iDunion

Empowering Sustainable Products and Consumer Confidence through Verifiable Credentials

– A Case Study on Digital Product Passport with GS1 Standards

Whitepaper

Version 1.01., 27.03.2023

Supported by:

Federal Ministry
for Economic Affairs
and Climate Action

on the basis of a decision
by the German Bundestag

Authors

European EPC Competence Center GmbH (EECC)

- Christian Fries
- Dr Sebastian Schmittner

GS1 Germany GmbH

- Dr Andreas Füßler
- Dr Paulina Drott
- Anna Klapper
- Dr Ralph Tröger
- Roman Winter

Robert Bosch GmbH

- Florin Coptil
- Werner Folkendt

SBB

- Cornelia Schalch
- Dominic Hurni

Siemens AG

- Marquart Franz

Spherity GmbH

- Dr Susanne Guth-Orlowski

As the paper describes work in progress, any feedback and exchange of thoughts to the approaches described are welcome.

To get in contact with IDunion in general: *https://idunion.org/start/kontakt/*.

Table of Contents

1 Motivation 4

2 Requirements 5

3 Relevant Terms 6

3.1 Self-Sovereign-Identity (SSI) 6

3.2 GS1 Digital Link (GS1 DL) 7

4 Customer & Participant Journeys – Use Cases 9

4.1 Customer Journey without Authentication 10

4.2 Customer respectively Participant Journey with Authentication 11

5 Technical Description 13

5.1 Product Verification – Issuing without Client Authentication 14

5.2 Accessing of Digital Product Passport with Client Authentication 16

6 Conclusion and Outlook 18

7 About IDunion 18

8 Annex 19

8.1 Sequence Diagram with User Authentication 19

8.2 Sequence Diagram Without User Authentication 20

1 Motivation

To meet the European Green Deal[1], it is crucial to embrace sustainability and circularity in the production and consumption of goods. The proposed legislations, the Eco-design for Sustainable Products Regulation (ESPR) (ESPR)[2] and the "new Battery Regulation"[3] provide the opportunity to drive this change by mandating the use of a digital product passport (DPP). This DPP shall help improve the sustainability, circularity, and resource efficiency of various product categories such as batteries, textiles, electronics, and buildings. To comply with the regulations, companies need to implement responsible corporate behavior throughout their global value chains.[4].

Companies must gain knowledge about the CO_2 emissions generated in supply chains, raw materials used, circularity potential and resource efficiency of products and components, and supplier's compliance with environmental, social, and governance (ESG) standards. This knowledge will help companies improve their activities in managing their supply chains and enable them to make more sustainable choices.

The ESPR mandates that information in the digital product passport must be verifiable, which creates a need for the industry to find solutions for providing (verifiable) digital product information. Companies need to develop innovative digital solutions that can provide reliable and verifiable data on product sustainability and circularity. These solutions should also enable the tracking of product information across the supply chain, making it easier for companies to make sustainable choices.

For product identification purposes, *the* well-established standard in industries like Fast Moving Consumer Goods (FMCG), Healthcare, Apparel or Do-It-Yourself (DIY) is the Global Trade Item Number (GTIN). In consequence, it is likely that the GTIN is applied for VCs in these industries as well. For that reason, the authors focus on the GS1 System in this paper. However, further approaches as proposed by association ZVEI (DPP4.0)[5] or solution provider Spherity[6] are not in focus of this publication to keep the paper in reasonable lengths.

The purpose of this paper is to delve into the potential advantages of integrating the established GS1 identification technology with the cutting-edge Self-Sovereign Identity (SSI) technology, specifically through the utilisation of Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). By exploring this topic, it is aimed to demonstrate how the current GS1 standards can facilitate the swift implementation of digital product information via the GS1 Digital Link, as well as how SSI technology can be leveraged to verify (and potentially certify) important product information in the digital realm. Ultimately, this paper seeks to showcase the synergistic benefits of combining these two technologies, highlighting how they can work together to enhance digital product identification and verification processes.

[1] EU 2020, https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en.
[2] EU 2022-1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0140&from=EN.
[3] EU 2022-2, https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/729285/EPRS_ATA(2022)729285_EN.pdf
[4] EU 2022-3, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1145.
[5] For example, the German ZVEI Association for the electro-technical industry has defined a path to the DPP based upon the Digital Name Plate 4.0 (DNP4.0). A description can be found at https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Technik/DMUEF/Vortraege2021/4-AS.html.
[6] Another approach, which abstains from ISO standardised identification schemes is described at https://medium.com/spherity/accessing-digital-product-passports-with-decentralized-identifiers-dids-175ca455cee3.

2 Requirements

As described in the ESPR, all product and operator identifiers should be globally unique and interoperable. The standard proposed by the EU commission is ISO/IEC 15459[7]. It is designed to guarantee interoperability of identification (in databases, registries, barcodes, RFID tags, labels, and on the web) across different sectors. ISO/IEC 15459 is the umbrella for all global identification schemes and serves all industries.

Further requirements are that all used identifiers shall need to function at the model-, batch/lot- or instance-level identification as well as be web-enabled. This means that any identifier that is physically placed on the product (e.g., in a 2D barcode) will act as a connection – also called data carrier – to access relevant data about that product on the web.

These requirements fit with the VC Data Model of the World Wide Web Consortium (W3C) recommendation for verifiable credentials, which requires that any identifier (credential ID, issuer ID, subject ID, etc.) has the syntax of a Uniform Resource Identifier (URI). The specific requirements for an identifier are that:

- "The ID property MUST express an identifier that others are expected to use when expressing statements about a specific thing identified by that identifier.
- The ID property MUST NOT have more than one value.
- The value of the ID property MUST be a URI." [8]

[7] See *https://www.iso.org/standard/54779.html*.
[8] *https://www.w3.org/TR/vc-data-model/#identifiers*

3 Relevant Terms

For a better understanding, the two core terms SSI and GS1 Digital Link are briefly explained below.

3.1 Self-Sovereign-Identity (SSI)

SSI stands for a technology approach that allows to keep control over the data that describes information relating to an identified natural person, such as ID card, driver's licence, or diploma and also to enable legal entities to issue credential for products such as carbon footprint. That means, instead of providing personal data to various central platforms, users authenticate and authorise themselves using VCs from their SSI wallet and present those to platforms or other actors on request. The basic functionalities and typical process steps are visualised in figure 1.

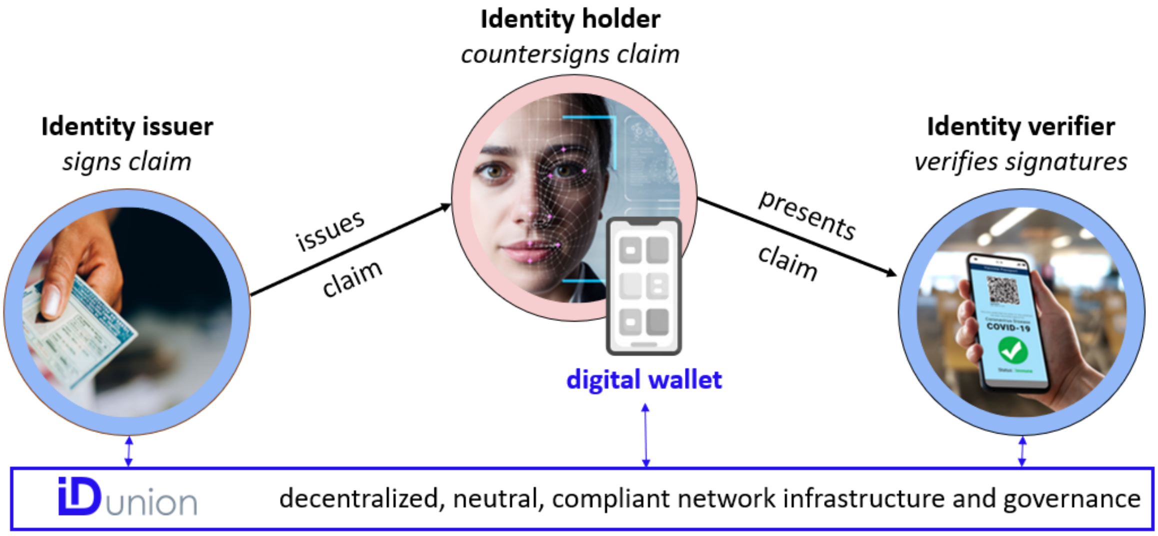


Figure 1: Typical process for Verifying Credentials Using SSI Technology

In this paper, we use this concept not only for describing the identity of a natural person, but also the ones of a legal person and products manufactured by both. SSI seems to be a promising approach as

- it is based on interoperable decentralised infrastructures run by multiple entities e.g., IDunion S.C.E.[9].
- it provides a decentralised infrastructure that holds only metadata of DPP and serves as trust anchor to verify content of DPP e.g., issuer or form to describe a product.
- it is easily accessible over multiple providers of access tools so called "agents" to connect with decentralized infrastructures.
- no central system needs to be built, maintained, and further developed to exchange data.
- it enables the verification of product information by cryptographic signatures, which could increase trust in DPP data.
- it creates accountability for the issuer for the data that it claims for a company or a product.
- it allows for business confidentiality. The access to data that supply chain actors share could be reduced to a minimum. The sharing conditions remain under their control, and
- it facilitates interoperability among participants by e.g., using standard exchange protocols.

[9] See https://idunion.org/2022/08/16/idunion-announces-successful-establishment-of-european-cooperative/?lang=en.

- it keeps the barrier to participate at the ecosystem low, as open-source implementations are being made available through e.g., the Gaia-X Federation Services[10].

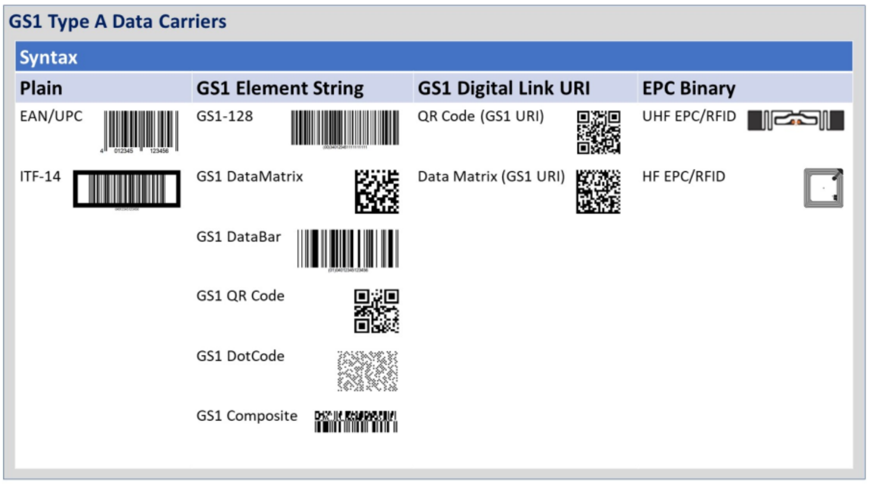
A **verifiable credential** is a set of tamper-evident claims and metadata that cryptographically proves who issued it. Verifiable credentials can be used to build verifiable presentations, which can also be cryptographically verified. A **verifiable presentation** shows data from one or more VCs on demand to the requester.

3.2 GS1 Digital Link (GS1 DL)

Depending on the area of application and business needs, GS1 identifiers can be expressed in various encodings. For instance, most pharmaceutical products carry a GS1 DataMatrix which encodes the GTIN along with a number of attributes (e.g., expiry date, batch/lot, and serial number) in the form of 'GS1 Element Strings'. In addition to an optical data carrier, many companies in e.g., the apparel sector require a serialised GTIN to be encoded onto UHF EPC/RFID tags as 'EPC Binary Strings'. And for FMCG trade items, the most prominent and commonly known application is the EAN/UPC barcode, which encodes the GTIN in 'Plain' syntax (figure 2).

A further syntax form to represent GS1 keys and related attributes is a GS1 Digital Link[11] URI (figure 3), often encoded in a QR code on product packagings. If needed (depending on the respective use case), all syntax forms mentioned in the first paragraph can be converted into a GS1 Digital Link URI though, too.

To enable the latter, GS1 Element Strings are embedded in a URL (a GS1 Digital Link URI). The (already existing) identifiers encoded in the QR code can then be linked to and from (see figure 3). For constructing GS1 DL URIs, any domain can be used – the company's own domain as well as 'id.gs1.org'. The advantage of using the latter ('canonical') GS1 Digital Link domain is that in case of acquisitions or else, GS1's resolver can redirect to web resources of the new licensee without needing to change the original URI.



GS1 Type A Data Carriers

Syntax

Plain	GS1 Element String	GS1 Digital Link URI	EPC Binary
EAN/UPC	GS1-128	QR Code (GS1 URI)	UHF EPC/RFID
ITF-14	GS1 DataMatrix	Data Matrix (GS1 URI)	HF EPC/RFID
	GS1 DataBar		
	GS1 QR Code		
	GS1 DotCode		
	GS1 Composite		

Figure 2: GS1 Data Carriers Overview

[10] See https://www.gxfs.eu/.

[11] https://www.gs1.org/standards/gs1-digital-link

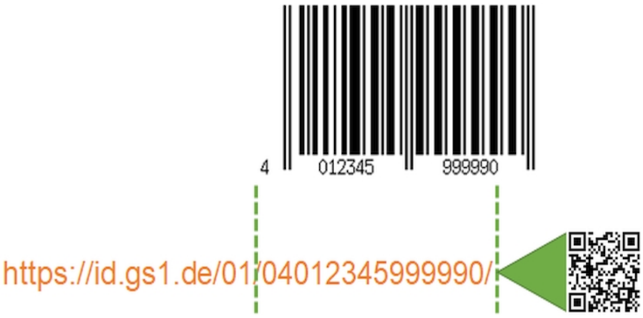


Figure 3: Embedding the GTIN into a GS1 Digital Link URI

In addition, the GS1 DL does not denote a syntax only (i.e., the GS1 Digital Link URI), but comprises several other layers that deliver an entire ecosystem, namely:

- link types[12] (i.e., labels characterizing related web resources),
- GS1 DL resolvers (services that connect a GS1-identified entity to one or more online resources that are directly related to it), and
- linked data (i.e., facilitating knowledge graphs when combined with Linked Data Vocabularies such as schema.org[13] or the GS1 Web Vocabulary).

For the use of a GS1-compliant Digital Link, a resolver service is required so that the GS1 Digital Link can not only refer to one website, but also to different online content, in a wide variety of formats and languages. The fundamental aim of GS1 Digital Link is to enable anyone to find answers to their questions about their products in front of them. Depending on which application or context, the appropriate information is returned.

A GS1 Digital Link resolver provides the connections between the identifier and one or more sources of information about it. None of the actual information is stored in a GS1 Digital Link resolver, just the target URLs to related online resources along with some descriptive attributes (e.g., link type[14], language and content type).

For detailed information on GS1 Digital Link, GS1 provides technical standards, an implementation guideline, tutorials, and further collateral. In addition, there are also a number of related open-source initiatives, published under a permissive licence on GitHub.[15] Though applicable for GS1 keys only, note that GS1 DL supports all GS1 keys, which in turn cover a wide range of business applications beyond the identification of products (e.g., physical locations, assets, parties, documents, service relations, etc.).

The next sections aim at exploring the technical feasibility of combining the SSI concept for products with existing GS1 Standards based technology.

[12] See *https://www.gs1.org/voc/?show=linktypes* for a list of all link types standardised so far.
[13] *https://schema.org/*.
[14] Link types are standardised terms to help humans and machines to find the very information resource(s) they are looking for.
[15] See *https://github.com/gs1*.

4 Customer & Participant Journeys – Use Cases

For supporting a better understanding of the various applications of the SSI approach in combination with the GS1 Digital Link, in this chapter different use cases during the customer journey[16] and actions performed by several parties are mapped as customer and participant journeys. For providing a recurrent theme the purchase of an electric screwdriver is used.

Not all data-related use cases require the same level of trust or depth of information. For instance, trading partners and consumers may demand a way to reliably ascertain whether a given carbon footprint certificate is genuine, while the same is typically not required for resources such as promotional videos, washing instructions or disposal information.

As an orientation guide, table 1 comprises a non-exhaustive list of web resources that may or may not require a high level of trust. Some of them may be considered differently depending on the respective conditions, regulatory or customer requirements prevalent in a given industry sector.

Table 1: Level of trust related information

Low(er) level of trust (primarily public information)	High(er) level of trust (primarily restricted information)
Product Information Page (e.g., carbon efficiency)	Certificate (e.g., carbon footprint), warranty)
Related video	Repair service
Promotion	Raw material certificates
Nutrition information	Remanufacturing-relevant information
Authenticity check	Legally required information by authorities
Manual	
Recipe	
Social media channel	
Frequently asked questions	

Depending on the required level of trust, use cases can be distinguished as follows:

- High trust use cases
  The reveal of information is based on a verifiable presentation using a trust infrastructure. In this case, a wallet is recommended to store additional information required for trusted processes.[17]
- Low trust use cases
  The reveal of the information is public. In this case, no wallet is required.

In the first case, the data is requested by the verifying party via a proof request and explicitly revealed through a verifiable presentation.[18]

Let's assume customer Jo wants to install a floor in her loft. For this purpose, she wants to buy a new electric screwdriver. Technically, there are two distinct ways how Jo could get digital product information of electric screwdrivers currently on the market. In both scenarios, the digital product passport (DPP) is issued in the form

[16] Lemon, K.N., Verhoef, P.C. (2016), Understanding Customer Experience Throughout the Customer Journey, https://doi.org/10.1509/jm.15.0420.

[17] The type of credentials which can be used are AnonCreds or W3C Credentials. A choice should depend on the use case requirements.

[18] In low trust use cases only, the credential might be verified. The presentation might be optional to avoid additional effort the required interaction with the issuer would afford.

of VCs.[19] Some attributes of the product passport might be shared for multiple product categories, while most are product category specific. The credential schemas are defined accordingly for the shared and individual properties following the proposal regulation for each product category: batteries, textiles, electronics, etc. The data from the product pass credential(s) contain the required information to assemble the DPP. The product passport proposed in section 4.1 is fully public and easily accessible. That's the first technical solution. In section 4.2, the second technical solution with a slightly different architecture requiring a user with more competence in SSI technology to authenticate towards the product information provider in order to obtain access to restricted fields of the DPP which are not fully public, is explained. The scope is also broadened beyond the end customer.

4.1 Customer Journey without Authentication

At the store, Jo scans the QR codes[20] on several electric screwdrivers that contain GS1 Digital Links to retrieve corresponding public information. Both, the domain of the resolver and the GTIN of the screwdriver are embedded in such a GS1 Digital Link (e.g., *https://id.gs1.de/01/04012345999990/10/20210401-A/21/XYZ-1234*[21]). The GS1 resolver service resolves the request and forwards it to an onward destination specified by the brand owner. Adding a verifiable Digital Product Passport, i.e., one built from verifiable credentials, enhances those already established features of a digital link alone:

- Purchase: Authenticity and certificates check by the customer at retail for making a responsible purchase decision

  At the retail store, Jo wants to make sure that her screwdriver of choice possesses the quality she ought to buy. By scanning the GS1 Digital Link in the QR Code, she is redirected to the product page of the cordless screwdriver via the GS1 resolver. The information[22] is provided by the manufacturer as digitally signed credentials and is available on the product web page. Adding digitally signed credentials about the product enhances trust and credibility of that information, in particular if certificates are issued by third party auditors, e.g., Technischer Überwachungsverein (TÜV). Jo can make sure that the manufacturer has authorised the retailer for sale or verify the serial number to ensure that she is looking at a genuine product. And she can be sure that, for example, a certified raw material origin has actually been certified by a trusted authority, or that the screwdriver is repairable and has a low ecological footprint besides offering the desired torque moment and power supply characteristics.

- Post purchase: Accessing product data from home

  After buying the screwdriver, Jo wants to start laying the floor right away. But which is the best tool to use for tightening the screws in her use case? Via the GS1 Digital Link she can quickly navigate to the relevant technical information or a DIY tutorial via the product information page. By going through the verifiable product page, she can be sure that the manufacturer authorised those instructions rather than just following some layman's advice from the internet.

- Post purchase: Warranty case

  After Jo laid a part of the floor, the screwdriver shows an unexpected malfunction. As this has happened within the warranty phase, the whole process of warranty handling can be digitized in a trustworthy, yet data-minimal way.[23] VCs can in this setting be used to build trust in multiple ways. The simplest one being the identification of repair shops in Jo's vicinity that are certified by the manufacturer to conduct the

[19] For a description of the concept of VCs in German see *https://idunion.org/2022/06/02/digitale-selbstbestimmte-identitaeten/*.

[20] From today's perspective a QR code is the most likely kind of Matrixcode to be used.

[21] Example of the encoding into a QR code:

[22] E.g., manufacturers description of the screwdriver, general, technical, and ecological product information, safety data sheets.

[23] There is an online demonstration with details for handling the warranty case to be found at *https://demonstration-ssi.gs1-germany.de/*. The technical setting here is closer to the one envisioned in section 4.2.

necessary repairs/replacement. Information about the warranty handling is an example of a new service which can be added to a digital product passport that requires a trust relationship.

4.2 Customer respectively Participant Journey with Authentication

Not all information about products can be shared publicly. In addition to the user verifying information about the product being trustworthy and authentic, the information provider (manufacturer) might want to authenticate requester and only gives the details of the DPP to authorised parties, such as border control. Furthermore, the DPP might offer additional services to authorised users.

In this scenario, it is assumed that Jo uses an SSI Wallet, e.g., in the form of a smart phone app, which she can use to receive, hold, and present verifiable credentials.

It is at the manufacturer's discretion which additional services are supported for the respective product.

- Post purchase: Online purchase warranty case

  In case Jo has bought the screwdriver from an online marketplace instead of the retail store, Jo receives a proof of purchase in the form of a VC into her wallet. This credential issuance can be initiated via email, web shop, or by scanning a suitable QR Code.[24] The advantage of using digital certificates is that the manufacturer can verify the purchase without directly talking to the seller about Jo. All information exchange is user-centric controlled by Jo herself who can make sure to reveal only the data needed for the use case (e.g., purchase date but not price).

  In the case of the broken screwdriver during the warranty phase, Jo would make use of the online warranty service of the seller and sends her request for warranty. Having the required data at hand, the online store having no repair workshop would decide to replace the screwdriver, inform Jo about the decision and procedure, and finally supply the new screwdriver to Jo.

  Once the screwdriver has been delivered, Jo would like to receive the warranty certificate into her wallet. To accomplish this, she scans the QR code on the new screwdriver. Technically, this initiates a credential exchange between her wallet and the wallet of the manufacturer. Jo is asked to present the proof of purchase and receives the warranty certificate. The warranty certificate is an example of a digital document with an embedded service. A warranty case can be opened directly via a link in the warranty certificate.

Apart from the end consumer scenarios of Jo the accesses to the information can be granted to any actors along the value chain: distributors, public authorities, repairers, remanufacturers, or recyclers.

- Prepurchase: CO_2 evidence provided by manufacturer

  Companies, customers, customs, or other public authorities need to verify specific information about products, for example the CO_2 footprint. To access business sensitive or highly detailed information that the manufacturer does not want to share publicly, the requesting party needs to be authorized. This is the main difference between this DPP use case and the ones presented in section 4.1.

  Via e.g., scanning a suitable QR code, the public authority's wallet establishes a connection to the manufacturer's wallet and the authority presents proof of her authorization. She then requests the screwdriver's CO_2 certificate (in form of a verifiable credential proof request). If the manufacturer is satisfied with the authority's proof, he will present the requested CO_2 certificate, which can be issued by himself, a supply chain partner, or an auditor.

  In this use case, the manufacturer maintains self-sovereign control over his product data, carefully identifying requesting parties and only sharing sensitive information upon authorized request.

- Repair process

  After a few months, the screwdriver suddenly stops working again. Jo checks her wallet and realises that the warranty is still valid and has not been revoked by the manufacturer. Jo can now trigger a warranty claim

[24] For a demonstration of the QR Code Scanning flow, see https://demonstration-ssi.gs1-germany.de/.

directly via the warranty certificate. The repairer shop proves to Jo that it is authorized for handling warranty cases by showing a suitable certificate to Jo and in turn asks Jo to provide proof of warranty by showing her credential. After Jo provides this information, the repair service provider repairs the product concluding the warranty case. Again, Jo has full control of the information flows by showing information from her certificates only upon authorized request to trustworthy counter parts.

- Post purchase: Raw material validation by manufacturer

  Jo has used the screwdriver for several years and it is beyond repair. Therefore, she brings the screwdriver to a local recycling centre.

  Before disassembling, the screwdriver for separating and recovering the different raw material, the recycler requires access to the raw material data of the screwdriver. For that purpose, the recycler scans the QR code on the screwdriver, establishes a connection to the manufacturer's wallet and requests the "raw material information" in form of a proof request. To provide the raw material data, the manufacturer requires proof from the recycler (e.g., organisation identification plus additional information proving that this organisation is a recycler). After the recycler provides this information, the manufacturer's wallet validates the information and provides the requested data.

- Circular Economy: Need for Information by remanufacturers

  Remanufacturers or other actors in post/prepurchase cycles[25] require specific information about the initial intermediates and their products. For that purpose, they scan the QR code of the product, establish a connection to the manufacturer's wallet and request the needed 'information' in form of a proof request. To provide this specific information, the initial manufacturer requests proof from the remanufacturer (e.g., organisation identification plus an explanation for the reason of the need for specific information). After the remanufacturer provides this information, the manufacturer's wallet validates it and exchanges the requested data.

[25] See "The Butterfly Diagram: Visualising the Circular Economy", https://ellenmacarthurfoundation.org/circular-economy-diagram.

5 Technical Description

In the design of using verifiable credentials (VCs) to certify product attributes as deployed in this paper, each unique model-, batch/lot- or instance-level of product must have its own URI. The products of concern are not active[26] and have no own wallet. The subject of a verifiable credential (see VC Data Model[27]) needs to be a URI, preferably resolvable. To this end, a URL form of an identifier, such as the GS1 Digital Link, is well suited as the subject ID of a verifiable credential.

A product is identified via a GTIN, embedded in a GS1 Digital Link URI, combined with a batch/lot or serial reference, if applicable. On this basis, a GS1 Digital Link resolver can point to a VC-capable resource (compliant with the W3C data model[28]) comprising the DID of the product or company responsible for the product.

The attempt here is to provide these verified attributes in the first place, e.g., via verifiable credentials, and secondly to make those detectable which are related to the product by resolving the GS1 Digital Link. This effort can be described by the following questions:

- Where are verifiable credentials about product data stored?
- How can a party access/query the credentials associated with a product/ID?
- How can information flow be controlled as every supply chain partner issue a VC for his process step?
- How are product data from multiple issuers linked in VC with each other without using a central platform and only using a single access point (URI)?

The proposed technical solution in this paper for creating DPPs is

- product-independent, meaning it can be applied to any product, regardless of its type or packaging.
- also technology stack and network independent, meaning a digital product passport is designed to work with a wide range of devices and platforms. By choosing a semantic and interoperable stacks and networks a full leverage of scalability potential in data exchange can be offered.
- trust infrastructure independent, means that it can operate without relying on any specific trust ecosystem. Instead, it is designed to be interoperable with different trust infrastructure.
- offers flexibility in defining future additional services (endpoints) supported by the holder.

To illustrate this approach, we used

- a screwdriver as a sample product
- on-chain solution over IDunion network or off-chain over an external storage for schema definition
- the IDunion SSI-network as a trust infrastructure to identify individuals, organisations, and devices, that interact with each other to establish and maintain trust.
- different service endpoints based on the level of trust, see table 1.

To define the DPP according to the business steps, the following technical steps are required:

1. The ESPR defines the necessary attributes of the DPP. To comply with specific regulatory proposals (e.g., EU sustainability strategy, product regulation, corporate sustainability (due diligence), EU Critical Raw Materials Act[29]), the attributes of the credential schema can be defined and made available in the business ecosystem.
2. The manufacturer prepares the attributes according to the relevant legislation. Moreover, the manufacturer can provide additional services for the product and make these services available through the DPP (e.g.,

[26] In the sense of not having an own energy source for actively starting data exchange by their own.
[27] https://www.w3.org/TR/vc-data-model/#identifiers.
[28] See https://www.w3.org/TR/did-core/#data-model.
[29] See https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13597-European-Critical-Raw-Materials-Act_en.

Digital Twin Information). This can be achieved by publishing the credential definition or defining a new credential based on the selected scheme.

3. The manufacturer introduces the product into the market (directly or through the economic operator) by issuing a VC for the product according to the credential definition and making it available for the product in a visible form (e.g., in form of a QR Code).
4. Once the product is introduced into the market, stakeholders can access the production information of the DPP, as described in the detailed use cases in Chapter 3.

By following these technical steps, companies can implement a standardized DPP that is compatible with the EU's regulations, while also providing valuable information to stakeholders about the environmental impact and sustainability of their products.

As already described in the customer journey above, the basic paths with and without user authentication are described technically in detail in figure 4 and in the following paragraphs.

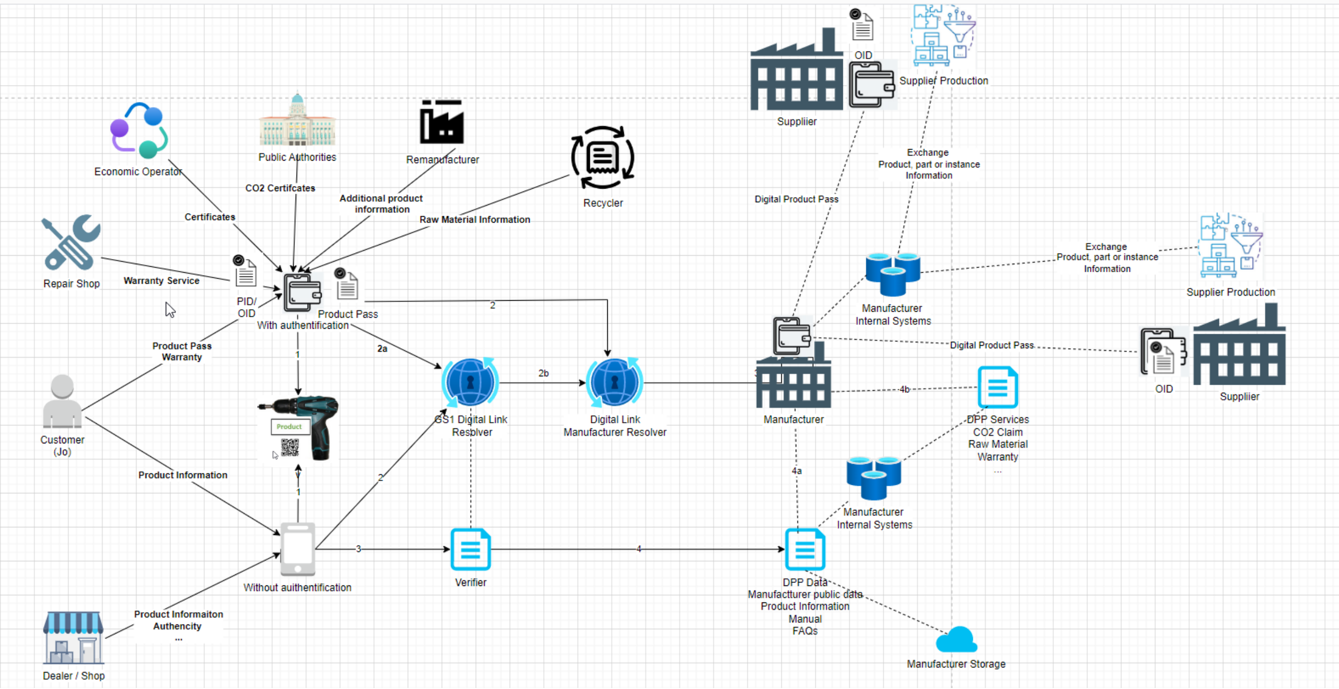


Figure 4: Technical approach overview

5.1 Product Verification – Issuing without Client Authentication

A user can make use of a GS1 Digital Link request to access verifiable data by appending the GS1 Digital Link URI with an appropriate 'Link Type' (yet to be standardised). The verifier, who could be hosted by an arbitrary trusted party, manages the credential and verification handling. The functionality of the verifier mainly consists in resolving the credentials the product identifier (the GS1 DL) is subject to and verifying the retrieved credentials.

In our case, there are two different types of credentials, the W3C verifiable credentials and Anonymous Credentials (AnonCreds) from the Hyperledger Indy ecosystem. In practical applications, these two differ mostly in the way a subject is bound to them. While in the W3C case the subject is publicly present within the credential by its identifier, this is not the case for AnonCreds where the subject of the credential explicitly equals the holder. Therefore, the course of action differs likewise:

For verifying an AnonCred, an interaction (DIDComm) with the credential holder or issuer is required in case the holder does not possess a DID as the subject of the credential could be a GS1 Digital Link. Hence, verifying an AnonCred involves a present proof request to the manufacturer wallet (5b in figure 4), which then actively verifies the claim about the identifier.

W3C verifiable credentials (5a) need to be discovered referencing the requested product identifier by querying various registries (e.g., dedicated services (API), federated registries (IPFS) or distributed registries (DLT)). After getting hold of the credentials, they can be verified locally due to their zero-trust architecture.

While for the W3C approach the verifier is a convenience feature, as the entire verification could be done locally by the client in a wallet-less fashion, it is mandatory for verifying AnonCreds as this process involves a wallet-to-wallet interaction, i.e., requires the (DID) wallet provided by the verifier.

The process can be illustrated by the following example flow of actions (see figure 5) referring to our protagonist Jo from the user journey above:

1. Jo wants to retrieve public information about a screwdriver.
2. To do this, she uses her mobile phone camera to scan a QR code decoding the embedded GS1 DL.
3. Both the domain of the GS1 DL Resolver as well as the GTIN of the screwdriver are embedded in the GS1 DL URI.
4. Jo’s scan triggers a GS1 DL request which routes her to an online resource (e.g., a product information page) specified by the brand owner. If provided by the manufacturer, a selection of further information is available to the customer on the product information page. This can be a FAQ site, a video, or a verifier service. By selecting the verifier service on the product information page, she gets to the DPP frontend from the verifier service.
5. The verifier collects the relevant VCs and all necessary information to verify those (this could be DID documents of issuers, schemas, and context files).

   5a. W3C: VCs and corresponding context are fetched from a (public) internet resource. In the W3C case the verifier is optional as the credentials can be verified locally even without a wallet.

   5b. Indy: VCs are fetched via a proof request from the relevant holder wallet, schema (credential definition) and DID documents from the Indy Ledger. The counterpart has to answer and verify the credential to deliver the proof of the proof request.
6. The product information and VC for the screwdriver are processed by the DPP frontend into a human-readable page.
7. Users like Jo can view the verified and certified product information on their mobile phone.

The described process flow based upon zero trust W3C credentials has been implemented in a demonstration case.[30] It aims to practically experience the technology of VCs.

[30] Access the demonstration via *https://id.gs1.de/01/04012345999990/10/20210401-A/21/XYZ-1234*.

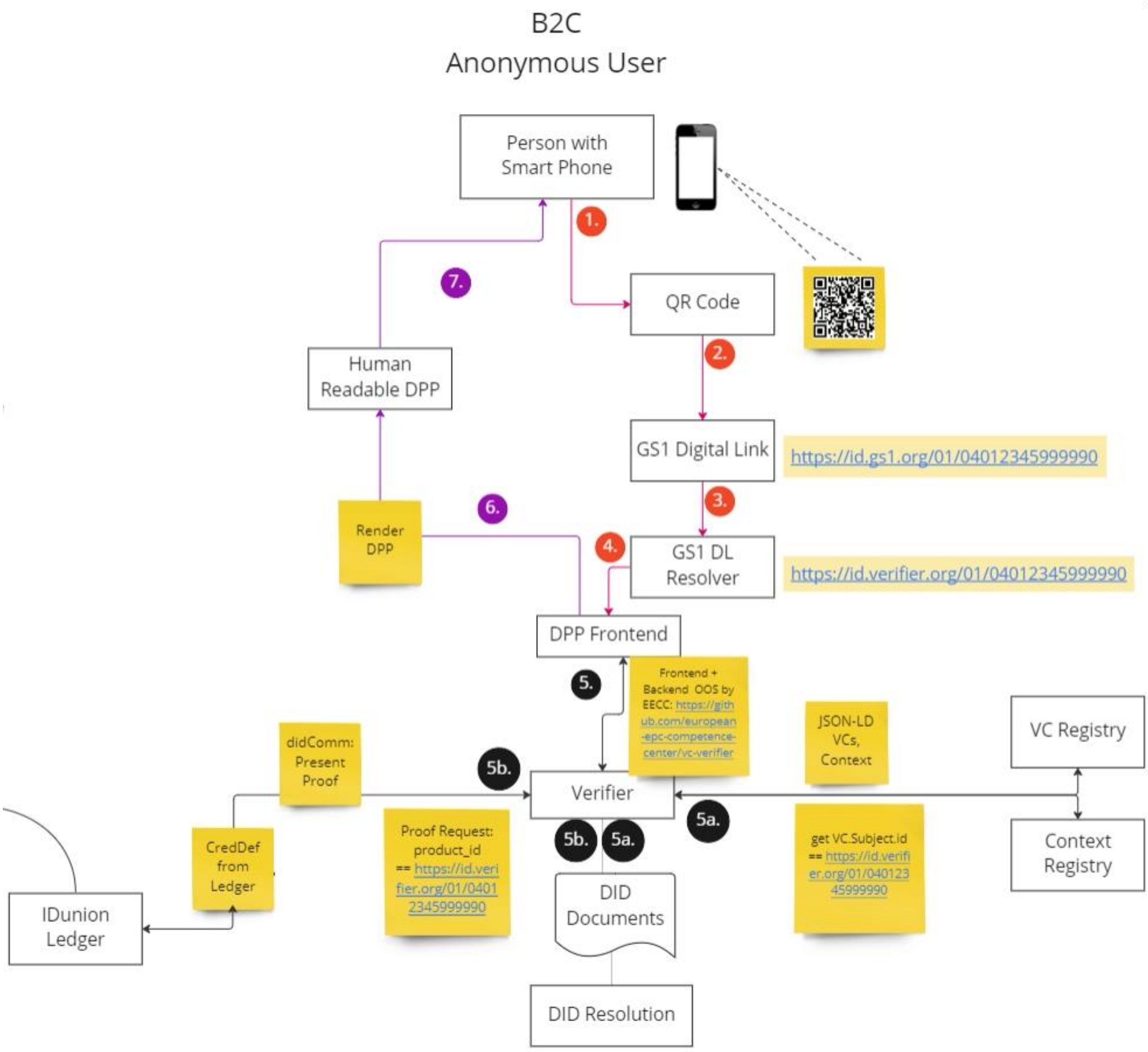

B2C
Anonymous User
Person with Smart Phone
1.
QR Code
2.
GS1 Digital Link
https://id.gs1.org/01/04012345999990
3.
GS1 DL Resolver
https://id.verifier.org/01/04012345999990
4.
DPP Frontend
5.
Frontend + Backend OOS by EECC: https://github.com/european-epc-competence-center/vc-verifier
6.
Render DPP
Human Readable DPP
7.
Verifier
5a.
5b.
JSON-LD VCs, Context
VC Registry
Context Registry
get VC.Subject.id == https://id.verifier.org/01/04012345999990
DID Documents
DID Resolution
didComm: Present Proof
Proof Request: product_id == https://id.verifier.org/01/04012345999990
CredDef from Ledger
IDunion Ledger

Figure 5: Process Chart Product Verification without Client Authentication

5.2 Accessing of Digital Product Passport with Client Authentication

The digital product passport (DPP) created by the manufacturer will provide access to all relevant and verified information about the product for customers, economic operators, and competent national authorities. Additionally, customers will be able to access product-related services for the products they own or want to buy/rent. The DPP will also be accessible to all actors along the value chain, including economic actors, end-users, distributors, repairers, remanufacturers, recyclers, and authorities, as defined by Article 7/8 of the Digital Product Passport Regulation.

The process can be illustrated by the following example flow of actions (see figure 6):

1. The requestor scans the QR code of the product with a wallet (e.g., Lissi wallet as a mobile solution or organisation wallet as an enterprise solution).
2. A GS1 Digital Link URI is encoded in the QR code. The request is forwarded to a GS1 Digital Link resolver and forwarded to the registered manufacturer depending on the manufacturer-specific option. The GS1 Digital Link is resolved and forwarded to the registered endpoint (manufacturer’s wallet).

3. The manufacturer wallet generates an invitation and sends it to the requester. The requester opens the invitation, reviews the information, and accepts it.
4. The manufacturer’s wallet transmits the product passport entitlement via the established channel.
5. The requestor can solicitate specific information/services (e.g., CO_2 certificate, raw material information, warranty claim, repair claim, etc.) through the open channel with the manufacturer.
6. The manufacturer wallet generates a verification request to prove the identity of the requester. The requestor must present the requested information in form of credentials, e.g., personal identification (PID), organisational identification (OID), additional use case specific credentials (e.g., proof of purchase, recycler certificate from authorities).
7. The manufacturer wallet validates the credential and generates the requested information in the form of credentials. Through the established channel, the requester can have peer to peer communications without a central entity. An example would be transparent information in form of a notification sent directly to the requester’s wallet about the status of the complaint (such as product/request received, request in process, etc.).

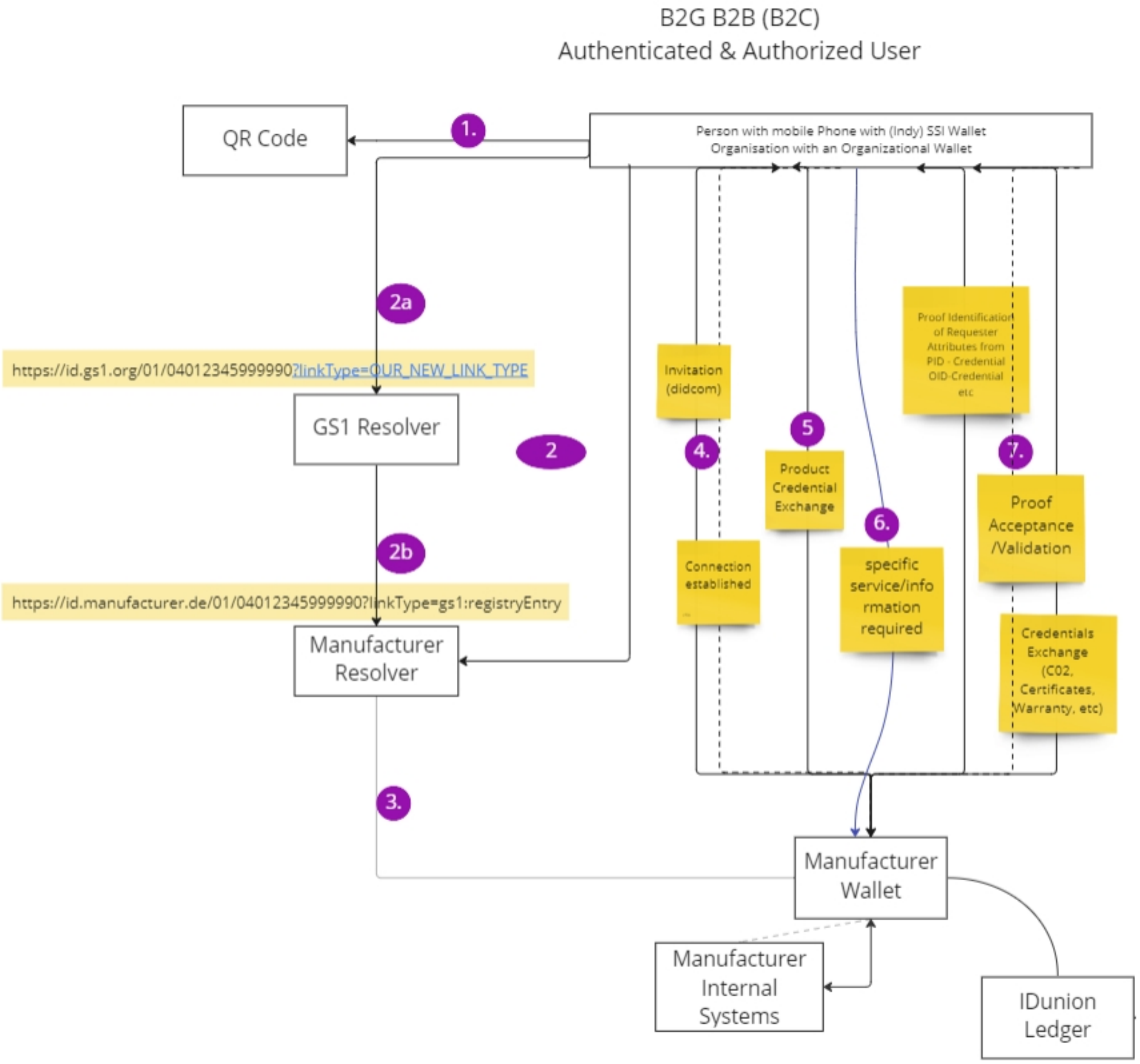

B2G B2B (B2C)
Authenticated & Authorized User
QR Code
1.
Person with mobile Phone with (Indy) SSI Wallet
Organisation with an Organizational Wallet
2a
https://id.gs1.org/01/04012345999990?linkType=OUR_NEW_LINK_TYPE
GS1 Resolver
2
2b
https://id.manufacturer.de/01/04012345999990?linkType=gs1:registryEntry
Manufacturer Resolver
3.
Invitation (didcom)
4.
Connection established
5
Product Credential Exchange
6.
specific service/information required
Proof Identification of Requester Attributes from PID - Credential OID-Credential etc
7.
Proof Acceptance /Validation
Credentials Exchange (C02, Certificates, Warranty, etc)
Manufacturer Wallet
Manufacturer Internal Systems
IDunion Ledger

Figure 6: Process Chart Product Verification with Client Authentication

6 Conclusion and Outlook

As demonstrated in the previous sections, a variety of use cases for commercial procedures can potentially be enhanced using verifiable credentials. Such commercial procedures have manifold requirements, one of them is to get a smooth integration into current product identification and ecological product information verification processes for achieving the European Green Deal. Established standards, as the GS1 standards, may function as a basis to implement verifiable credentials-based solutions under current industry circumstances on product level. In this sense, established standards could work as an accelerator for implementation of new technologies which are particularly required for scaling the DPP in FMCG, Healthcare, Apparel or DIY industries.

The technological development of VCs is progressing rapidly, and potentials arise for various industries. This white paper is meant to inform interested readers and support their decision making.

Beyond this paper the partner organisations within work package 10.5 of the IDunion project work together to validate the findings via POCs respectively demonstrators and prototypes.

7 About IDunion

This paper was created by partners of the IDunion project. The IDunion research project is funded by the Federal Ministry for Economic Affairs and Climate Action as part of the Secure Digital Identities Showcase programme. The objective of the research project is to build an innovative secure infrastructure, which enables the verification of data and is based on a jointly operated decentralized database.

The Project's Technical Network has been set up by a cooperative of private companies, associations, government institutions, educational bodies, and other legal entities. Given this range of involved participants, several different use cases are now being tested in various pilot implementations within the IDunion research project, with the necessary software components being provided by the partner companies within the consortium. It also meets all the requirements in terms of data location strategy, keeping the core competence at the European level, while it can be used on an international scale. For more information about IDunion, please visit the project website[31].

[31] https://idunion.org/.

8 Annex

8.1 Sequence Diagram with User Authentication

- Verification process

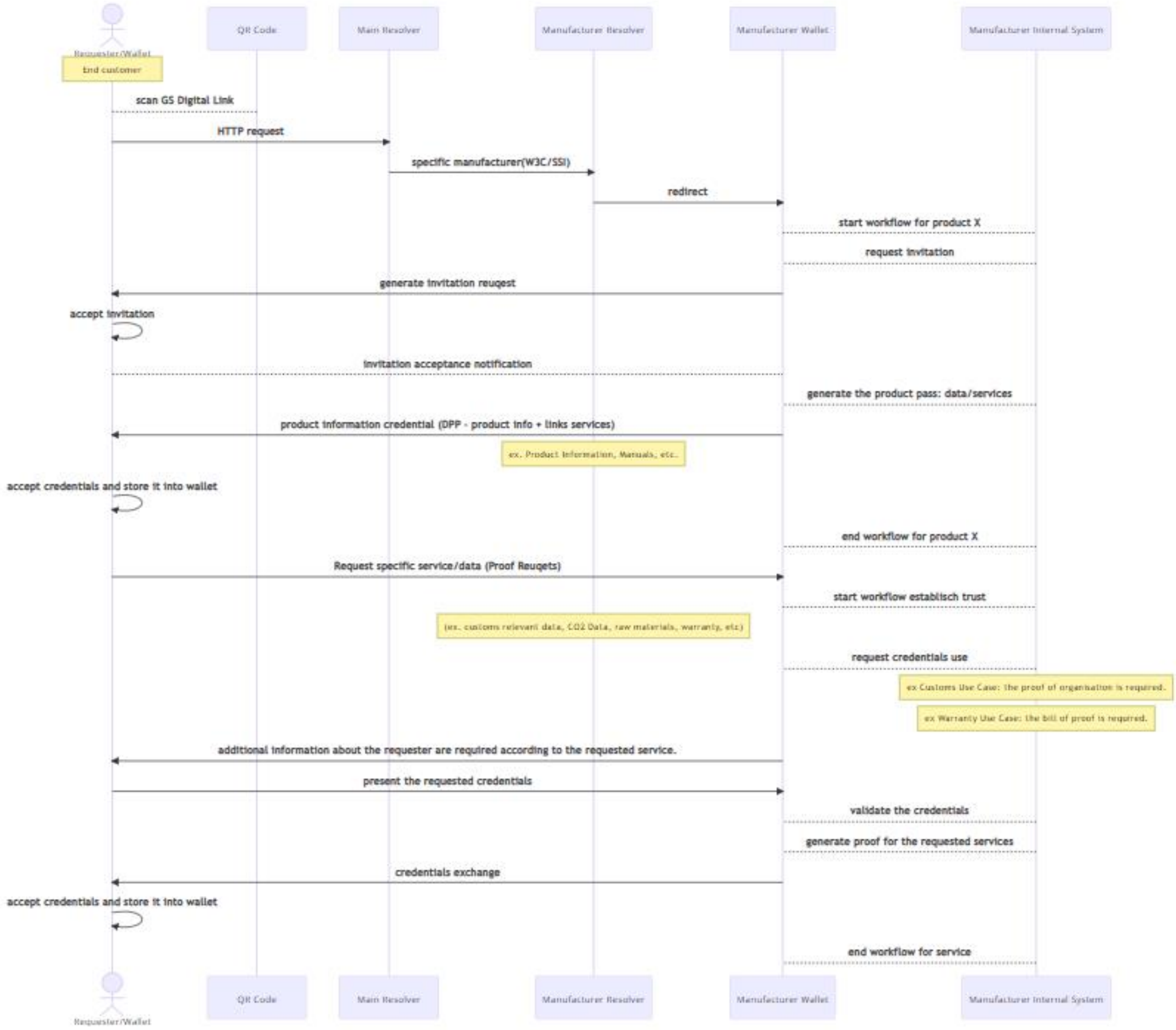

Requester/Wallet
QR Code
Main Resolver
Manufacturer Resolver
Manufacturer Wallet
Manufacturer Internal System
End customer
scan GS Digital Link
HTTP request
specific manufacturer(W3C/SSI)
redirect
start workflow for product X
request invitation
generate invitation reuqest
accept invitation
invitation acceptance notification
generate the product pass: data/services
product information credential (DPP - product info + links services)
ex. Product Information, Manuals, etc.
accept credentials and store it into wallet
end workflow for product X
Request specific service/data (Proof Reuqets)
start workflow establisch trust
(ex. customs relevant data, CO2 Data, raw materials, warranty, etc)
request credentials use
ex Customs Use Case: the proof of organisation is required.
ex Warranty Use Case: the bill of proof is required.
additional information about the requester are required according to the requested service.
present the requested credentials
validate the credentials
generate proof for the requested services
credentials exchange
accept credentials and store it into wallet
end workflow for service
Requester/Wallet
QR Code
Main Resolver
Manufacturer Resolver
Manufacturer Wallet
Manufacturer Internal System

Figure 7: Sequence Diagram Verification Process

- Embedding of information into the DPP
  - embed the required information of the product,
  - enable services related to remanufacturing, repair, recycling, and re-use of the product, and
  - make this information available for other actors along value chain: customers, economic operators, public authorities, etc.

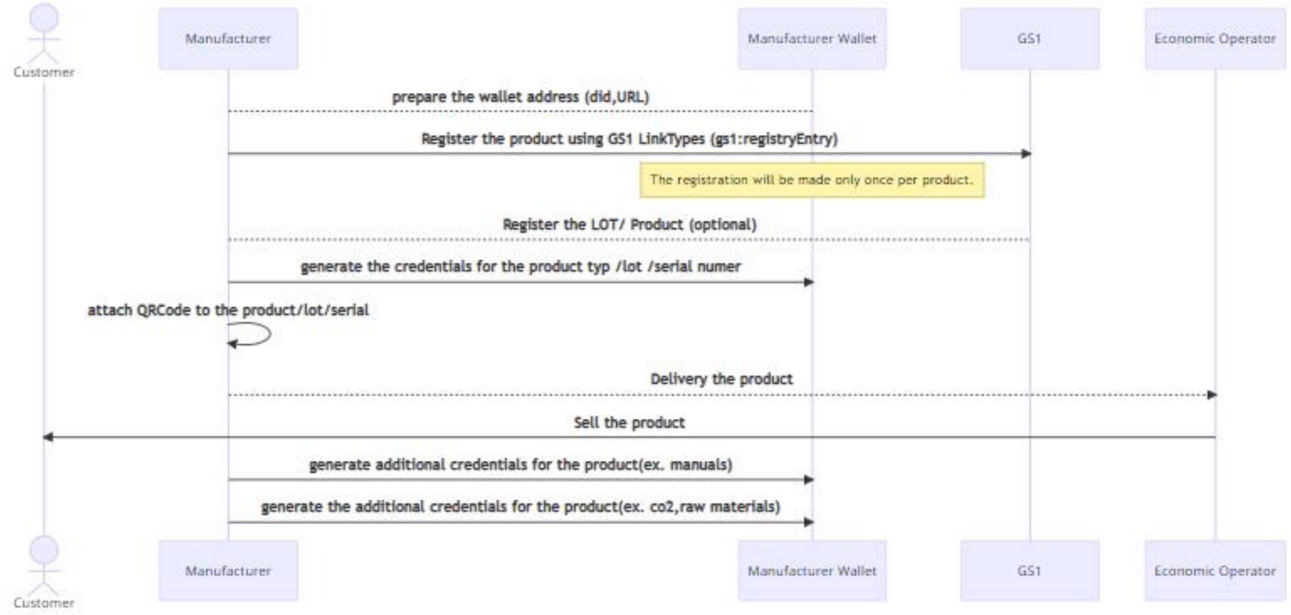

Customer
Manufacturer
Manufacturer Wallet
GS1
Economic Operator
prepare the wallet address (did,URL)
Register the product using GS1 LinkTypes (gs1:registryEntry)
The registration will be made only once per product.
Register the LOT/ Product (optional)
generate the credentials for the product typ /lot /serial numer
attach QRCode to the product/lot/serial
Delivery the product
Sell the product
generate additional credentials for the product(ex. manuals)
generate the additional credentials for the product(ex. co2,raw materials)
Customer
Manufacturer
Manufacturer Wallet
GS1
Economic Operator

Figure 8: Sequence Diagram Embedding of Information into the DPP

8.2 Sequence Diagram Without User Authentication

- Sign product credentials

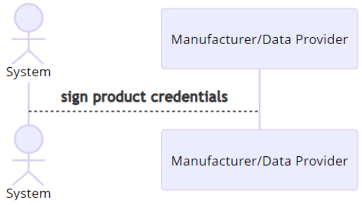


Figure 9: Process Signage of Product Credentials

- Digital Link Resolution + VC Verification Sequence Diagram

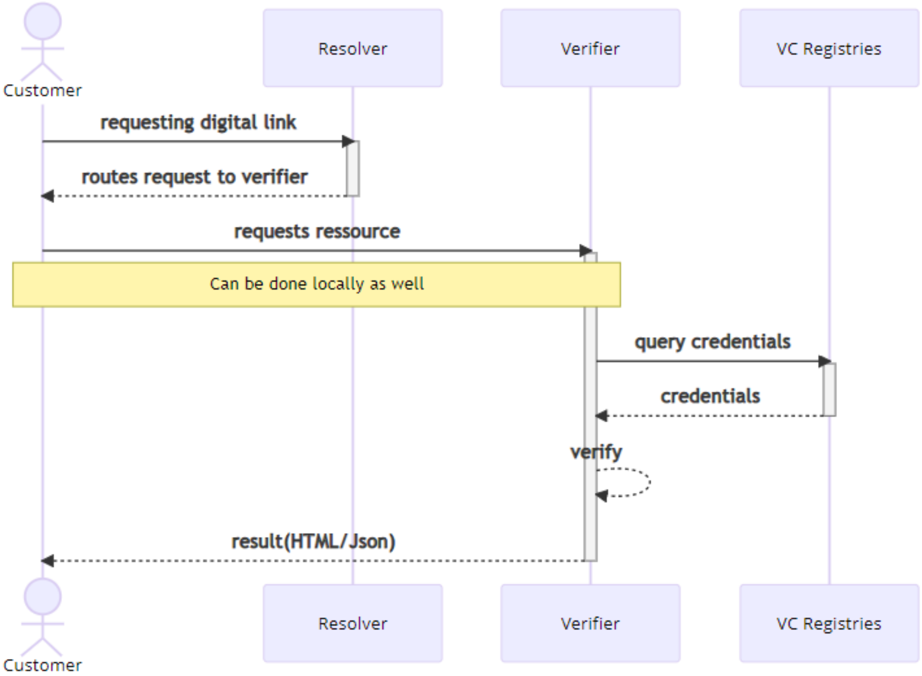


Figure 10: Sequence Diagram Digital Link Resolution

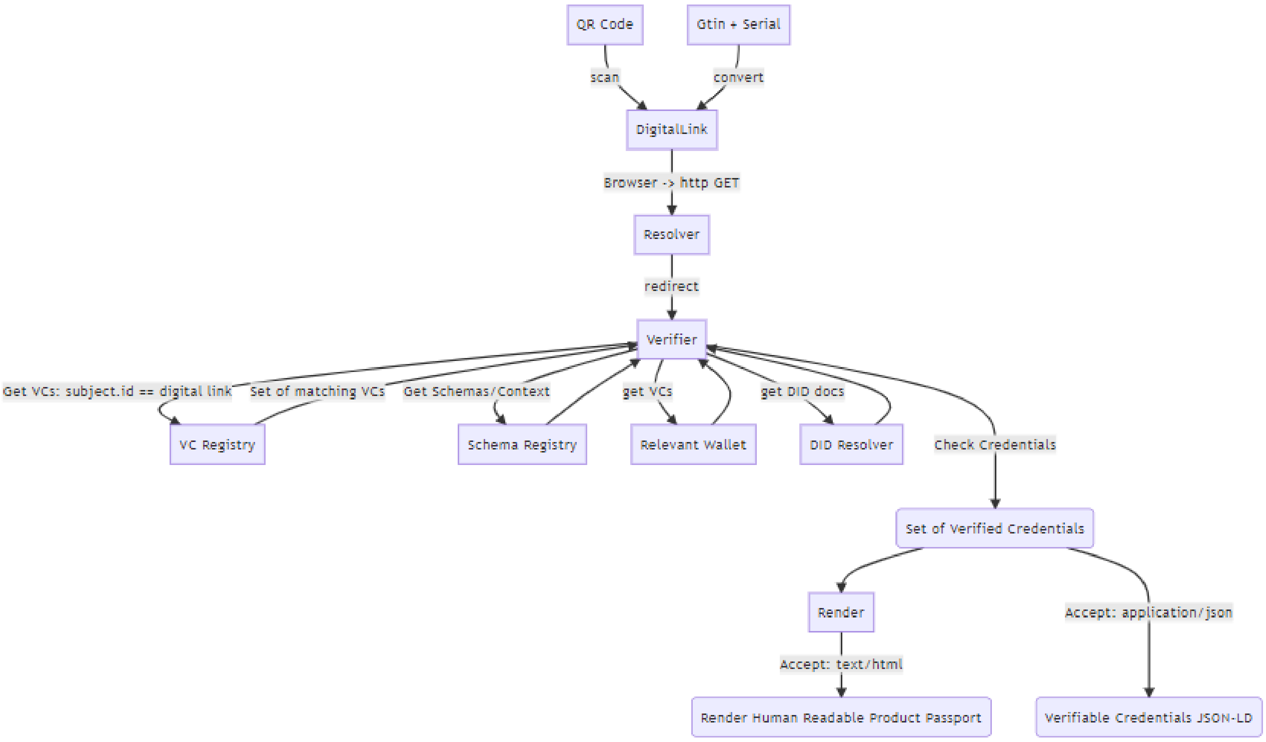


Figure 11: Sequence Diagram VC Verification