



Designation: D8558 – 24

Standard Guide for Verification of a Certificate of Authentication Used to Track Products through Their Supply Chain by Utilizing Blockchain Technology¹

This standard is issued under the fixed designation D8558; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This guide was written to introduce the concept of tracking physical and digital goods as well as crypto assets for transactions or marketing and branding purposes on a Web3 blockchain technology storage platform. This represents a significant shift in technology, where blockchain assets are available on a public digital ledger, open for all to view and verify. It marks a paradigm shift from the private cloud storage currently used in Web2 infrastructure platforms. This guide provides minimum requirements for the secure verification of a Certificate of Authentication (COA) used to track any product through their supply chain by utilizing Blockchain Technology. The implementation of blockchain technology can enhance the transparency, traceability, and trustworthiness of the supply chain, ensuring product quality and authenticity while reducing the potential for fraud, tampering, and other malicious activities. Each Certificate of Authenticity (COA) is minted on the blockchain, featuring a screenshot of the summary page on the front of a Non-Fungible Token (NFT) with the unique traits of that lab report tagged as metadata. Examples of this metadata include the name of the lab, the name of the client, the unique identifier of the sample tested, and the date the test was performed. To enhance the tracking and security of these COAs, various tracking devices can be linked to the COA on the blockchain, depending on the product's specific needs and the nature of the supply chain. These devices include RFID tags, QR codes, holograms, micro transponders, and embeddable watermarks. Each serves a unique purpose, from instant verification via QR codes to advanced security and tracking through RFID and micro transponders. Holograms and embeddable watermarks provide additional layers of security, making counterfeiting significantly more challenging and verifying authenticity more straightforward and reliable.

¹ This guide is under the jurisdiction of ASTM Committee D37 on Cannabis and is the direct responsibility of Subcommittee D37.05 on Security and Transportation. Current edition approved July 1, 2024. Published July 2024. DOI: 10.1520/D8558-24.

1.2 Certificates of Authenticity (COA's) should be verified by authorized parties in accordance with the applicable regulations within the authority having jurisdiction. It is the requirement of each party to ensure compliance and legal authority for the verification process.

1.3 A verification plan, based on a risk assessment, should be in place and executed for tracking products using a Certificate of Authenticity on the blockchain. The verification plan should identify/address:

1.3.1 The assets and data to be protected and the identified threats to those assets and data during the phases of the supply chain process. An example of this is a lab report that copied onto the blockchain with the image of the summary page on the front of the Non Fungible Token (NFT).

1.4 The specific verification measures to be deployed in the COA tracking program commensurates with the value of the physical assets being tracked and are broken into three key areas. Physical security measures for a COA ensure that the hard copies of the certificate, as well as any samples or products associated with it, are stored safely and are protected from unauthorized access, tampering, or damage. Tracking devices used to track the physical products could include RFID, QR codes or micro transponders. Technical security measures for a COA revolve around protecting the The digital versions or electronic records of the certificate once it is minted onto the blockchain. Administrative security measures for a COA encompass policies, protocols, and practices to oversee its lifecycle, ensuring compliance, authenticity, and trust through regular audits, training, and defined responsibilities.

1.5 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety, health, and environmental practices and determine the applicability of regulatory limitations prior to use.*

1.6 *This international standard was developed in accordance with internationally recognized principles on standardization established in the Decision on Principles for the*