ISO 20435:2026-10 (E)

Framework for representing physical assets using tokens

Contents

Page

Foreword vi

Introduction vii

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Overview 4
4.1 Background 4
4.2 Problems to address 4
4.3 Objective of the standard 5
4.4 Use case - digital product passport (DPP) 5

5 DID registry framework or reference architecture 7
5.1 Overview 7
5.2 DID registry framework 7
5.2.1 General 7
5.2.2 Data storage locations 8
5.3 Resolving the DID across multiple independent DID registries 8
5.3.1 General 8
5.3.2 Lookup registry 8
5.4 Tokenizing the DID data using NFTs 8
5.4.1 General 8
5.4.2 "Wrapping" the DID address in an NFT 8
5.4.3 NFT provides the DID registry encryption layer 9
5.4.4 Benefit: Ability to leverage advanced NFT features 10
5.5 pNFT minting sequence diagram 10
5.5.1 General 10
5.5.2 User interaction with inventory system 11
5.5.3 Data handling through middleware 11
5.5.4 Off-chain storage system interaction 11
5.5.5 Verifiable data registry and universal "Lookup" 12
5.5.6 Physical NFT (pNFT) creation 12
5.6 Alternate tokenization implementations 12
5.6.1 General 12
5.6.2 Data model in DID registry only implementation 12
5.6.3 Data model stored on-chain in the NFT layer 12
5.7 Framework conclusion 12

6 Physicalassetidentifier(PAI)generationmethod 12
6.1 Background and introduction 12
6.1.1 General 12
6.1.2 Rationale for hashing pre-existing universally unique identifiers 13
6.1.3 Harmonization with existing supply chain standards 13
6.2 DID generation method 14
6.2.1 General 14
6.2.2 DID generation method example 14
6.2.3 Use of alternate PAIs 14
6.3 Physical asset identifier (PAI) selection 14

6.4 PAI data object ... 15
6.5 Universal serial number (USN): a "DID URL shortening" method ... 15
6.5.1 General ... 15
6.5.2 USN shortening method ... 16
6.5.3 USN example ... 16

7 Assetdatamethods ... 16
7.1 Overview & general requirements ... 16

7.2 Types of asset data objects ... 17
7.3 Hashing method selection ... 17
7.3.1 Technical background ... 17
7.3.2 SHA-256 is the default hashing algorithm ... 17
7.3.3 Storing asset data history ... 17
7.3.4 Use of a non-binary hash tree approach ... 18
7.4 Encryption of data objects ... 18
7.5 Data object metadata ... 18
7.6 Quantum agility ... 19
7.7 Hash tree method - details ... 19
7.8 Snapshots and version identifiers ... 20
7.9 Hash tree generation and updating example ... 20
7.9.1 Overview ... 20
7.9.2 Initial minting of a pNFT ... 20
7.9.3 Remove data object A and re-mint the pNFT ... 21
7.9.4 Replace data object B with D ... 21
7.9.5 Hash tree generation and updating example conclusion ... 22
7.10 Hash tree explanation using a spreadsheet model ... 22
7.10.1 General ... 22
7.10.2 Snapshot 1: Initial minting ... 22
7.10.3 Snapshot 2: Deletion of data object A ... 22
7.10.4 Snapshot 3: deletion of B and addition of D ... 23
7.10.5 Snapshot 4: modification of metadata for object D ... 23
7.11 Justification for hash tree model ... 24
7.12 Hash tree storage location ... 24
7.13 Document size and computational considerations ... 24
7.14 Document management ... 24
7.15 Asset data permanence ... 24

8 Data objects and metadata ... 24
8.1 Overview ... 24
8.1.1 General ... 24
8.1.2 Schema and ontology ... 25
8.1.3 Default minimum viable schema to enable the transport layer ... 25
8.2 Alternative schema identification ... 25
8.2.1 General ... 25
8.2.2 Examples of schema identification ... 25
8.3 Data object types, schemas, metadata, attributes ... 26
8.3.1 General ... 26
8.3.2 Global attributes ... 26
8.3.3 System-level data object types ... 26
8.3.4 Mandatory system-level data object types ... 26
8.3.5 Optional system-level data object types ... 27
8.3.6 Optional business-level data object types ... 28
8.3.7 Traceability system integration ... 31
8.3.8 Designating permanent data objects ... 31
8.4 Metadata format ... 31
8.4.1 Ordering and required attributes ... 31
8.4.2 Use of structured data ... 31
8.5 Conclusion ... 32

9 Physicallayerverification ... 32
9.1 Introduction ... 32

9.2 Resolving physical asset identifier (PAI) conflicts 32
9.2.1 General 32
9.2.2 Resolving ambiguity between "part number" vs "model" 32
9.2.3 Handling inconsistent identifiers for the same asset 33
9.2.4 Handling missing identifiers 34
9.2.5 Handling colliding identifiers 35
9.3 Documenting data extraction methods 36

9.3.1 General 36
9.3.2 Retrieval methods 36
9.3.3 Manual data entry 37

10 DID method scheme 37
10.1 General 37
10.2 Overview of DID roles and components 37
10.3 DID document and metadata 38
10.4 DID generation method requirements 39
10.5 DID format and syntax 39
10.6 Standardized DID and API operations 39
10.6.1 General 39
10.6.2 Resolve DID 40
10.6.3 Register DID 40
10.6.4 Update DID 41
10.6.5 Deactivate DID 41

11 Trust anchors and legalities 41
11.1 General 41
11.2 Natural person identification 42
11.2.1 Digital credential requirements 42
11.2.2 Trust anchor requirements 42
11.3 Machine/software identification requirements 42
11.3.1 Software interaction signing 42
11.3.2 Trust anchor validation 42
11.4 Issues and considerations 42
11.4.1 Maturity of SSI/decentralized identity standards 42
11.4.2 Maturity of trust anchor standards 42
11.4.3 Legal ownership framework 42
11.5 Current domain-specific implementation 42
11.5.1 Role of trade and membership associations 42
11.5.2 Authority requests for device ownership 43
11.6 References to ISO/TR 23644 43

12 Encryption, privacy and cybersecurity 43
12.1 Overview 43
12.2 DID authentication and encryption options 43
12.3 Data transfer methods for encrypted pNFTs 44
12.3.1 General 44
12.3.2 Off-chain re-encryption method 44
12.3.3 Keystore transfer method 44
12.3.4 Implementation considerations 44
12.4 Encryption methods 44
12.4.1 Data object encryption 44
12.4.2 Optional individual encryption 44
12.5 DID and USN generation security considerations 44
12.6 Privacy considerations 45
12.6.1 Hashing and privacy 45
12.6.2 User responsibility 45
12.6.3 GDPR and privacy regulations 45
12.7 Cybersecurity best practices 45
12.8 Limitations and user responsibilities 45
12.8.1 Limitations of the standard 45
12.8.2 User responsibilities 45

12.9 References to DID method specification 45
12.10 Security conclusion 45

13 Conclusion 45

Bibliography 47