a vast range of therapeutic categories, ranging from substandard generics to fraudulent brand-name drugs [21].

Beyond the immediate risk to patient safety, these products impose severe direct economic costs. Legitimate manufacturers suffer significant revenue losses, which directly impedes their ability to fund essential research and development for future medical innovations. Furthermore, the National Association of Boards of Pharmacy (NABP) indicates that counterfeit drugs contribute to an annual global loss of approximately \$75 billion [21]. Figure 3 encompasses increased healthcare expenditures arising from treatment failures and prolonged illnesses, as well as the heavy administrative burden placed on regulatory and enforcement agencies tasked with monitoring these illicit activities.

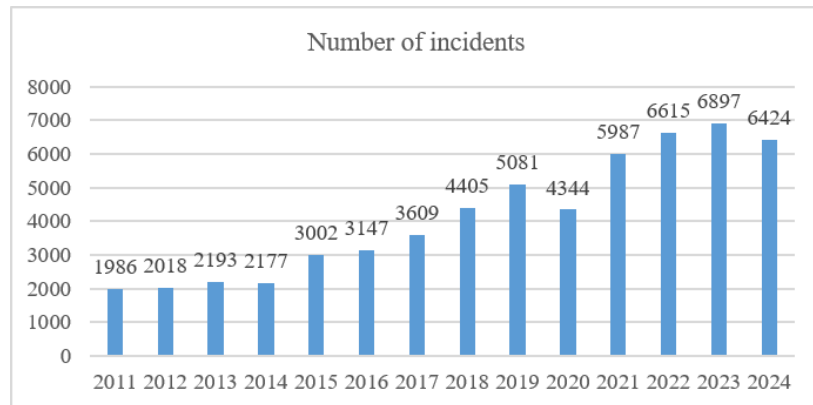


Figure 3. Total number of counterfeit incidents concerning pharmaceuticals worldwide [22]

Data from the Pharmaceutical Security Institute (PSI) shows that counterfeit medicines continue to increase worldwide. In 2024, the organization recorded almost 6,500 pharmaceutical crime incidents, representing a 6.9% percent decrease compared to the previous year, but as histogram shows, the amount of counterfeit incidents is high [22].

Standard RTLS and standard electronic RFID tags, while efficient for warehouse management, are inherently vulnerable to content substitution. An attacker can carefully remove a legitimate tracking tag from an authentic vial or container and affix it to a counterfeit product, thereby tricking the logistical system into verifying a dangerous fake.

In these mission-critical applications, NanoSign provides a forensic-level defence mechanism through its physical construction [1, 2]. If an unauthorized party attempts to open a pharmaceutical package or a chemical container to adulterate the contents, the NanoSign marker is destroyed. Any subsequent attempt to scan the label using the designated application will fail to authenticate the nanoscale pattern, instantly alerting the supply chain network to the tampering event. This application demonstrates that in highly regulated industries, traceability must be inherently coupled with physical integrity – a requirement that legacy tracking systems are fundamentally unequipped to fulfil.

4.4. Brand protection for high-value assets and consumer trust

Beyond regulatory compliance, the economic stability of premium brands relies heavily on the perceived authenticity of their products. Counterfeiting is no longer limited to luxury fashion, it has expanded into industrial components, automotive parts, and high-tech equipment, where non-original parts can lead to catastrophic mechanical failures.

The critical importance of physical-to-digital integrity is most starkly illustrated by the AOG Technics scandal in 2023, which sent shockwaves through the global aviation industry. The London-based distributor allegedly supplied thousands of engine components for CFM56 turbines (powering the majority of the world's Boeing 737 and Airbus A320 fleets) using falsified regulatory release certificates [23]. As Luke Peters reported to Aerospace Global News, “The fraud involved more than 60,000 parts, generating roughly \$10 million in revenue, with over 90% of it linked to fraudulent activity. Airlines faced an estimated \$53 million in costs for inspections, engine teardowns, and grounding.”

This case highlights a fundamental verification gap, while the digital and paper-based documentation appeared legitimate, there was no way to verify the physical authenticity of the parts themselves upon arrival. If these high-value components had been equipped with a PUF like NanoSign, the forgery would have been detected immediately at the first point of inspection.

While the aviation and pharmaceutical sectors represent life-threatening risks, the fashion and apparel industry remains the largest battlefield for intellectual property infringement. The annual global trade in counterfeit fashion goods (clothing, shoes, bags, watches) is estimated at more than \$450 billion [24]. Within the EU, recent data shows a significant escalation in counterfeit activity. According to a report published in November 2024, 2023 marked a record year for seizures of counterfeit goods. EU law-enforcement agencies confiscated 152 million items, representing a 77% increase compared to the previous year. The estimated market value of these goods exceeded €3.4 billion, which is 68% higher than in 2022 [25]. Clothing and branded consumer products remain among the top three most frequently seized categories, reflecting both their high demand and the scale of illicit production.

At first glance, it may appear that only large global brands suffer from counterfeiting. However, the broader economic impact is far more substantial. According to the EU Intellectual Property Office (EUIPO), the legal EU industry loses approximately €12 billion in revenue every year due to counterfeit goods. These losses translate directly into reduced employment: in 2021 alone, EUIPO estimated that 160,000 jobs were eliminated as a result of counterfeit activity [26].

While NanoSign cannot realistically solve the problem of counterfeit clothing, given the mass-market nature of the sector and the complexity of its supply chains, it can still offer value to major brands facing counterfeiting not only of their products but also of their

verification codes and authenticity labels. By integrating NanoSign markers into high-value or limited-edition product lines, brands could significantly strengthen consumer trust. Each NanoSign scan is securely recorded, meaning that a product could be verified as authentic if the only registered scan prior to reaching the customer occurred at the manufacturing facility. This creates a level of tamper-proof, physically anchored authentication that conventional digital labels cannot provide.

Table V synthesizes the primary application areas explored in this research, illustrating how NanoSign addresses the structural vulnerabilities of current tracking standards.

Table V.
Strategic Synthesis of Applications

Application area	Core vulnerability	NanoSign strategic advantage	Possible impact
Sanctioned goods	High risk of spoofing GPS data or cloning electronic IDs.	GPS-linked scans with irreproducible physical markers.	Avoidance of multi-million dollar fines.
EV battery tracking	Digital records can be detached from the physical battery.	Immutable trust anchor for the DPP.	Prevention of Greenwashing cases and penalties.
Pharmaceuticals	Tags can be moved from authentic to fake vials.	Tamper-evident destructive labels; immediate alert on breach.	Elimination of counterfeit health risks.
High-value assets	Reliance on easily forged digital or paper certificates.	Forensic verification: instant object-level authentication.	Prevention of catastrophic failures and recalls.
Consumer brands	Gray-market entry and high-quality fakes.	Direct consumer verification via smartphone.	Increased trust and data-driven marketing.

As demonstrated in the table above, NanoSign does not merely supplement existing tracking technologies, it provides a forensic layer that is fundamentally absent in these systems. While RFID and UWB excel at answering the question of “Where?”, NanoSign provides the answer to “Is this asset genuine and untampered?”.

5. LIMITATIONS AND SCIENTIFIC OBJECTIVITY

To maintain scientific objectivity, it is necessary to explicitly outline the methodological boundaries of this study. Because NanoSign is an emerging optical PUF technology currently in its developmental stage, this comparative evaluation is fundamentally qualitative and exploratory. The assessment relies on a synthesis of foundational optical PUF physics, theoretical state-of-the-art bounds, and manufacturer specifications rather than a comprehensive empirical field dataset. A complete quantitative and statistical validation of NanoSign within real-world logistics environments requires further empirical testing across several critical operational performance metrics:

- Cryptographic PUF security metrics: future studies must evaluate the statistical randomness and stability of the optical marker using normalized distance measurements, measuring the variation between distinct markers to guarantee that no two generated optical responses are statistically identical and evaluating the

repeatability of reading the same marker under fluctuating operational environments, including variable ambient lighting, camera angles, reader noise, and surface wear

- Biometric and verification accuracy: comprehensive evaluations require benchmarking explicit statistical error rates, specifically the false acceptance rate (FAR) and false rejection rate (FRR), to define the receiver operating characteristic (ROC) curve of the optical reader algorithms.
- Environmental reliability: practical logistics integration necessitates measuring the physical durability of the destructive paper substrate, successful scan rates under adverse condition (e.g., dust, moisture, surface abrasion), scan latency, and spatial resolution bounds of the reader hardware.

By explicitly delineating these operational metrics, this study does not claim definitive performance for NanoSign. Instead, it provides a structured, literature-backed theoretical baseline to guide future testing, field trials, and standardized benchmarking of hybrid optical-PUF technologies in supply chain security.

6. CONCLUSION

Logistics tracking has undergone a significant transformation, evolving from basic identification methods to sophisticated systems designed to provide increasingly robust protection against loss, counterfeiting, and operational delays. Today, counterfeiting is a global epidemic, where the sophistication of fake goods has reached a point where they are virtually indistinguishable from original products.

In this context, where traditional security measures often fail to provide absolute certainty, NanoSign emerges as an innovative breakthrough. By moving away from deterministic digital codes and utilizing the stochastic or chaotic arrangement of tens of thousands of pixels at the nanoscale, the system creates a physical fingerprint that is highly improbable to replicate through software or external tampering. This shifts the focus from digital encryption, which can eventually be hacked, to physical irreproducibility, which is governed by the laws of physics.

Although NanoSign markers are designed to be cost-effective at scale, the total cost of ownership, including specialized scanning hardware, software integration, and technical maintenance, remains a significant factor for potential adopters. Furthermore, due to the novelty of the technology, there is currently a lack of long-term, large-scale commercial case studies to serve as a definitive proof of concept.

However, the true potential of NanoSign lies in its architectural flexibility. Rather than replacing legacy systems, it can be integrated into a multi-layered security strategy. For instance, combining RFID for bulk pallet tracking with NanoSign markers on individual items creates a robust authentication loop that covers both logistical efficiency and forensic integrity.

The identification of high-risk sectors, including sanctioned goods, high-value assets, pharmaceuticals, fashion brands, and electric vehicle battery passports, provides a clear roadmap for the technology's future. Each of these areas currently suffers from systemic "security holes" that traditional tracking cannot plug. Implementing NanoSign in these fields would serve as the ultimate test for its theoretical advantages.

In conclusion, while the technology is highly promising on paper, its value as a definitive logistical standard will ultimately be determined by its performance in rigorous field tests and its ability to prove economic viability in a real-world environment.

AUTHOR CONTRIBUTIONS

A.S. conducted the research and wrote the manuscript. P.T. supervised the research, provided conceptual guidance, and reviewed and edited the manuscript. All authors have read and agreed to the published version of the manuscript.

Declaration of generative AI and AI-assisted technologies in the manuscript preparation process

During the preparation of this manuscript, the authors used Gemini (Google) to improve language clarity and stylistic quality and to support the analysis and synthesis of the scientific literature. After using this tool, the authors carefully reviewed and edited the content as needed and take full responsibility for the content of the published article.

REFERENCES

- [1] NanoSign Holding Zrt. Retrieved from <https://www.nanosign.eu/#about>, (2026.09.04).
- [2] SMark Technology Zrt. Retrieved from <https://smark.eu/>, (2026.09.04).
- [3] Shaimurat, A. & Tamás, P. (2026). *Applications of the NanoSign labelling and tracking system in logistics* [TDK thesis / Scientific Student Conference paper]. Faculty of Mechanical Engineering and Informatics, University of Miskolc.
- [4] Kim, S. C., Park, J. H., Chin, S. O., Kim, J. & Kim, D. (2026). Recent advances in anti-counterfeiting technology using fluorescent hybrid materials. *Advanced Composites and Hybrid Materials* **9**(1), 24, <https://doi.org/10.1007/s42114-025-01534-4>
- [5] Majzooobi, M., Koushanfar, F. & Potkonjak, M. (2009). Techniques for design and implementation of secure reconfigurable PUFs. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)* **2**(1), 1-33, <https://doi.org/10.1145/1502781.1502786>
- [6] Dwivedi, A. & Dwivedi, A. (2012). Emerging trends in nano technology for modern industries. *Int J Eng Innov Technol (IJEIT)* **2**(6), 4-13.
- [7] Mazakov, T. Z. & Abilkhaiyr Z. S. (2020). Using barcodes to identify products. *VESTNIK KazUTB* **8**, Retrieved from <https://rmebrk.kz/journals/6224/1157.pdf#page=8>, (2026.09.04).
- [8] Ahmed, M. R., D'silva, F. & D'silva, D. (2022). An Introduction to RFID Systems. *Journal of latex class files*, **14**, 8. https://www.researchgate.net/publication/362581874_An_Introduction_to_RFID_Systems, (2026.09.04).
- [9] Fortuna, G. & Gaspar, P. D. (2022). Implementation of Industrial Traceability Systems: A Case Study of a Luxury Metal Pieces Manufacturing Company. *Processes* **10**(11), 2444, <https://doi.org/10.3390/pr10112444>
- [10] Gandhi, J. (2026). BLE vs UWB Technology Comparison for RTLS Deployment. *Locaxion Tracking Simplified*. Retrieved from <https://locaxion.com/blogs/ble-vs-uwb/>, (2026.09.04).
- [11] Mizerák, M., Trojan, J., Trebuňa, P., Kliment, M. & Mozol, Š. (2026). Integration of UWB-Based RTLS and Simulation for Data-Driven Optimization of Manufacturing Layouts. *Applied Sciences* **16**(14), 7183, <https://doi.org/10.3390/app16147183>
- [12] Skurowski, P., Nurzyńska, K., Pawlyta, M. & Cyran, K. A. (2022). Performance of QR Code Detectors near Nyquist Limits. *Sensors* **22**(19), 7230, <https://doi.org/10.3390/s22197230>
- [13] Miao, S., Wang, P., Liu, Z., Hao, Q. & Qu, W. (2026). Design of UHF RFID Tag Antenna for Metallic Surfaces. *Scientific Journal of Technology* **8**, 86-95, <https://doi.org/10.54691/vzgs036>
- [14] Coppens, D., De Poorter, E., Shahid, A., Lemey, S. & Marshall, C. (2022). An Overview of Ultra-WideBand (UWB) Standards (IEEE 802.15.4, FiRa, Apple): Interoperability Aspects and Future Research Directions. *IEEE Access* **10**, 70219-70241, <https://doi.org/10.1109/ACCESS.2022.3187410>

- [15] Ranganathan, A., Danev, B., Francillon, A. & Capkun, S. (2012). Physical-layer attacks on chirp-based ranging systems. *WiSec'12 - Proceedings of the 5th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 15-26, <https://doi.org/10.1145/2185448.2185453>
- [16] Inpixon RTLS: *Real-Time Location System for Industrial Operations*. Retrieved from <https://www.inpixon.com/technology/rtls>, (2026.09.04).
- [17] Balkema, M. E. (2023). *Using RFID-Technology For Improved Traceability And Information Sharing; Creating An Integrated Food Supply Chain From Farm To Fork*. University of Twente. Retrieved from https://essay.utwente.nl/fileshare/file/97204/Escolano%20Balkema_MA_BMS.pdf, (2026.07.26).
- [18] Latvian State Security Service (VDD) (2026). *Press release on the prosecution of individuals regarding illegal exports of dual-use goods*. Government of Latvia. Retrieved from <https://www.prokuratūra.lv/lv/aktualitates/2026/aktualitates/11-gadi-ieslodzijuma-par-atbalsta-nodrosinasanu-krievijas-armijai-3710>, (2026.09.04).
- [19] Barth, F., Eckert, C., Gatzert, N. et al. (2022). Spillover Effects from the Volkswagen Emissions Scandal: An Analysis of Stock and Corporate Bond Markets. *Schmalenbach J Bus Res* **74**, 37–76, <https://doi.org/10.1007/s41471-021-00121-9>
- [20] Official Journal of the European Union (2023). *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*. Retrieved from <https://eur-lex.europa.eu/eli/reg/2023/1542/oj/eng>, (2026.09.04).
- [21] World Health Organization (WHO). (2017). *A Study on the Public Health and Socioeconomic Impact of Substandard and Falsified Medical Products*. Retrieved from <https://www.who.int/publications/i/item/9789241513432>, (2026.09.04).
- [22] Pharmaceutical Security Institute. (2025). *Incident trends*. Retrieved from <https://www.psi-inc.org/incident-trends>, (2026.09.04).
- [23] Serious Fraud Office (2026). *SFO secures 4-year prison sentence for aircraft parts fraud*. Retrieved from www.gov.uk, (2026.09.04).
- [24] OECD (2025). *Mapping Global Trade in Fakes 2025. Report. Global Trends and Enforcement Challenges*, <https://doi.org/10.1787/94d3b29f-en>
- [25] European Union Intellectual Property Office (EUIPO) (2024). *EU enforcement of intellectual property rights: results at the EU border and in the EU internal market 2023*. Official report. Retrieved from <https://euipo.europa.eu/>, (2026.09.04).
- [26] *Joint Statement for the inclusion of Intellectual Property Crime as a priority in the EU Commission's EMPACT 2026-2029 policy cycle* (2024). Retrieved from <https://www.indicam.it/wp-content/uploads/Joint-Statement-EMPACT-IP-Crime-Priority-Support.pdf>, (2026.09.04).