Global Distributed Tracking of Supplies via Free-libre Open Source Cryptography Obviating Authentication

Robert L. Read President
Public Invention
Austin, TX, USA
ORCID: 0000-0003-4749-7045

Victoria Jaqua Medical Community Lead
Open Source Medical Supplies
ORCID: 0009-0006-9907-5150

Christina A. Cole Head of Documentation
Open Source Medical Supplies
San Francisco, CA
ORCID: 0009-0002-7912-6425

Francesca Williams GOSQAS Regulatory Lead
Public Invention
Lake Worth, FL, USA
ORCID: 0009-0002-5500-7317

Nina Lahoti UX Developer
Public Invention
Houston, TX, USA
ORCID: 0000-0002-9467-1272

Nora Moor Incoming Student
Carnegie Mellon University
ORCID: 0009-0000-4256-1197

June 24, 2025

Abstract

In higher-income countries, manufacturers, processors, and logistics managers of life-affecting goods such as food, medicine, and medical equipment are required to document product life cycles from factory, to warehouse, and eventually to the end-user. However, some low and middle-income countries (LMICs) do not have logistic management systems or regulatory agencies overseeing processing standards. Global aid shipments may be impossible to track in low-resource environments, and bad actors may flood markets with counterfeit products.

Global Distributed Tracking (GDT) provides a novel solution: anyone handling an object may securely and anonymously document the object by uploading media, shipping manifests, location receipts, and quality reports without authentication. This encrypted, time-stamped "provenance" becomes a discoverable self-audit, granting the end-user trust through transparency. GDT allows an end-user to directly report adverse events pertaining to an object. This feature creates automatic fulfillment of some FDA and EU regulatory requirements for medical device distribution.

Keywords: cryptography, human-computer interaction, humanitarian engineering, zero-knowledge encryption.

1 Introduction and Motivation

Global humanitarian aid shipments risk theft and diversion, preventing essential supplies from reaching intended recipients [1]. Even organizations with good inventory control systems struggle to track shipments leaving central warehouses bound for rural locations, i.e, "the last mile" [2]. Bad actors who openly manufacture [3] and trade counterfeit goods sow distrust by flooding markets with low-quality supplies [4, 5]. Medical equipment purchased and distributed by non-governmental organizations (NGOs) to Low and Middle-Income Countries (LMICs) may prevent establishing an end-user/manufacturer relationship, thus increasing the risk of "dumping" [6, 7] and equipment failure due to unknown maintenance requirements and expired licenses. Global Distributed Tracking (GDT) [8] believes that our philosophy of "Trust Through Transparency" can solve these problems.

By constructing an uneditable, append-only data history, GDT provides transparent access to the entire humanitarian logistics life cycle. It fights counterfeiting by allowing for the construction of a complete chain of custody. It allows data access without requiring proprietary database management. The novel use of old-school cryptography avoids requiring global supply chain users to authenticate, thus maximizing convenience for everyone handling an object and avoiding compromise of personal data.

The "last mile" tracking issue affects users who may not share language with distributors or have access to secure networking or reliable electricity [9]. They may have tenuous or no business relationships with a distributor. It is unlikely that such users would sign up for a system that requires a login and user authentication.

Users may securely participate in the tracking and documentation of an object throughout its entire life cycle, including final use and disposal, without requiring authentication. Anyone who obtains a recorded object and scans the attached GDT QR code has the ability to add to (but not edit) that object's history. Identity disclosure is not required, although there are no barriers that prevent a user from revealing their identity. Users may upload documentation such as shipping manifests, quality inspection documents, or photos of the shipped object to expand the history of a shipment or object. Each addition builds a paper trail viewable to anyone holding a GDT-labeled object. This provides an inimitable "provenance" which proves an object's origin.

2 Related Research

One meta-study [10] found that 13.6% of medicines (pharmaceuticals) worldwide were of poor quality. Although GDT does not focus on pharmaceuticals, this finding may apply to devices as well [11].

Kootstra [12] comprehensively reviews track-and-trace systems (particularly for pharmaceuticals) to combat substandard and falsified medicines that have been implemented via regulation in many countries. In contrast to the language of that paper, GDT is a voluntary, non-national track-and-trace system that applies to more than pharmaceuticals.

Some papers [13] describe a powerful system for non-fungible tokens to track and trace items. Such systems require identity and authentication to track ownership or custody of the digital twin. This can enforce the right to transfer the ownership to a different party, but requires active participation across the supply chain. In contrast, GDT is purely voluntary, which has the disadvantage of not directly enforcing ownership but the advantage of minimizing user effort.

3 Basic Use Case

The fundamental use case of a product that fights substandard and falsified medical supplies in a global supply chain is depicted in Figure 1. In this example, the goal is to convince a medical doctor in Tanzania that a medical device made in the Czech Republic is trustworthy and of high quality. The life cycle of the object in the supply chain is:

1. An item is made in Prague by a maker or a manufacturer named J. Cale. To increase trust in her product, she hires an independent third party to test it. She creates a unique GDT key for her product, downloads a QR code that links to her product's auto-generated GDT history record, and labels her product with the QR code.

2. K. Novak receives the product in Prague and completes testing. He scans the QR code on the product, adds his test report, and ships it back to Prague.

Figure 1: Building Trust Through a Transparent Supply Chain

3. J. Cale verifies receipt and documents shipping to a distributor, S. Gamal in Egypt.

4. S. Gamal receives the product, uses her phone to add a record confirming receipt in Egypt, and documents shipment to a marketer, A. Juma, in Tanzania.

5. A. Juma scans the QR code with his phone to verify receipt, and after purchase by a Tanzanian customer, ships it to Tanzania.

6. Dr E. Adil, the buyer and ultimate user in Tanzania, points his phone at the QR code and sees a complete, intact, and uneditable chain-of-custody demonstrating quality testing and a realistic and comprehensive supply chain transit path from manufacturer to marketer. Because this documentation would be nearly impossible to fake, Dr. Adil trusts the item.

The addition of records to the history of the item is always voluntary. Since users in each step of the supply chain have a vested interest in increasing trust in the products they are making or distributing, it is worth the small amount of time to scan the QR code and add a tag, upload a document, or attach a photo to their product's history record. Since authentication is not required, the barrier to entry is very low—no download, login, fee, or password is needed. They still may voluntarily choose to reveal their identity. For example, A. Juma

might be more than happy to provide his email address to the medical personnel to whom he sells products.

When our hypothetical Dr. Adil points his smartphone at the QR code, he sees the screen captured in Fig 2. Notice that each record entry has an indelible timestamp.

With consistent participation, the historical record will be very hard to fake because each record entry is automatically timestamped; the user cannot manually set it. In order to deceive Dr. Adil using a GDT record, a fraudster would have to start months ahead of time and be integrated into the supply chain because Dr. Adil knows that he purchased this from A. Juma. If A. Juma himself is corrupt and part of a fraudulent scheme, he is participating and adding to a highly documented paper trail, which could eventually lead to his discovery. We believe documentation is the natural nemesis of thieves and scammers.

4 A Novel Security Model

Merriam-Webster [14] defines *provenance* as

> the history of ownership of a valued object, or work of art or literature.

In the past, the US patent office used an "inventor's notebook" as the basis for judging conflicting invention claims. Such a historical record created over time is difficult to counterfeit due to the temporal nature of record entries. GDT provides "Trust Through Transparency" by creating a unique version of "provenance", a timestamped "record history" of relevant documentation is extremely difficult to forge.

Typically, the right to comment online is based on one's identity, loosely verified through a sign-up process. On some sites and applications, one can comment on something without any authentication whatsoever. Neither of these models work well to track objects across the global supply chain to an end user, over national boundaries and across language barriers. It is impossible to expect every supply chain member to be part of a trust network, especially if one includes the end user. Giving anyone the privilege to comment regardless of personal connection allows for vandalism and malfeasance, whether by human or robotic malware.

Our solution is to construct a new model, which we call the *hand-hold model*:

> You have the right to read the history of and append-only comment on an object if you have held it in your hands.

Consider a crate. The hand-hold model gives anyone in close physical proximity to the crate the the right to see the record history of the crate and the right to append new comments to the same record history.

The hand-hold security model is implemented by a secret key that is physically attached to the object, such as through a printed and attached QR code.

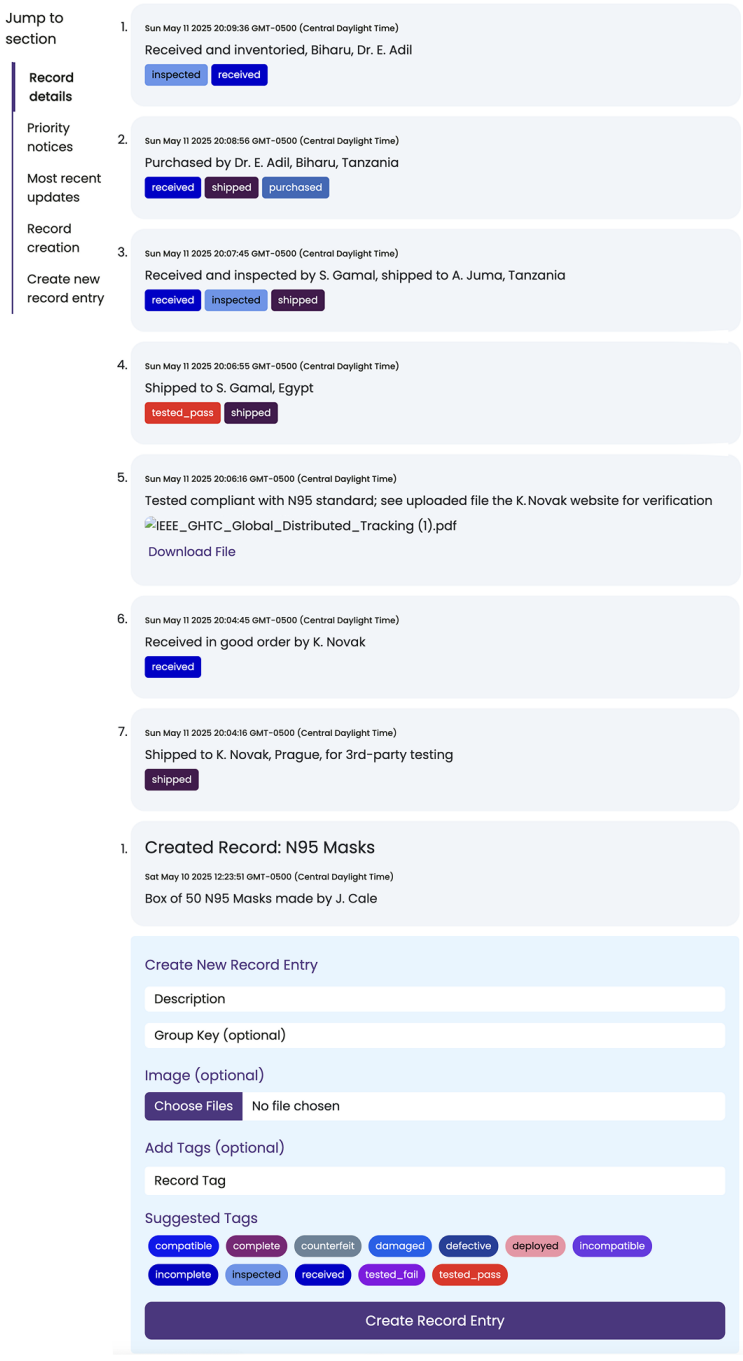

Figure 2: The History Record

This model has several security disadvantages that must be mitigated by policy:

- Everyone who sees the QR code is able to see the entire history, including the history that will be added later when they no longer possess the object.
- Anyone who sees the secret key could publish the key, making it no longer secret and opening it to the possibility of spam and malfeasance.

Mitigation approaches are described in Section 9.

When applied to global tracking, the hand-hold model has a number of tremendous advantages that outweigh its potential shortcomings:

- It requires no authentication.
- It supports defense-in-depth. If a key is compromised, that may allow a record to be vandalized, but it does not erase the previous history or damage the security of any other keys.

4.1 Differences with the FDA UDI

The US FDA Unique Device Identifier (UDI) [15] shares some properties with the GDT Record Key. However, there are key differences between the "hand-hold" model and the UDI.

1. GDT is a computer system that uses an identifier implemented via a website; the UDI is an identifier.
2. The UDI is required by US law on some devices (this set is expanding.)
3. The GDT key and the "hand-hold" model give people the ability to attach documentation to the GDT history record at any time. The UDI provides no such capability; it is only a number. A UDI may be placed in separate databases to identify objects, though, as some lament [15], this is optional and spotty.
4. The UDI is public information and can be used to construct statistics across multiple manufacturers and distributors or independently of those distributors.
5. The GDT Key unlocks a record originated by the creator and distributed to users who may append to it through the "hand-hold" security model. Only the distributor is capable of constructing a product-wide statistical picture if they choose to do so.

Global Distributed Tracking intends to harmonize with the US FDA UDI. We envision a future world in which devices are labeled with both codes. Although tracking is the purpose of both codes, the actual use case differs.

5 Zero-Knowledge Encryption

GDT implements *zero-knowledge encryption*. GDT does not store keys and cannot read the history of the objects tracked by GDT. Since there is no single store of keys, no single act of cyberhacking can compromise all keys.

GDT thus offers strong privacy, subject to the limitations already mentioned of the "hand-hold" model.

6 Labeling Granularity

GDT supports the maker, manufacturer, or distributor of objects by supporting keys at different granularities corresponding to the packaging processes of that organization. For example, an individual object might be packed ten to a box, ten boxes to a carton, and 50 cartons to a crate, and a manufacturing batch might contain 15 crates. GDT provides a group key system in which keys have a tree relationship. This allows keys to be associated with every level of a manufacturer's packaging and shipping process. In this example, an ancestor key may be created to represent the entire manufacturing batch of 15 crates. This key allows the entire tree (that is, all of the individual objects in each crate, carton, and box) to be recalled in a single action.

By design, a holder of a group key can see all the keys of the items in the group. (In other words, the parent can know who the children are.) However, a child cannot discover a parent. Once a group is broken apart and distributed (for example, when a box of ten objects is opened and each object sold individually) a handler of a single distributed object cannot reveal the keys to the object's siblings. In this way, a bad actor can deface a single object but cannot deface objects that they do not directly handle.

In order to allow reporting on the condition of a container (for example, if a carton containing 10 boxes is crushed in shipping) a *reporting key* is associated with the carton. A shipper may report that the carton was crushed and add a photo by scanning the QR for the reporting key. The distributor will become aware of this shipping problem. The group key, however, should not be printed or published in any way. Therefore, nobody can deface all 10 boxes or 100 items without taking the trouble to open each carton and take 100 specific actions.

Fig. 3 depicts an example of 2 levels of group keys. Each of the 10 items $T0 - T9$ is packed into a carton called $C0$. At manufacturing or distribution time, the labeler uses GDT to product a parent key $C0$ and 10 item keys $T0-9$. On the diagram, only two carton keys, $C0$ and $C1$ are depicted. These are both children of the group B that tracks a whole batch. The distributor can recall the entire batch B with a single action because the record for each individual items T_x is a descendant (grandchild) of B.

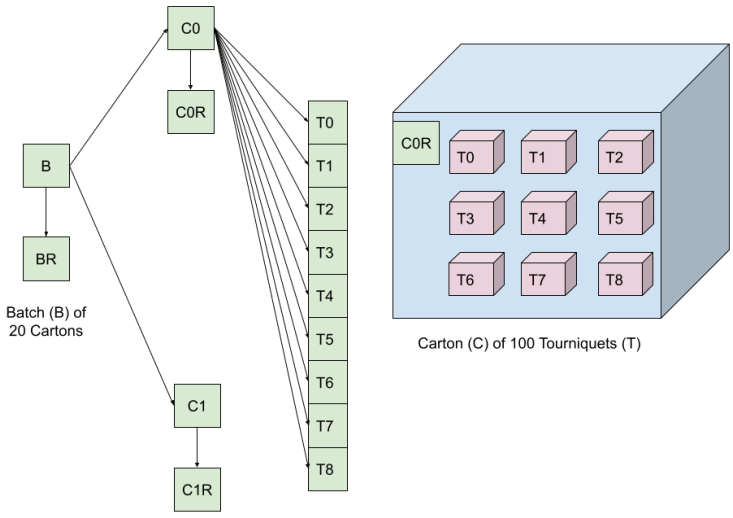

Figure 3: Group Key Example

6.1 Reporting Keys

We believe a best practice is the generation of a secret key for every individual device that is worth labeling, or, for example, that would obtain a Unique Device Identifier under the FDA rules. This provides the greatest defense-in-depth. However, to prevent a malicious user from recalling every individual item in, for example, a carton containing 10 items, we generate *reporting keys* as depicted in Fig. 3. $C0R$ and $C1R$ represent *reporting keys*. A reporting key is *not* a parent of the items, but a sibling of the items. Therefore, it cannot be used to recall or annotate the individual items in the carton. Since the parent key $C0$ need not be published at all, nobody can vandalize all 10 $T0-9$ records without taking 10 actions. However, the carton key, whose QR code can be printed on the carton, allows the carton to be commented on, such as "This carton was crushed in shipping," or "This carton was found abandoned on the highway." If the distributor learns from its reporting key that a carton has been stolen or damaged, they can annotate all of the item keys in that group with a single action on $C0$.

7 Harmonization with the US FDA

The U.S. Food and Drug Administration (FDA) regulations on medical devices [16] are surprisingly easy to understand by lay-persons.

The FDA requires manufacturers of medical devices to establish systems that

ensure traceability, complaint handling, and recall preparedness as outlined in Title 21 of the Code of Federal Regulations. These requirements support patient safety and device accountability long after a product leaves the production line. The European Medical Device Regulation (EU) 2017/745 (MDR) [17] holds similar requirements for systemic and proactive gathering of user experience once a product is placed on the European market. European post-market surveillance is especially important to remember in relation to European-manufactured devices that are purchased and subsequently distributed to LMICs, which may be geographically outside the EU market but benefit from the EU regulatory environment.

NGOs play an essential role in the distribution of medical aid to LMICs. They manage needs assessment, procurement, purchase, storage, and eventual distribution of medical equipment to medically under served communities. However, this role is often that of the middleman—the relationship between the purchaser (NGO) and the vendor or manufacturer ends once the equipment is delivered. This leaves the end-user with no direct relationship to the manufacturer and no way to communicate possible equipment failures, calibration needs, license expiration, or maintenance schedules and training [18]. Manufacturing headquarters are often in higher-income, western countries, with no local representation in the end-user locale. This relationship gap results in "dumping" (end-of-life equipment being sent to LMICs) and overall equipment failures because there is no way to collect and facilitate user experience data.

Inspired by the just-in-time rapid manufacturing occurring locally or internationally in response to humanitarian crises [19], often incorporating open-source designs, GDT was originally built to promote trust in open-source medical devices. We believe that increasing device safety transparency of open-source medical supplies is a requirement for global acceptance. Hence, the closed-loop tracking provided by GDT allows anyone with access to a GDT-labeled open-source medical device to view the record history and append to it via a website. These features useful to open-source medical device transparency are also relevant to regulatory compliance post-market surveillance interface, for both the FDA and EU. Data housed within GDT becomes a discoverable self-audit which can be accessed and amended without requiring an end-user or organization to maintain a proprietary database.

GDT is being developed to support compliance objectives by providing a tamper-evident, distributed method of recording complaint data and device feedback. Although it does not yet fulfill all FDA regulatory requirements, GDT's architecture introduces traceability features that align with the intent of the FDA's post-market and recall framework, particularly in settings where traditional quality infrastructure is limited. Greater community uptake and diverse needs mapping will improve current limitations within the GDT platform.

7.1 Post market Surveillance

The FDA defines post-market surveillance as the active, systematic, and scientifically-valid collection, analysis, and interpretation of data or other information about

a marketed device. Requirements are codified under 21 CFR Part 820 (Quality System Regulation) [20] and, in specific cases, 21 CFR Part 822 [21]. This includes the requirement to maintain complaint files (820.198), investigate failures, and record all device-related feedback for the lifetime of the product. GDT continues to troubleshoot and develop systems that prioritize safety supervision and maintain FDA surveillance compliance.

GDT contributes to these goals by maintaining immutable, timestamped records of each submitted device entry. Although current entries are not attributable to individual users, a requirement under 21 CFR Part 11 [22], GDT ensures that each record cannot be altered or deleted and its integrity can be verified. This sustains audit readiness by ensuring that a complete, chronological trail of end-user recorded feedback is available. GDT's process security is specifically notable and is achieved by appending new entries to a write-once, append-only record, which ensures that each event is cryptographically anchored with both a time and event signature. Through this architecture, GDT has developed a comprehensive chronology of compliant data that is permanently retained and verifiable. The strength of the records' immutable, timestamped nature effectively makes the tracked device not tamper-proof, but tamper-evident. However, features such as status tracking, complaint escalation, and corrective action linkage—as required by Part 820.198 [23] and ISO 13485:2016 [24] section 8.2.2—are currently rudimentary and prone to human error due to reliance on inconsistent manual tagging. GDT remains eager to reduce barriers for smaller-scale or decentralized manufacturers to meet FDA post-market expectations, but doing so would potentially require integration into a broader validated quality system to support full compliance.

7.2 Recalls

Parts 7, 810, and 806 detail product recalls, corrections, and removals for medical devices. 21 CFR Part 7 [25] recommends that product recalls exist predominantly as a voluntary action a manufacturer or distributor takes in the event a defect with a medical device or label has the potential to cause a health or safety concern. 21 CFR Part 806 [26] requires domestic manufacturers and importers to report specified device corrections and removals to the FDA, mandating that non-reportable correction and/or removal documentation be maintained. 21 CFR Part 810 [27] details specific mandatory recall procedures initiated by the FDA under certain conditions. The scope of Part 810 applies when there is a reasonable probability that a device would cause serious adverse health consequences or death, and is implemented when companies refuse to act on serious health risks. The FDA's recall authority, established under 21 CFR Parts 7, 806 [26], and 810 [27], empowers the agency to request or mandate the removal of unsafe devices from the market. Effective recalls depend on the manufacturer's ability to identify and trace distributed devices accurately and in real time, especially in response to complaints or adverse events. GDT's current structure meets CFR Parts 7, 806, and 810 by enabling prompt identification, traceability, and field correction of devices through its tamper-evident serialization and audit

trails. It supports voluntary recalls (Part 7) by allowing manufacturers and distributors to track and document evidence distribution. GDT ensures Part 806 compliance through structured record keeping and standardized data capture for corrections and removals. If mandated under Part 810, GDT's architecture can facilitate FDA-directed recalls by maintaining immutable chain-of-custody data and demonstrating recall readiness via real-time device status tracking.

While GDT's append-only architecture provides strong data permanence and transparency, compliance with recall regulations would depend on procedural controls external to the system, including manual batch records, event escalation workflows, and communication protocols with the FDA.

8 Architecture

GDT uses Nuxt [28] and Vue [29] for its front end, cleanly separated from the back-end API hosted with Azure [30], which accesses Azure blob storage.

The front-end/back-end architecture is a now-classic pattern that separates the graphical user interface (GUI) from the "business logic" details. Since our ethos is free-libre open source software, we invite 3rd party developers to write code using our live backend, enabling them to repackage it to serve a set of users, such as a given language community, more effectively. Following Public Invention Free-Culture License Guidelines [31], all of our code is released under free-libre open-source licenses. Everyone is free to use our code [8] to implement and host their own completely independent data store. In all cases, however, we reserve all rights to our trademarks, names, and logos in order to prevent confusion among users.

The database (back-end) structure is very simple. It consists of a set of encrypted blobs referenced by a device ID. Each record may have a set of encrypted attachments as well. These blobs can be decrypted only with the key created when the record was created. Each decrypted blob consists of a set of historical entries containing:

- A description
- A timestamp
- Optional tags
- An optional attachment

8.1 Encryption Details

Counter-intuitively, a user uses a key, not a device ID, to access a record. The decryption of the key provides the device ID so the record can be retrieved from blob storage. The device ID without the key has no value and provides no decipherable information. Because the device ID is a hash of the key, anyone can decrypt a key into a device ID. However, the key cannot be obtained from the

device ID. Even if the entire database were made public, nobody but key-holders would be able to read any records.

Global Distributed Tracking encrypts user data and ensures its accessibility only through the unique record key linked to a QR code. A cryptographic hash function securely references data via the record key. AES encryption with 128-bit keys is used [32] along with SHA-256 [33] for cryptographic hashing. This process is performed in a zero-knowledge manner, ensuring that the Global Distributed Tracking team never stores a key (though obviously it uses keys "in flight".) Only Global Distributed Tracking users, and individuals with whom they share a record key, have access to record history stored within the key.

8.2 User Interface

The user interface is simple and lightweight, allowing for fast load times even in locations with unstable and weak internet connections. The interface is available in dark mode to help users save battery if using the application for extended periods. To accommodate those sensitive to eye strain and avoid other accessibility concerns with dark mode, the application's color mode automatically matches the user's device preferences. The design features large-scale text and high contrast color schemes to aid in readability and enhance overall accessibility.

In each history record, users can upload and attach documentation files such as relevant photos or PDFs. When creating a new record entry, users have the option to either select from a list of common, color-coded status tags to standardize documentation or enter custom tags. This design not only ensures visual consistency but also enhances readability and allows users to quickly identify common tags by colors alone. The color assigned to a tag remains permanently associated with the tag. Moreover, light and dark color variants are separated to maintain legible contrast, adjusting the tag text color accordingly. This feature reinforces GDT's focus on usability in low-resource environments by making information more scannable, accessible, and intuitive at a glance.

Additionally, to reduce the risk of malicious or inappropriate use, the team sourced and reviewed a list of forbidden tag names, banning sexually explicit or illicit terms in non-medical contexts. As part of this process, we developed and curated a prohibited word list to prevent the abuse of the GDT tagging system for imparting inappropriate content. This list was integrated into the tagging infrastructure so that any contributions to record histories remain professional and aligned with GDT's humanitarian values.

9 Security Weaknesses

There are several identifiable security weaknesses:

- We do not store keys, but we cannot currently prove that to the user. Although verification can be proven in our open source code, there is no way to prove that code is precisely the code running our servers. This can

be addressed by allowing browser-based hashing to blind the key. This feature can be implemented when users request it.

- Since we offer GDT completely free of charge, we are subject to a denial of service attack, which would consume some space resources on our servers. We combat this with throttling.

- If a key is erroneously published or "stolen," someone may use that key to vandalize a record. Note, however, this does not invalidate the record history before that point. If deception is attempted, such as placing the same QR code on a fraudulent item, they can make an item appear trustworthy while being detectably different. However, if the original item is not also stolen, it will eventually become apparent that the same item is claimed to be in two different places at the same time, exposing the fraudster to significant risk.

10 Current Usage

GDT is completely functional and, at the time of writing, has been used by two groups to track medical devices. Both groups are manufacturing the open-source Glia tourniquet [34].

11 Future Work

We are constructing a system that allows user subscriptions to record amendments via email notification. The initial implementation will rely on simply recording email addresses. Ultimately, this notification system will become a 3rd party service, allowing GDT zero-knowledge of individual email addresses in order to maintain product security standards. Similarly, we never store keys or unencrypted data, but the user is currently unable to verify that claim. Because we use off-the-shelf encryption, which runs in the browser, we plan to demonstrate that no unencrypted data ever leaves the user's browser. Currently, GDT has no cultural standing within the broad humanitarian logistics network when compared to large commercial systems. We believe that GDT will become most effective when user adoption scales value propositions ("GDT reduced our rural overland shipment loss by 53%") and becomes a logistics standard ("to renew your next funding cycle, you must track medical shipments within GDT"). To achieve this, we must expand our user base significantly. Markets may eventually require Global Positioning System (GPS) capability to provide robust location tracking within a GDT record history. This feature could be implemented upon user demand.

Acknowledgment

The GDT development team includes or has included: Serene Belhadj-Yahya, Coco Chen, Christina A. Cole, Ben Coombs, Alison Gilpatrick, Victoria Jaqua, Sofiya Koretskaya, Nina Lahoti, Nora Moor, Hieu Van Ngo, Harry Pierson, Katie Pryal, Anya Ranavat, Robert L. Read, Jara Rodriguez, Anusha Shringi, Divya Reddy Suram, Hira Taqueer, Francesa Williams and Judith Weng Zhu.

References

[1] Giulia Paravicini, Steve Stecklow, and Tiksa Negeri. UN food agency failed to act as U.S. aid was looted in Ethiopia, 2024. https://www.reuters.com/investigates/special-report/famine-aid-ethiopia/.

[2] Mahdi Noorizadegan, Mohammad Fattahi, Esmaeil Keyvanshokooh, and Jon M Stauffer. Last-mile humanitarian logistics planning with isolated communities, 2024. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4894219.

[3] Emma Hooper. Fake pharmaceutical industry thrives in West Africa, 2020. https://www.bbc.com/news/world-africa-53387216.

[4] CA Goodman, SP Kachur, S Abdulla, P Bloland, and A Mills. Regulating tanzania's drug shops–why do they break the rules, and does it matter? *Health policy and planning*, 22(6):393, 2007.

[5] 1 in 10 medical products in developing countries is substandard or falsified, 2017. https://www.who.int/news/item/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified.

[6] Isobel H Marks, Hannah Thomas, Marize Bakhet, and Edward Fitzgerald. Medical equipment donation in low-resource settings: a review of the literature and guidelines for surgery and anaesthesia in low-income and middle-income countries. *BMJ global health*, 4(5):e001785, 2019.

[7] Sophie Ingline. X-RAY MACHINES : Africa's Broken System, 2020. https://vimeo.com/323994866.

[8] Global Distributed Tracking (GDT). GitHub repository, 2025. https://github.com/gosqasorg/asset-provenance-tracking.

[9] Driving Last-Mile Solutions to Ensure Access to Public Health Commodities, 2023. https://www.ghsupplychain.org/driving-last-mile-solutions-ensure-access-public-health-commodities?utm_source=chatgpt.com.

[10] Sachiko Ozawa, Daniel R Evans, Sophia Bessias, Deson G Haynie, Tatenda T Yemeke, Sarah K Laing, and James E Herrington. Prevalence

and estimated economic burden of substandard and falsified medicines in low-and middle-income countries: a systematic review and meta-analysis. *JAMA network open*, 1(4):e181662–e181662, 2018.

[11] Substandard and falsified medical products, 2024. https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products.

[12] Joeke Kootstra and Tineke Kleinhout-Vliek. Implementing pharmaceutical track-and-trace systems: a realist review. *BMJ global health*, 6(Suppl 3):e003755, 2021.

[13] Senay A Gebreab, Haya R Hasan, Khaled Salah, and Raja Jayaraman. NFT-based traceability and ownership management of medical devices. *IEEE Access*, 10:126394–126411, 2022.

[14] Merriam-webster online dictionary, 2025. https://www.merriam-webster.com/dictionary.

[15] Madris Kinard and Lisa McGiffert. Medical device tracking—how it is and how it should be. *JAMA Internal Medicine*, 181(3):305–306, 2021.

[16] USC 21, Chapter I, Subchpater H, Section 800.

[17] REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, 2017. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745.

[18] Victoria Jaqua. Why a Global Open Source Quality Assurance System (GOSQAS)? Motivating Solutions for Diverse Use-Cases, 2024. https://drive.google.com/file/d/1N-lX5oFsy0uqPPFxEe9CqiuSgUexDNQl/view.

[19] Design, Make, Protect: A report on the open source maker and manufacturer response to the COVID-19 PPE crisis, 2021. https://opensourcemedicalsupplies.org/wp-content/uploads/2021/01/Design-Make-Protect_21.01.27.pdf [Accessed: (May 16th 2024)].

[20] 21 u.s.c. § 820. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-H/part-820, 2025. Section 820 of Title 21 of the United States Code.

[21] 21 U.S.C. § 822. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-H/part-822, 2025. Section 822 of Title 21 of the United States Code.

[22] 21 U.S.C. § 11. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11, 2025. Section 11 of Title 21 of the United States Code.

[23] 21 U.S.C. § 820.198. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-H/part-820/subpart-M/section-820.198, 2025. Section 820.198, of Title 21 of the United States Code.

[24] Iso 13485:2016(en) medical devices — quality management systems — requirements for regulatory purposes.

[25] 21 U.S.C. § 7. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-7, 2025. Section 7 of Title 21 of the United States Code.

[26] 21 U.S.C. § 806. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-H/part-806, 2025. Section 806 of Title 21 of the United States Code.

[27] 21 U.S.C. § 810. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-H/part-810, 2025. Section 810 of Title 21 of the United States Code.

[28] Kareem Dabbeet and Mahmoud Baalbaki. *Nuxt 3 Projects: Build Scalable Applications with Nuxt 3 Using TypeScript, Pinia, and Composition API*. Packt Publishing Ltd, 2024.

[29] Erik Hanchett and Ben Listwon. *Vue. js in Action*. Simon and Schuster, 2018.

[30] Jonah Carrio Andeersson. *Learning Microsoft Azure*. O'Reilly, 2023.

[31] Public invention free-culture license guidelines (v0.1). https://github.com/PubInv/PubInv-License-Guidelines, 2025.

[32] AES Primitives. Advanced encryption standard (aes)(fips-197). 2003.

[33] FIPS 180-4 Secure Hash Standard (SHS), 2015. https://csrc.nist.gov/pubs/fips/180-4/upd1/final.

[34] The Glia Tourniquet Project, 2025. https://glia.org/pages/the-glia-tourniquet-project.