Accessing Digital Product Passports with Decentralised Identifiers

How DIDs can serve as a single point of truth for the digital twins of products.

Susanne Guth-Orlowski
Chief Innovation Officer
Spherity GmbH
Dortmund, Germany
susanne@spherity.com

***Abstract*—Product information of tomorrow will be digital, i.e., every product will have a digital twin. The first regulation that is mandating digital product information in the form of a digital product passport is the "new battery regulation". Those digital product passports need to be easily accessible, and their information needs to be verifiable, as it may come from untrustworthy sources from all over the world.**

Verifiable credentials are digital, verifiable attestations which can be used to capture such product information. They are always related to an identifier, in most cases to a decentralized. This article explains what requirements a product identifier has, how decentralized identifiers can be used as the future unique identifier for products, what benefits this brings, what work needs to be done to get there and what projects already use decentralized identifiers today.

Keywords—decentralized identifiers, digital product passports, digital twins, accessing product information.

I. Requirements for Digital Product Identifiers

Finding the right identifier for digital products is not an easy task, therefore let's start with the requirements, which have been collected from various relevant sources in the product passport ecosystem; such as from the talk of the European Commission about the digital product passport, from internal discussions of IDunion, from the "new Battery Regulation", from discussions in the Global Battery Alliance Track & Trace Group, from discussions in Gaia-X / (Cartena-X) and internal Spherity discussions.

1. The identifier must be globally unique.

2. The identifier solution must be scalable for global use.

3. The identifier must be suitable for being transported by a data carrier, such as a QR code

4. The QR Code shall contain some minimal information that is readable without an internet connection.

5. When scanning the QR code, the identifier must serve as a globally unique, uniform resource locator (URL) on the internet.

6. Customer facing technology to search for product information should be the same for all industries.

7. It must be possible by other means than scanning a QR code to search for the identifier on the internet and find product information.

8. The identifier must be usable for end consumer products but also for B2B - and pre-products.

9. The identifier format should be the same in all vertical and horizontal industries, so that each (pre-) product can be connected to another.

10. Identifiers should be suitable for batches but also for serialized products, i.e., with unique identifiers per product.

11. The identifier should allow to refer to/reuse existing widely used identifiers, such as universal product code (UPC), European Article Number (EAN), Global Trade Item Number (GTIN), the International Standard Book Number (ISBN), or the ISO/IEC 15459 Unique Transport Unit ID.

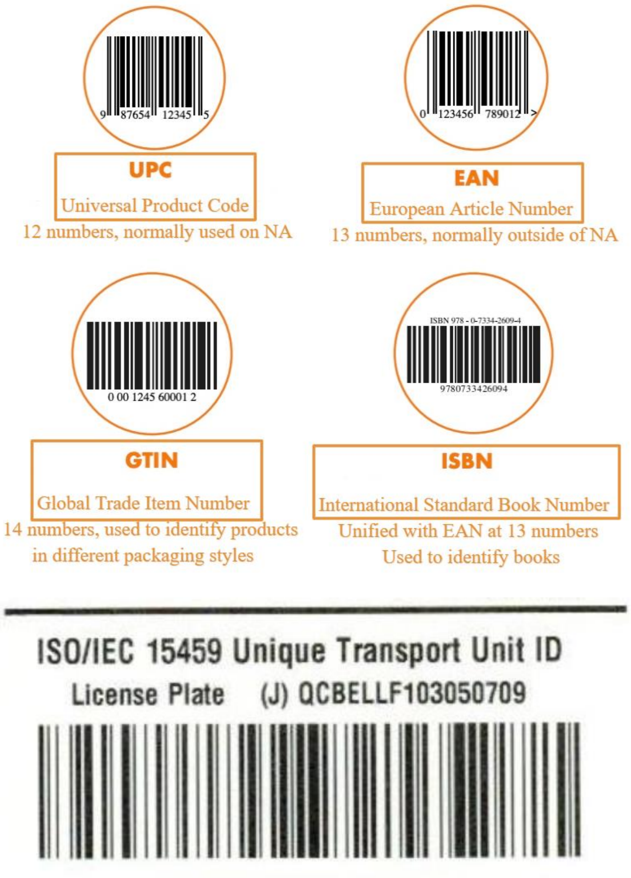

9 87654 12345 5
UPC
Universal Product Code
12 numbers, normally used on NA
0 123456 789012 >
EAN
European Article Number
13 numbers, normally outside of NA
0 00 1245 60001 2
GTIN
Global Trade Item Number
14 numbers, used to identify products in different packaging styles
ISBN 978 - 0-7334-2609-4
9780733426094
ISBN
International Standard Book Number
Unified with EAN at 13 numbers
Used to identify books
ISO/IEC 15459 Unique Transport Unit ID
License Plate (J) QCBELLF103050709

Figure 1: Widely used identifiers for products

12. It also must be possible to relate the product identifier to company identities, machine identities or human identities. This is necessary to e.g., identify a company that is responsible for and can be held liable for a product (identity).

13. Data that describes the product should be originated by its commercially responsible company.

14. The commercially responsible company must be able to manage the identifier.

15. The identity technology must be based on open standards and be applicable for various use cases and industries.

16. The barriers to use the worldwide unique identifier should be low.

17. It should be compliant to Gaia-X, which was also mentioned by Boris Böhme, Referatsleiter, Department Digitalpolitik of the German Ministry of Economic Affairs and Climate Action, on the first Cyberfrühstück about DPP of DIN on February 10th, 2022. Gaia-X was initiated to create a next generation European data infrastructure, i.e., a secure, federated system that meets the highest standards of digital sovereignty.

18. The information that the identifier leads to should be trusted and cryptographically verifiable

19. The product identifier must allow to collect life cycle information of the product.

20. No central look up components should be involved that lead to bottlenecks or allow (mass) data analytics.

II. Solution approach with decentralized identifiers

The identification technology that we propose for products is decentralized identifiers (DIDs) that are closely related with verifiable credentials (VCs), both standardized by the W3C. Using DIDs, product identifiers are not managed centrally by an organization (such as GS1) but in a decentral way by the product owner himself. Information that describes the product (also called subject) is issued by the product owner, audit organizations, or business partners in the form of electronically signed, trustworthy verifiable credentials or simple web links to additional resources.

For example, the manufacturer of a plastic part issues the plastic raw material code of the product as a verifiable credential. The verifiable credential is linked to the decentralized identifier of the plastic product. With this mechanism any product information can be linked to the plastic part.

Decentralized identifiers are often stored on distributed ledgers (DLT), such as Ethereum. However DIDs can also exist without blockchains, by using other trusted sources (such as a web domain, see `did:web`) to manage their DID documents. DID documents link to the storage location of the verifiable credentials (or web-based resources) that describe the DID subject further and most importantly contain the public key for electronic signature validation.

The string below is an example for a decentralized identifier. DIDs have the same syntax as URLs:

did:web:spherity-responder-pre-prod.wallet.us.spherity.io

DIDs start with did defining the URI scheme, followed by the DID method/namespace (here: `did:web`) followed by the DID method specific identifier, here the string “spherity-responder-pre-prod.wallet.us.spherity.io”. This string leads to a Spherity subdomain, where the DID document is stored and can be found under the well-known URL. The DID method specifies how the DID document is managed (e.g., created, found(resolved), updated or deactivated).

Excurse: Multiple DID methods exist. In other DID methods, such as `did:ethr,` the DID documents are stored on a distributed ledger (in this case Ethereum) and the identifier string is the public key of the DID.

The combination of the DID method and the method specific identifier ensure that a DID is globally unique, which leads us to our analysis of how decentralized identifiers fulfill the requirements of section A.

1. DIDs are globally unique.

2. The scalability of the solution will grow. Today most DIDs are resolved by the Universal Resolver which is not production grade. However, production grade solutions are offered by more and more suppliers, for example by Spherity.

3. DIDs can easily be encoded as QR code and when scanned

4. the QR code can show human readable information that does not require an internet connection and/or

5. lead to a URL.

6. The customer/user of the product passport would for any product have the same user experience, which is scanning in the QR code which leads him/her to more product information. This might require a dedicated application (see Section C).

7. Having a DID at hand, a search with a DID resolver will always lead you to the DID document of the product and thus to more information about it. DID resolvers can also be queried by APIs.

8. DIDs can be used for everything, also for products, pre-products, services, etc.

9. in all industries and

10. for all commercial sizes. Sometimes a DID is issued for a single product, sometimes for a product batch.

11. DIDs can be used as an abstraction level for already established identification schemes, such as GTINs, EANs, UPCs, ISBNs, or identifiers that conform to ISO/IEC (e.g., ISO 15459). We give an example of how DIDs can be related to GTINs in Section C.

12. Additionally, DIDs can be used for company identities so that products can be linked to the company that placed the product on the market. The Global Legal Entity Identity Foundation (GLEIF) is currently beta testing their DID/VC based verifiable LEI, other approaches foresee the binding of the company DID to a X.509 certificate or a GLN.

13. By issuing DIDs for their products, the commercially responsible companies can manage their products,

14. keep control about the product information and who accesses it. Also, fake products can be detected this way when a product identifier is not linked to a verified manufacturer.

15. The technology is completely based on standards. Additionally, the Gaia-X federation services will provide open-source reference implementations of all needed components to work with DIDs and verifiable credentials in 2022.

16. Thus barriers to use the technology will be low and

17. the interoperability to Gaia-X is ensured.

18. The signed verifiable credentials make product information verifiable and thus trusted. For more benefits of the decentral approach, please refer to "The product passport and its technical implementation" by Dr. Susanne Guth-Orlowski

19. In principle everyone can issue information about a given identifier. So also, consumers can issue product usage information during the product life cycle (please also refer to Section D).

20. Due to the decentral nature of the technology, no central components are needed. DID resolvers can easily scale and grow on the job as well as other technologies around them.

Of course, even though no central technical components are required, this approach needs a Governance that decides on standards, e.g. the description standards of the product such as the product circularity data sheet or the GS1 standards EPCIS & Core Business Vocabulary, the used encryption algorithms, the accepted company identification schemes and did-methods. One first example of such a governance is the Open Credentialing Initiative (OCI) that defines the standards for the pharmaceutical supply chain in the US to comply with the Drug Supply Chain Security Act (DSCSA).

III. Example implementation with GS1 digital link and DID binding

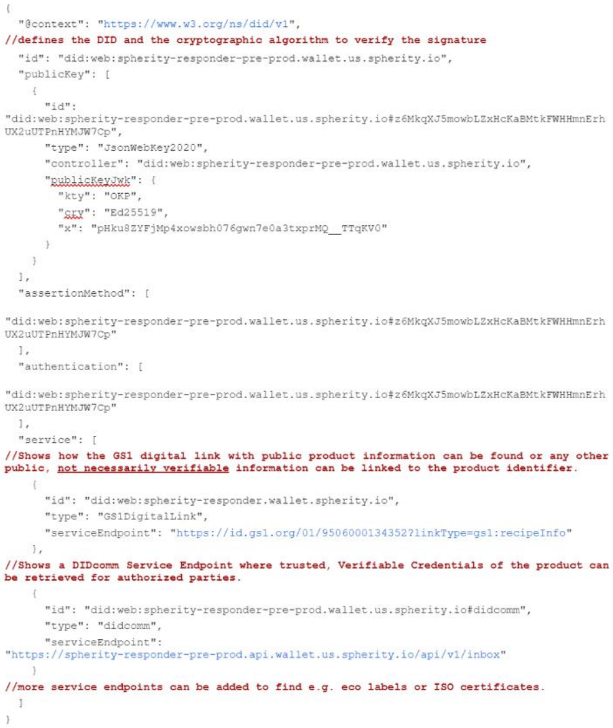
This section shows how decentralized identifiers can be linked to already established industry identifiers, such as (S)GTINs of GS1. The same principles can be applied to other widely used identifiers, such as International Standard Book Number (ISBN), ISO/IEC 15459 Unique Transport Unit ID, Universal Product Code (UPC), and many more. The decentralized identifier works here as an abstraction layer for existing identification standards.

What is special about the GS1 standard, is that to every GS1 identifier, there is already the possibility to register a GS1 digital link and define several link types that lead you to a web based product page. We will use the GS1 digital link in our example below.

To create a globally unique product DID, the manufacturer would use an open source or commercially available wallet. Using our DID example from above the DID document below is stored under the well-known URL of a web domain (not on a DLT / blockchain). It contains the DID, the cryptographic algorithms used and includes service endpoints where more information about the product DID can be found. It is the gateway and single source of truth to product information.

One service endpoint is the GS1 digital link which leads to more (public) product information. The second service endpoint leads to a protected storage for verifiable credentials. To receive those credentials, a requestor needs to be authorized to access the storage and send requests that are compliant to the DIDcomm protocol. Additional service endpoints can lead to other descriptions and certificates of the product, such as a digitally signed eco label by the ministry of environment or an ISO certification. The DID above described DID document has the following syntax.

Note: You can check out the DID document yourself by resolving the DID "`did:web:spherity-responder-pre-prod.wallet.us.spherity.io`" with the Universal Resolver or using the API of SURE (Spherity Universal Resolver for Enterprises).



```
{
  "@context": "https://www.w3.org/ns/did/v1",
//defines the DID and the cryptographic algorithm to verify the signature
  "id": "did:web:spherity-responder-pre-prod.wallet.us.spherity.io",
  "publicKey": [
    {
      "id":
"did:web:spherity-responder-pre-prod.wallet.us.spherity.io#z6MkqXJ5mowbLZxHcKaBMtkFWHHmnErh
UX2uUTPnHYMJW7Cp",
      "type": "JsonWebKey2020",
      "controller": "did:web:spherity-responder-pre-prod.wallet.us.spherity.io",
      "publicKeyJwk": {
        "kty": "OKP",
        "crv": "Ed25519",
        "x": "pHku8ZYFjMp4xowsbh076gwn7e0a3txprMQ__TTqKV0"
      }
    }
  ],
  "assertionMethod": [

"did:web:spherity-responder-pre-prod.wallet.us.spherity.io#z6MkqXJ5mowbLZxHcKaBMtkFWHHmnErh
UX2uUTPnHYMJW7Cp"
  ],
  "authentication": [

"did:web:spherity-responder-pre-prod.wallet.us.spherity.io#z6MkqXJ5mowbLZxHcKaBMtkFWHHmnErh
UX2uUTPnHYMJW7Cp"
  ],
  "service": [
//Shows how the GS1 digital link with public product information can be found or any other
public, not necessarily verifiable information can be linked to the product identifier.
    {
      "id": "did:web:spherity-responder.wallet.spherity.io",
      "type": "GS1DigitalLink",
      "serviceEndpoint": "https://id.gs1.org/01/9506000134352?linkType=gs1:recipeInfo"
    },
//Shows a DIDcomm Service Endpoint where trusted, Verifiable Credentials of the product can
be retrieved for authorized parties.
    {
      "id": "did:web:spherity-responder-pre-prod.wallet.us.spherity.io#didcomm",
      "type": "didcomm",
      "serviceEndpoint":
"https://spherity-responder-pre-prod.api.wallet.us.spherity.io/api/v1/inbox"
    }
//more service endpoints can be added to find e.g. eco labels or ISO certificates.
  ]
}
```

Figure 2: The product's DID document: A gateway to the GS1 digital link and verifiable credentials

Now, how do I get from the DID to the product information as an end customer? For this, the user needs a mobile app that is able to use the camera, scan in the QR code, read out the DID, send it to a DID resolver, receive the DID-document, find the GS1 digital link and open the product page in a browser. Alternatively, DIDs can be resolved by a web server that calls a resolver. With SURE, the Spherity Universal Resolver for Enterprises this 'deep link' looks as follows:

```
https://uni-resolver.spherity.io/1.0/identifiers/did:web:spherity-responder-pre-prod.wallet.us.spherity.io
```

Most mobile devices only support the latter today.

You could argue that we should use the digital link in the product QR code directly. True, but that only works for consumer goods that have a (S)GTINs and manufacturers that are GS1 customers. In the supply chain, though, we have many pre-products that do not have an (S)GTIN and use other identification schemes as mentioned above. Also, we believe that issuing identifiers by a central organization will be less needed in the future (see also: A primer for decentralized identifiers); with a wallet in your hand, you can create globally unique product codes yourself.

Finally, for very sensitive information, the second service endpoint can be contacted to receive signed verifiable credentials. For this the user app needs to be a full featured wallet that can communicate with a secured service endpoint (e.g. via DIDcomm), has the necessary access rights, that can ask for verifiable credentials, and that can verify their signatures / proofs. This is a built-in security layer which is required when it comes to highly confidential supply chain data that should only be accessible to authorized parties.

As an alternative, organizations that issue identification schemes, such as GS1, ISBN, ISO, etc. can create their own DID method that is optimized to their specific use cases. We could think of a GS1 DID method `(did:gs1:[gtin])` an ISBN DID Method (`did:isbn:[ISBN]`) or an ISO DID method (`did:iso-15459:[iso-15459]`), that return DID documents with DID-method specific service endpoints.

IV. D. Summary & Discussion

This section aims to summarize the benefits when using DIDs for product identification the future work that needs to be done and mention some projects that have used DID to identify IOT devices and products. **Benefits** in our view are:

- With DIDs the world would have a **standard entry point to product information** and respects already existing identifiers.
- Using a wallet, every commercial actor can **create and manage their own** globally unique product identifier. As mentioned above, free, open-source wallet reference implementations for all roles are currently developed by the Gaia-X project, which means that technical entry barriers will be low.
- Existing public product information is accessible in the same way as critical highly confidential product information which becomes **verifiable** and thus **trusted**.
- DIDs can be applied to all “things” that need to be identified and thus open up the potential application area to e.g., the **Smart Home, all supply chains and the Industry 4.0 sector.**
- Product DIDs can be connected to everything else, such as enterprise DIDs (e.g., a verifiable LEI or verifiable GLN) and have the potential to serve as a **basis for VAT or CO2 taxation.**

To walk towards DIDs as product identifiers, some **future work** is required:

- **Migration and integration efforts** are necessary to move from existing identifiers to DIDs or to integrate them into the existing landscape. The described concept is thus a long-term goal towards unified product identification. However, we assume that all technical components will be available as free, open-source components. For integrations into existing identity provider infrastructure, please refer to “On SSI-enabled IDP Solutions” by Carsten Stöcker.
- **Different DID methods** lead to different storage locations and management of DID-documents. Interoperability between various DID methods need to be made available by technology suppliers and in the long run by additional standardization efforts.
- **Costs** might occur for secure key generation of product keys. E.g., if the DID document of every product would need to be anchored to Ethereum this would cost approx. 1 USD per product / batch. This is not affordable for most serialized pharmacy products.
However, Layer 2 and other
scaling approaches marginalize those costs. Alternative solutions such as private-, consortia-, para chains can serve as a DID anchor as well and of course not using a blockchain at all (as explained in the example in this article with the `did:web` method) is an attractive solution.
- High available **resolvers** are needed for this solution approach. Next to the Universal Resolver, which is not production grade today, some companies (such as Spherity) already started product grade resolvers that are easily scalable.

For some aspects further concept work is needed, for example how to add **usage information** to a product. In the case of batteries, the state of health (SOH) needs to be added to the product records to later decide on their reusability. However, the user does not control the DID document of the battery, so how can a user issue Verifiable Credentials about the battery DID, for example for each storage procedure? One solution could be that the consumer receives a delegation key with limited rights to sign usage records in the form of verifiable credentials to the battery DID.

This solution has already been implemented and tested in the dena research project of the German Ministry of Economic Affairs and Climate Action, when implementing a machine identity ledger for smart meter gateways that issued metering records as verifiable credentials. Other projects, where DIDs have been used for "things" and products are:

The M-Trust project by Merck KGaA, enabling food product authenticity and product data transparency. It gives actors the possibility to access, attach and request data associated with a food product. Manufacturers, logistics providers, and suppliers always stay in control of their data and manage the access rights to it.

The Rail Chain Project funded by the German "Bundesministerium für Verkehr und digitale Infrastruktur (BMVI)". In this project, Spherity issued a DID for each intelligent train component which made them addressable and enabled communication among them in a secure way.

References

All refences can be found in the online version of this article at: https://medium.com/p/175ca455cee3

Acknowledgements

Thank you for contributing to this article, Dr. Carsten Stöcker, Nicolas Mietz, Ricky Thiermann, Sebastian Schmittner und Ralph Tröger.