The Global Language of Business

GS1 Identification and Data – Integrity and Security

GS1 Architecture Finding

Release 1.0, Final, Feb 2026

Document Summary

Document Item	Current Value
Document Name	GS1 Identification and Data – Integrity and Security
Document Date	Feb 2026
Document Version	1.0
Document Issue	
Document Status	Final
Document Description	GS1 Architecture Finding

Contributors

Name	Organisation
Kevin Dean	Dolphin Data Development Ltd.
Junyu Wang	Auto-ID Lab Fudan University
Sue Schmid	GS1 Australia
Eugen Sehorz	GS1 Austria
Roberto Matsubayashi	GS1 Brasil
Ralph Tröger	GS1 Germany
Peta Ding	GS1 GO
Sean Lockhead	GS1 GO
Craig Alan Repec	GS1 GO
Piergiorgio Licciardello	GS1 GO
Staffan Olsson	GS1 Sweden
Sylvia Rubio Alegren	ICA
Mark Harrison	Milecastle Media Limited
Terry Burton	Terry Burton Consulting
Elizabeth Waldorf	TraceLink

Log of Changes

Release	Date of Change	Changed By	Summary of Change
1.0	Feb 2026	Kevin Dean	Release 1.0 approved by the GS1 Architecture Group (meeting date 02/04/2026)

Disclaimer

This document is not an official GS1 standard or guideline, and was not developed pursuant to GS1's IP Policy (https://www.gs1.org/standards/ip). Please note the possibility that an implementation of anything described in this document may be the subject of a patent or other intellectual property right.

Accordingly, GS1 recommends that any person or organisation developing an implementation of anything described in this document should determine whether any patents or other intellectual property may encompass such implementation, and whether a licence under a patent or other IP right is needed. The implementer should determine the potential need for licensing in view of the details of the specific implementation being designed in consultation with that party's patent counsel.

THIS DOCUMENT IS PROVIDED “AS IS” WITH NO WARRANTIES WHATSOEVER, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR PARTICULAR PURPOSE, ACCURACY OR COMPLETENESS, OR ANY WARRANTY OTHERWISE ARISING OUT OF THIS DOCUMENT. GS1 disclaims all liability for any damages arising from any use or misuse of this document, whether special, indirect, consequential, or compensatory damages, and including liability for infringement of any intellectual property rights, relating to use of information in or reliance upon this document.

GS1 makes no commitment to update the information contained herein, and retains the right to make changes to this document at any time, without notice. GS1® and the GS1 logo are registered trademarks of GS1 AISBL.

Table of Contents

1 Executive summary

The GS1 system, originally created to standardise identification and barcoding for retail, has evolved into a global framework for unique identification, reliable data capture (out of scope for this document), and trusted data exchange throughout the supply chain.

At the heart of the system are two intertwined principles:

- **Integrity** – Ensuring that identifiers and data are accurate and correctly applied.
- **Security** – Ensuring that only authorised parties can issue identifiers or provide data.

Security may also include access control. In general, identifiers are public: the presence of the identifier in a barcode or RFID tag makes it accessible to anyone with an appropriate reader. Data is often public, at least in some representations, as it appears on a product label or in a business directory. Some data may be restricted to trading partners (e.g., pricing, manufacturing lead time). Access control is out of scope for this document.

Trust in GS1 identification underpins global commerce, regulatory compliance, and consumer safety. Maintaining integrity requires rigorous validation of identifiers and data, supported by both centralised registries and decentralised event-sharing systems. Future-proofing the system involves adopting digital trust technologies (e.g., Verifiable Credentials) to meet regulatory and market demands. GS1's role is to develop the standards and guidelines that, in their application, support every identifier being unique, every piece of data being accurate, and every actor in the supply chain being trusted.

The advent of the Internet and the technologies it enables have made data available like never before. Where parties previously required a direct connection and established relationships to trade with each other, it's possible today to trade with parties you'll never meet, buying products sight unseen. Enabling this requires not only standards for identification and data sharing, but also for assuring parties that it can be trusted. GS1's own standards and services provide that, but so do others, and integrating with them is key to the ongoing support for GS1's leadership in the supply chain.

This is not a prescriptive document. It doesn't make direct recommendations on standards and technologies to be applied to the principles of integrity and security. Rather, it provides a framework in which standards and technologies may be evaluated.

2 Introduction

GS1 came into being long before the ubiquitous connectivity of the Internet as we know it today. It started with what is now the Global Trade Item Number (GTIN) and has grown to encompass a portfolio of identification and data standards.

2.1 Identification

From the beginning, GS1 identification was a distributed system, and it is still so today. Identification is coordinated by GS1 Global Office (GO), which delegates parts of the system to individual GS1 Member Organisations (MOs), who in turn delegate to individual user companies, as shown Figure 2-1. The user companies are the ones ultimately responsible for the final assignment: GTINs to trade items, SSCCs to shipping containers, GLNs to parties and locations, and so on. When properly managed, the identifiers that result are unique.

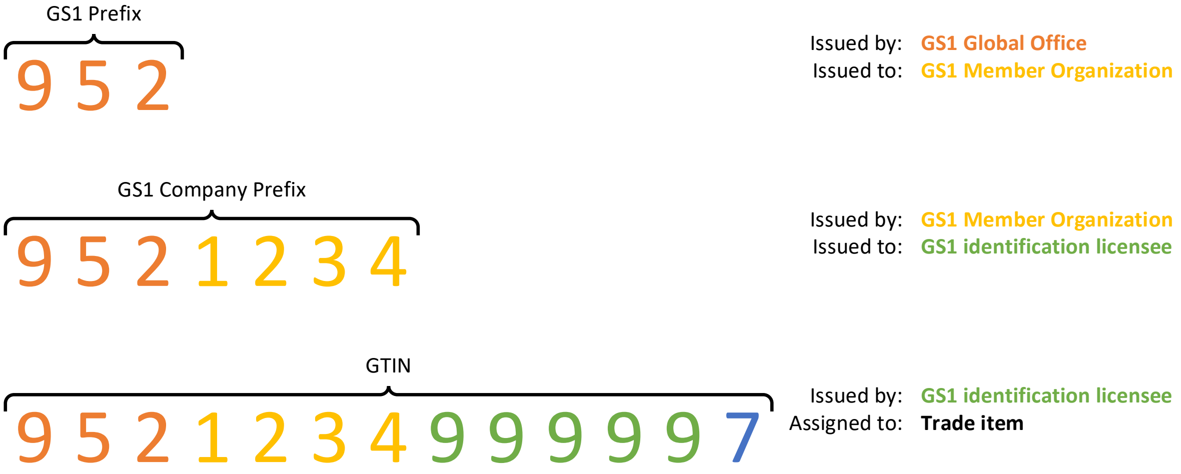
GS1 Prefix
9 5 2
Issued by: GS1 Global Office
Issued to: GS1 Member Organization
GS1 Company Prefix
9 5 2 1 2 3 4
Issued by: GS1 Member Organization
Issued to: GS1 identification licensee
GTIN
9 5 2 1 2 3 4 9 9 9 9 9 7
Issued by: GS1 identification licensee
Assigned to: Trade item

Figure 2-1 Example of GS1 identification delegated structure with GS1 Company Prefix (GCP) licence

The genesis of the GS1 system was driven more by the need for barcoding than for identification: retailers wanted to scan a barcode and lookup the price rather than relying on price stickers being correctly applied when stocking the shelves and the prices being entered correctly at checkout. Large retailers already had a workable internal identification system, but no two retailers used the same identifiers for the same product. As it was impractical for manufacturers to segment inventory and encode each retailer's identifier in a barcode, a new identifier, unique across all manufactures and retailers, had to be created. For this to work, industry had to agree on a barcode standard (the EAN/U.P.C. family of barcodes) and the content of the barcode (the U.P.C. and EAN, today known as the GTIN).

2.2 Data

Once identification is applied, the next question is what, exactly, has been identified? Initially, retailers managed the data themselves via paper listing forms provided by the manufacturers, linking the identifier in the barcode to their internal identifier, which in turn referenced the description and price. However, this too meant that there was significant duplication of effort across multiple retailers as well as for manufacturers, who had to provide the same data in different formats to each retailer.

Once again, with GS1's predecessors acting as facilitators, industry developed standards for sharing master data and, over time, transactional data associated with the exchange of goods, and visibility data providing detailed, instance- and lot-level information as entities move through the supply chain.

All of this is done based on trust: parties that assign identifiers or provide data are trusted to do so in accordance with GS1 standards. Trust is undermined by malign actors operating outside of the GS1 system or by carelessness of those operating inside it. Data providers with limited understanding of their trading partners' requirements will often provide data they believe to be “good enough” but that causes problems for trading partners that attempt to apply it (e.g., the wrong height for a product, leading to stocking issues because the shelf isn’t tall enough).

In this document, trust has two components: integrity and security. Integrity is about the accuracy of the data, whereas security is about who has the right to provide it and who has the right to receive it. The two components are intertwined: integrity of identification can be used to identify the parties that can provide or receive data, and security in the provision of data can dictate who gets to generate it and allocate the identification to it.

The purpose of this document is to identify the degree to which integrity and security matter in various use cases and to discuss mechanisms by which they can be achieved.

□ Authentication and Authorisation

Authentication and authorisation are two sides of the same coin. In short, authentication is about confirming who you are (validating your identity) and authorisation is about determining what you are allowed to do (the roles that may be performed based on your identity).

Authentication and authorisation each require trust anchors.

- Whom do you trust to assert identity?
- Whom do you trust to assert access rights?

The anchor for one is not necessarily the anchor for the other. For example, in a single sign-on environment, the service trusts an identity provider to assert the identity of their users, but the service itself is typically the one responsible for asserting the access rights. In this model, the identity provider is the trust anchor for authentication, and the service is the trust anchor for authorisation.

Authentication and authorisation domains are broadly defined. The GS1 identification system relies on a distributed model to identify entities in their domain. If each party manages the ranges assigned to it correctly, the identifier that results is guaranteed to be globally unique. The trust anchor for the GS1 identification system is GS1 Global Office, which is itself authorised as an Issuing Agency by the International Organisation for Standardization (ISO) under ISO/IEC 15459, and this maps easily to authentication and authorisation:

Party	Authenticates…	Authorises…
Government business registrar (multiple)	ISO/IEC GS1 Global Office GS1 Member Organisation User company	
ISO		GS1 Global Office as an Issuing Agency
GS1 Global Office (as GS1 identification Issuing Agency)	GS1 Member Organisation	The GS1 Prefix assigned to a GS1 Member Organisation
GS1 Member Organisation (as GS1 identification licensor)		The licence for a GS1 Company Prefix assigned to a user company
User company (as GS1 identification licensee)		The use of a GS1 identifier to identify an entity in their domain

Note: For further information on the distributed structure of GS1 identification, including delegated licensing not covered here, please refer to the GS1 General Specifications section on Managing uniqueness with GS1 Prefixes and GS1 Company Prefixes.

Multiple trust anchors can be used to establish a set of facts in support of a use case. For example, to do business with a new trading partner, you may need to verify them as a legitimate business and as using legitimate GS1 identifiers in the identification of their trade items. The trust anchor for business legitimacy is a known government business registrar, and the trust anchor for identification is ISO (via GS1 Global Office and a GS1 Member Organisation).

Many supply chain processes rely solely on GS1 identification so for the sake of this document, GS1 Global Office will be considered as a trust anchor.

3 Use cases

3.1 Identification

The following use cases highlight ways in which GS1 identifiers may be misused and, without proper management or validation, enable misrepresented entity identification in the supply chain. The victims are the users of the GS1 system, those that rely on unique and accurate identification in their processes.

3.1.1 Vendor listing

A vendor wants to sell a new product through an online retailer. They have a valid and active license for the GS1 Company Prefix underlying the product's GTIN, issued by their local GS1 Member Organisation. When they try to register the product with the retailer, their request is rejected as the same GTIN has already been assigned to a different trade item, by an organisation without the proper right to do so.

Such cases of "pirated" or "guessed" GTINs are not rare and entail significant inconveniences for both trading partners. The retailer must first identify which of the two is the legitimate licensee, approach and possibly penalise the fraudulent supplier, and figure out how to handle existing data and business processes related to the GTIN. The manufacturer cannot list their GTIN until the fraudulently identified trade items are removed and may take legal action against the other company. All parties face losses as a result.

There are many similar cases:

- A vendor listing a product with a retailer is required to identify their product using a GTIN. Rather than acquire an appropriate license from a GS1 Member Organisation, the vendor "misappropriates" a GTIN for a non-adjacent product (e.g., taking a legitimate GTIN from a grocery product to identify their hardware product) and applies it. The hardware retailer does no validation, so the listing succeeds. When the hardware retailer expands into the grocery category, the duplication is discovered, and the grocery vendor's listing is blocked.
- A vendor listing a product with a retailer is required to identify their product using a GTIN. The vendor follows an online advertisement to a barcode reseller, purchases a GTIN, and applies the GTIN to their product. The retailer does no validation, so the listing succeeds. When the vendor decides to expand their offering by providing online information using the GS1 Registry Platform, they find that they have no ability to do so as they are not the one to whom the GS1 Company Prefix underlying the GTIN has been licensed.

3.2 Distributed management

While most use cases for GS1 identification are self-contained (i.e., the party issuing the identifier is the one allocating it to an entity), there are exceptions where a strong business relationship exists between parties.

3.2.1 Third-Party logistics

A third-party logistics provider is required to place SSCCs on all a customer's containers leaving their facility. The logistics provider doesn't have their own GS1 Company Prefix, and so, with the customer's permission, they create SSCCs using the customer's GS1 Company Prefix. If the customer and the logistics provider don't coordinate the management of the GS1 Company Prefix properly, both may end up shipping multiple containers with duplicate SSCCs. This can cause problems for traceability as the same container can appear to be in two places at once.

3.2.2 Shared services

A group of independent hospitals collaborates on purchases and inventory management through a shared services organisation. To better manage inventory and delivery within the hospitals, GLNs are required to identify hospital locations such as inventory carts, wards, storage closets, and more. Rather than having each hospital acquire its own GS1 Company Prefix and issue GLNs for its locations, the shared services organisation acquires a single GS1 Company Prefix and uses it to issue GLNs for all locations across all hospitals. This can simplify location identification for group purchasing and inventory management but can cause confusion if a hospital has its own identification (whether GLN or proprietary) for the same location for other purposes.

3.3 Data sharing

3.3.1 Pharmaceutical traceability

Many regulators today mandate detailed identification and traceability of certain pharmaceutical products as part of a consumer safety mandate. Identification may be at the lot level or at the instance level. Consider the following sequence of EPCIS events, as illustrated in Figure 3-1:

- Pharmaceutical manufacturer A
  - EPCIS commission event with 5,000 SGTINs
  - EPCIS packing event 5,000 SGTINs → SSCC 1
  - EPCIS shipping event SSCC 1 A → Distributor B
  - All events are digitally signed by A to prove that the event data is authentic
- Distributor B
  - EPCIS receiving + unpacking event SSCC 1
  - EPCIS packing event with 1,500 SGTINs → SSCC 2
  - EPCIS packing event with 3,500 SGTINs → SSCC 3
  - EPCIS shipping event SSCC 2 B → Dispenser C
  - EPCIS shipping event SSCC 3 B → Dispenser D
- Dispenser C
  - EPCIS receiving + unpacking event SSCC 2
  - EPCIS dispensing event SGTIN

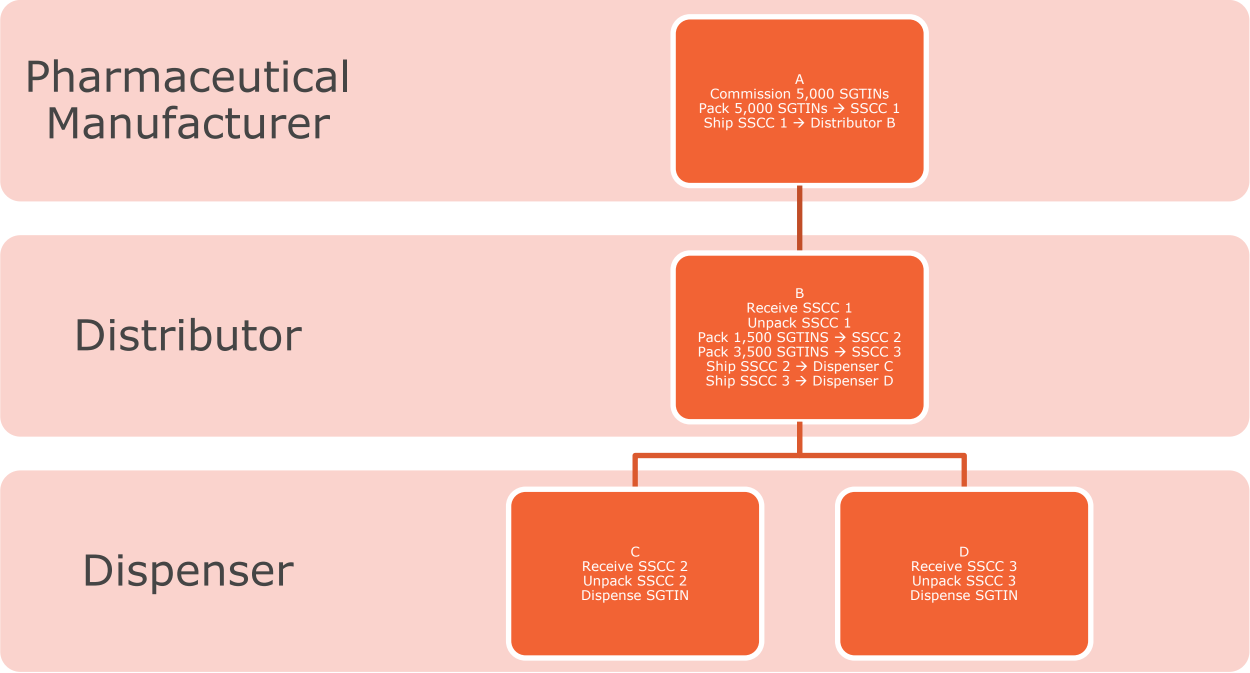
Pharmaceutical Manufacturer
A
Commission 5,000 SGTINs
Pack 5,000 SGTINs → SSCC 1
Ship SSCC 1 → Distributor B
Distributor
B
Receive SSCC 1
Unpack SSCC 1
Pack 1,500 SGTINS → SSCC 2
Pack 3,500 SGTINS → SSCC 3
Ship SSCC 2 → Dispenser C
Ship SSCC 3 → Dispenser D
Dispenser
C
Receive SSCC 2
Unpack SSCC 2
Dispense SGTIN
D
Receive SSCC 3
Unpack SSCC 3
Dispense SGTIN

Figure 3-1 Sequence of EPCIS events

Dispenser **C** is not in a direct business relationship with pharmaceutical manufacturer **A** and so relies on distributor **B** to forward data about the 1,500 SGTINs shipped to them.

It often happens that a downstream recipient (dispenser **C**) does not get all items whose IDs are specified within the original commissioning event (provided by pharmaceutical manufacturer **A**). Therefore, event data is redacted (by distributor **B**) when forwarding a given set of events to the recipient. If digital signatures are being used to verify the integrity of the data, dispenser **C** can easily verify the integrity of the data provided by distributor **B**, but can only verify the integrity of the (partial) data provided by pharmaceutical manufacturer **A** if the signing of the original EPCIS data and the removal of 3,500 SGTINs is done in manner that preserves the signature. Done properly, dispensers **C** and **D** receive only the events for the SGTINs shipped to them, neither can see events for the other, and they can each verify the digital signatures of the data they received.

3.3.2 Pharmaceutical distributor validation

To be accepted as a distributor by a pharmaceutical manufacturer, the distributor must prove that:

- they are a legitimate business, registered in the appropriate jurisdiction, according to the government of that jurisdiction;
- they are licensed to handle pharmaceutical products, perhaps including narcotics, according to the appropriate regulator; and
- the GLN they present for trading purposes is based on a legitimate GS1 Company Prefix license, according to their GS1 Member Organisation.

These facts are asserted by different parties. While it is possible for a single party to aggregate the necessary facts and assert them all, such an assertion would apply only to that set of facts. Any use case that requires other facts would require a separate combination, and it would be necessary for the party combining the facts to prove that it has the processes in place to verify them individually. Instead, the distributor should be able to present the individual facts as required, with the party to which they are presented being able to verify them individually with the appropriate issuer.

4 Actors

Actors in a security context can be persons (natural or legal) or services. To avoid the ambiguity that can arise from the use of "person" as well as to narrow the meaning of "service", the following terms shall be used:

- Human
  - Natural person.
- Business
  - Legal person.
  - While most businesses are registered, some may be a human operating in a business context without any formal business registration (e.g., a freelance artist selling their artwork).
- Service
  - An automated capability that can interact with other actors, including other services.

As this document focuses on the GS1 system, businesses may be further broken down as follows:

- GS1 Global Office
  - Formally GS1 AISBL, incorporated in Belgium, responsible for the GS1 federation and the GS1 system of standards, serving as the GS1 identification Issuing Agency.
- GS1 Member Organisation
  - A local representative of GS1 in a specific region, typically but not always a country, serving as a GS1 identification licensor.
- User company
  - A business that uses GS1 standards.
  - May or may not have a formal relationship with a GS1 Member Organisation or GS1 Global Office.
- GS1 identification licensee
  - A user company that has been licensed one or more GS1 Company Prefixes or single-issue GS1 identifiers.

4.1 Example actors, licenses, and relationships

Again, for the sake of clarity, the questions will refer to specific actors, licenses, and relationships. All except GS1 Global Office are fictitious.

- GS1 Global Office
  - GS1 Global Office is the root of the GS1 identification system and therefore the trust anchor for GS1 identification.
- GS1 Utopia
  - GS1 Utopia is a GS1 Member Organisation, responsible for managing the GS1 identification system in the region of Utopia.
- GS1 Prefix 952
  - GS1 Prefix 952 is reserved for demonstration and documentation purposes. For the sake of this document, it is assigned to GS1 Utopia.
- Healthy Tots
  - Healthy Tots is a vendor selling organic baby food through various retailers.
- GS1 Company Prefix 9521234
  - GS1 Company Prefix 9521234 is issued and licensed by GS1 Utopia to Healthy Tots, which Healthy Tots uses to identify its products for sale.

- Sell Anything & Everything (SA&E)
  - SA&E is a hybrid retailer with both an online marketplace and physical retail outlets.

5 Core questions

This document will ask and answer several questions. While it's possible to ask the questions in a very generic way (e.g., "How do we know that a GS1 identifier is genuine?"), for the sake of clarity the questions will be much more specific. For the most part, the questions will involve the ubiquitous GTIN, with other examples called out as necessary.

5.1 Authenticity of identification

How do we know that a GTIN is genuine? Given GTIN 9521234999997, what can we say about it? Structurally, it's valid: it's 13 digits long, it's composed entirely of numeric characters, and the check digit is correct.

We know from the above that the GTIN is constructed from GS1 Company Prefix 9521234, which is licensed to Healthy Tots. If the GTIN appears on a Healthy Tots product or in data provided by Healthy Tots, we know that it's genuine due to the following chain of authenticity:

- GS1 Global Office, as the root of the GS1 identification system, is authorised to issue GS1 Prefixes in any numeric range to GS1 Member Organisations.
- GS1 Utopia is authorised by GS1 Global Office to issue licenses for GS1 Company Prefixes in the range of (i.e., starts with) GS1 Prefix 952.
- Healthy Tots is authorised by GS1 Utopia to issue GS1 identifiers in the range of GS1 Company Prefix 9521234.
  - The GS1 Company Prefix is in the range of (i.e., starts with) GS1 Prefix 952 issued to GS1 Utopia.
- GTIN 9521234999997, if it appears on a Healthy Tots product or in data provided by Healthy Tots, is authentic.
  - The GTIN is in the range of (i.e., starts with) GS1 Company Prefix 9521234 issued to Healthy Tots.

At every step, the range of control narrows, until there's a single GTIN at the end, identifying the product that Healthy Tots sells. The authenticity of the GTIN is determined by the unbroken chain of control of the GS1 identification system, and each party is responsible for maintaining integrity of assignment within their range of control (e.g., GS1 Utopia is responsible for ensuring that they don't issue duplicate or overlapping GS1 Company Prefixes).

In summary, to determine if a GTIN is genuine, we must establish who is making the attestation that it's genuine and in what context. In summary:

- Is the GTIN structurally valid?
- Has the GTIN been issued from a valid GS1 Company Prefix license?
  - Has the GS1 Company Prefix been issued from a valid GS1 Prefix?
- Is the party making the attestation to the GTIN in control of it and therefore authorised to do so (i.e., the brand owner), or is it possible to determine their authorisation (e.g., certification agency, authorised distributor) to do so through other means?

The last bullet is the hardest question to answer:

- Even with information about the company to whom a GS1 Company Prefix has been licensed, the name of the brand or the product often has no obvious correlation with the name of the company.
- Distributors are often responsible for managing local data for imported products. They may or may not have a direct relationship with the brand owner, and there are no standard ways to verify that they do. Furthermore, even if they pass through data from the brand owner without modification, there are no mechanisms within the GS1 data sharing standards to verify the source.
- A local manufacturer, licensed by a foreign brand owner to manufacture or package their product for the local market, may use their own GTINs to identify the product. If data were

verifiable as having come from the brand owner, there would still need to be proof that the local manufacturer is authorised to apply their own GTIN to the product.

5.2 Authenticity of association

The question about the party making the attestation to the GTIN bullet goes beyond identification. It concerns the data and can involve processes that are currently not regular practice.

The presence of the GTIN on its own is not enough to assert its authenticity. Even if we know enough about it to know that it is in the range of the GS1 Company Prefix licensed to Healthy Tots, without an association with Healthy Tots, we can't say that it's genuine. If a malign actor decides to use the GTIN for their own product, we can say definitively that the GTIN is not associated with Healthy Tots, so the GTIN in that context is not valid.

How do we know what a GTIN refers to? We've established that GTIN 9521234999997 is genuine (because Healthy Tots, the GS1 Company Prefix licensee, says that it is), and that it refers to one of their products. We know that the association of the data to the GTIN is genuine because the data was provided by Healthy Tots, the same entity that issued the GTIN. In short, the data is authentic because we can prove an association between the party responsible for the identifier and the party responsible or the data (in this case, they are the same).

This is a common model for identification: the party that issues the identifier determines what it identifies and can generally be trusted to provide the correct data for it. The model doesn't apply to everything; not all the data associated with the GTIN is trusted if it comes from the licensee. For example:

- Is the product kosher, organic, or fair trade?
- Are the dimensions and weights complete and correct?

The first question has to do with the fact that the brand owner is not authorised to make some attestations at all; the consumers interested in such attestations trust only the certifying agencies responsible for them. The second question has to do with the fact that the brand owner can't be trusted to make some attestations correctly; very often, the individual that is entering the data (e.g., a product manager) is far enough removed from the source of the data (e.g., a packaging designer) that they can't get the original data (e.g., gross dimensions and weights) and therefore are no more likely to enter it correctly than anyone else.

In such cases, data should be provided by trusted third parties. Such parties may be trusted by virtue of their position within a community (e.g., religious dietary certification) or through some other, independent certification process.

This creates an important distinction in the classification of data. Data that is provably associated with an identifier (i.e., that is provided by the party responsible for the identifier or by a party that has been delegated that responsibility by the party responsible for the identifier) is genuine. Data that is provided by a party that is provably competent to do so is trusted. It's possible to have one without the other: the claim by a company that their product is organic is genuine but not necessarily trusted without additional documentation, or the certification by an agency that a product is organic is trusted but not necessarily genuine without a provable association between the company and the certification agency.

If Healthy Tots wants their products to be certified as organic (third-party certification is a requirement in many countries when making organic and other claims), then they need to defer to a certification agency. Who ultimately provides the attestation (Healthy Tots or the certification agency) that GTIN 9521234999997 identifies an organic product is an open question.

Figure 5-1 below shows the ways in which a declaration may be made.

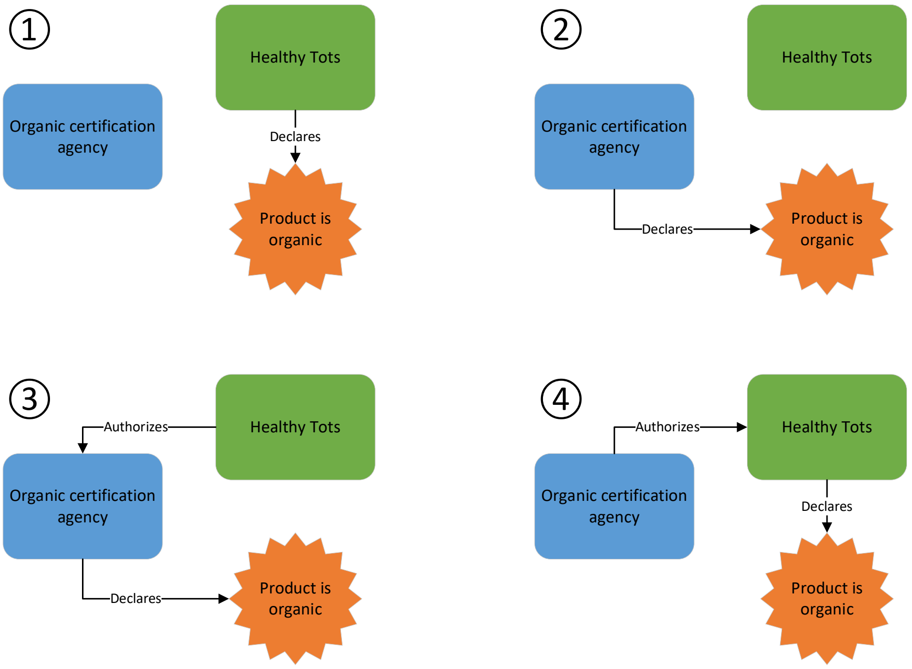

Figure 5-1 Examples of various declaration methods

1. Healthy Tots issues the declaration itself. If the retailer trusts Healthy Tots, they can accept the declaration. This option is the riskiest, as the retailer must trust every vendor to make the declaration honestly and correctly.
2. The organic certification agency issues the declaration itself. If the retailer trusts the agency, they can accept the declaration, provided that the agency includes the GTIN and/or enough data about the product (e.g., brand and description) to ensure they have the right one. This option is generally safe, as the retailer need only trust a limited number of organic certification agencies, but it’s not a common model.
3. Healthy Tots authorises the organic certification agency to issue declarations about its products, based on data provided by Healthy Tots. This is similar to option 2, with the authorisation ensuring that the agency is acting in good faith in making declarations about products manufactured by Healthy Tots. This option can be enabled quite easily with GS1 Digital Link: the vendor provides a certification link that points to the organic certification agency, who provides an endpoint that returns the certification data.
4. The organic certification agency authorises Healthy Tots to issue declarations about their own products. This authorisation would be based on an evaluation of processes at Healthy Tots, including ingredient sourcing and manufacturing, so the agency is certifying the company or a product line, not the individual products. This is the most common model.

In summary:

- How do we discover what the GTIN refers to?
- What does the GTIN refer to?
- Who provided the data?
- Is the party that provided the data authorised to do so by the licensee of the GTIN, or are they authorised or trusted to do so through other means?
- Is the party that provided the data trusted to provide it or capable of providing it correctly?

As before, the last bullet is the hardest question to answer. In the case of an agency that defines its own requirements and certification processes, it can generally be trusted to apply them consistently and correctly, though it often relies on the brand owner to relay the data. In other cases, such as data provided by the brand owner itself or by an outside party that implements but doesn’t define the requirements and processes, GS1 has provided guidance on data quality, covering Master Data Programmes, a Data Quality Framework, Standards, Training, and the Verified by GS1 service.

6 Solutions

Solutions fall into two broad categories: centralised and decentralised.

A centralised solution is one where decision-making, data, and control are concentrated in a single point or entity. A single authority manages operations, and a central database or service processes all information. A centralised solution makes it easier to enforce uniform policies and standards, and decision-making is faster due to fewer parties being involved.

By contrast, a decentralised solution distributes decision-making, data, or control across multiple independent entities or nodes. Multiple actors can participate, and the solution is often more resilient to failures or attacks. While it can enable greater transparency and autonomy, it is harder to establish trust, and it may lead to inconsistencies or slower coordination.

Many solutions are hybrid. EPCIS, the GS1 standard for creating and sharing visibility event data, is designed as a distributed solution for recording and querying event data, but the initiation of any movement of goods depends on a centralised, trusted service within each trading partner that maintains relationships with other trading partners. From the perspective of someone querying the data, EPCIS is decentralised. How the data comes about (who has what) is a function of centralised decisions within each company about sourcing, pricing, logistics, and more.

For a more comprehensive discussion see RFC 9518 – Centralization, Decentralization, and Internet Standards.

6.1 GS1 registry platform

The GS1 Registry Platform is a repository of all licenses issued by GS1 Member Organisations as well as of millions of GTINs and GLNs. GS1 Global Office hosts a branded front-end called Verified by GS1, which responds to queries and provides basic license, product, party and location information. The Verified by GS1 service has no public API, provides only a few attributes, and limits the number of queries per day, but many GS1 Member Organisations offer UI and API services that provide richer data in volume, often using a private API to retrieve non-local data from the GS1 Registry Platform.

With access to the GS1 Registry Platform, it’s possible to authenticate the licensee and validate the GTIN or GLN by verifying the attributes in the registry against the data in hand.

Another feature of the GS1 Registry Platform is the GS1 Resolver service. Based on the GS1 Conformant Resolver standard, it is a free, high-performance, high-resilience system that resolves a GS1 identifier to one or more sources of information about the identified item. For example, it can link a GTIN to nutritional information, drug fact sheets, warranty information, instruction manuals, recall status, and more.

Data in the GS1 Registry Platform is managed by the GS1 Member Organisations. In general, MOs are responsible for data in the range of the GS1 Prefixes that are assigned to them by GO. This may vary by mutual agreement between MOs, but the important principle is that the MOs are the gatekeepers of data that is provided to them by brand owners or their delegates.

Whether queried through Verified by GS1 or via an API provided by a GS1 Member Organisation, the GS1 Registry Platform is a centralised service. Trust in the service depends on the level of trust in the GS1 federation.

6.2 Global Data Synchronisation Network

The Global Data Synchronisation Network (GDSN) is a distributed network that connects data sources, who publish product data, and data recipients, who subscribe to product data. Each node in the network, called a data pool, registers the products it hosts with the GS1 Global Registry, a centralised service that allows data sources and recipients to connect across data pools.

GDSN does not natively support license validation, although some data pools may require it. The same product may appear multiple times from multiple sources, as many sources are distributors and each source operates independently. Accordingly, the level of trust in the data is dependent on the level of trust that the recipient has in the source.

6.3 Persistent identification

Persistent identification ensures that the same identifier refers to the same thing for the lifespan of the identified entity.

The GTIN has been subject to non-reuse since 2019 (earlier for healthcare items), ensuring that the same GTIN applies to the same trade item for all time, though variants of the trade item itself (sometimes indistinguishable from each other in their formulation) may have different GTINs over time as the trade item evolves to meet the needs of the market. Persistent identification ensures that information behind the identifier is always referenceable, even if the company itself is out of business. This is one of the significant value propositions of the GS1 Registry Platform.

Regulatory requirements are a significant driver of persistent identification. Given the consumer safety issues involved, healthcare items required persistent identification long before GTIN non-reuse became required for everything else. Modern regulations, such as the EU Digital Product Passport, are driving that further, requiring data to be available long after a product has been withdrawn from the market. Such regulations also mandate ease of access, i.e., that access to such data be possible without requiring the download of additional software. This is driving Ambition 2027 for 2D barcodes at retail point of sale, a key component of which is GS1 Digital Link, which enables web access using GS1 identifiers.

A comprehensive discussion of persistent identification using GS1 identifiers may be found in the Web-enabled, structured path identification whitepaper by GS1 in Europe.

Verifiable credentials

The W3C Verifiable Credentials standard is a robust and flexible way for one party to assert facts about another. At its core, a Verifiable Credential breaks down as follows:

- Issuer – The party that issues the Verifiable Credential.
- Subject – The party about whom the Verifiable Credential is making a claim.
- Claim – The claim itself; the fact that is being asserted.

Issuers and the subjects are typically identified using W3C Decentralized Identifiers, which provide a standardised way of locating the cryptographic material associated with a party. The issuer's cryptographic material is used to sign the Verifiable Credential and the subject's cryptographic material is used to sign the presentation (i.e., to prove that the subject is the one making the presentation).

The structure of the claim is typically defined by the issuer or by some standardisation process. Universities, for example, could work together to define the structure of an education claim, showing the degree and graduation year, along with any additional honours the graduate received.

While it's technically possible for anyone to issue any Verifiable Credential to anyone with any claim (e.g., to forge an unearned university degree), the business rules surrounding any Verifiable Credential typically include the identification of one or more trust anchors. There may be a publicly available directory, for example, with the Decentralised Identifier (DID) of each accredited university. If the issuer DID in the Verifiable Credential isn't in the list, the Verifiable Credential can't be trusted.

The use of such a list, though, reduces the effectiveness of Verifiable Credentials. How do you know that the list is valid? How do you know that it hasn't been tampered with? How do you deal with universities that lose their accreditation without invalidating all the degrees that they issued prior to that?

One of the strengths of Verifiable Credentials is flexibility, and that flexibility allows claims to be chained: a claim made by an issuer about a subject can allow the subject to issue claims themselves. For example, a single government department of education could issue university accreditations, including in each claim the disciplines for which the university is accredited. The claim made by the department of education thereby authorises the university to issue degrees in the accredited disciplines.

Now, whenever the university issues a degree credential, it would provide a copy of its accreditation credential to the graduate. The graduate would present both to a prospective employer, who can now authenticate them:

- The DID of the department of education is well known (e.g., published on their website).

- The issuer of the accreditation credential matches the DID of the department of education and the digital signature is valid, so the accreditation is valid.
- The issuer of the degree credential matches the subject of the accreditation credential, the digital signature is valid, and the discipline of the degree matches one of the disciplines for which the university is accredited, so the degree is valid.
- The subject of the degree credential is the same party that digitally signed the presentation, so the employer knows that the degree belongs to the job applicant.

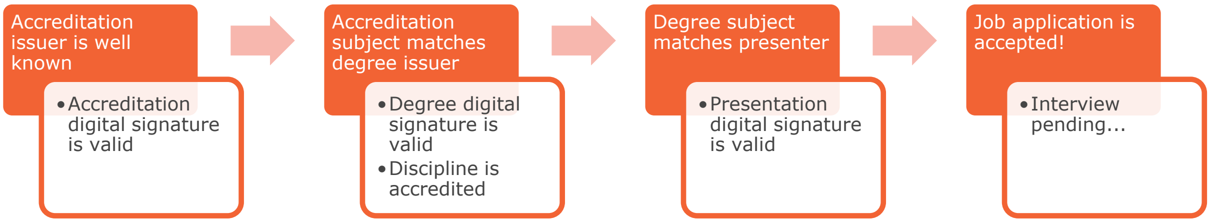
Accreditation issuer is well known
• Accreditation digital signature is valid
Accreditation subject matches degree issuer
• Degree digital signature is valid
• Discipline is accredited
Degree subject matches presenter
• Presentation digital signature is valid
Job application is accepted!
• Interview pending...

Figure 6-1 Job application presentation

Returning to the pharmaceutical distributor validation use case, it's easy to see how it maps to Verifiable Credentials.

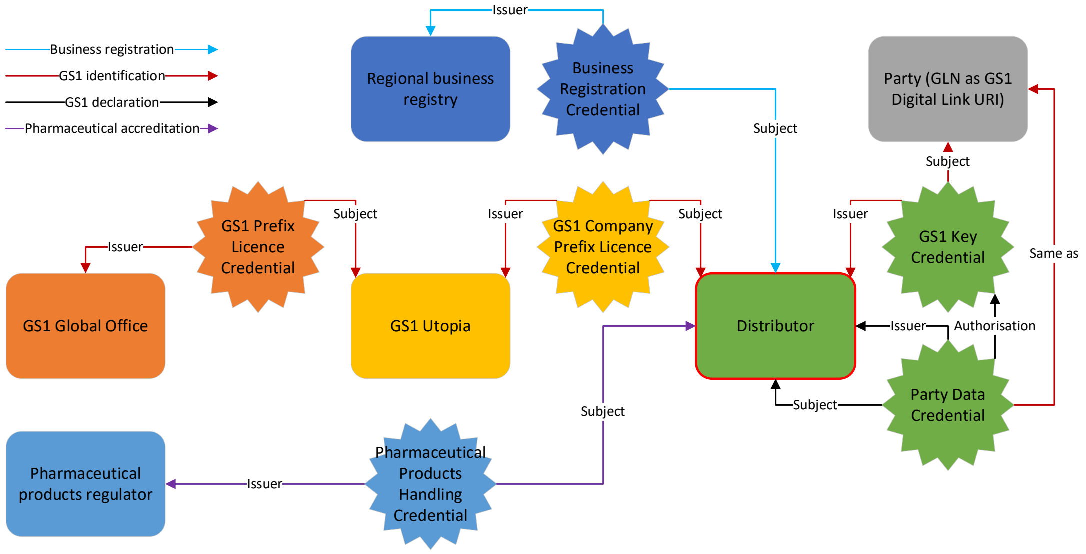
Business registration
GS1 identification
GS1 declaration
Pharmaceutical accreditation
Issuer
Regional business registry
Business Registration Credential
Subject
Party (GLN as GS1 Digital Link URI)
Subject
Same as
Issuer
GS1 Prefix Licence Credential
Subject
Issuer
GS1 Company Prefix Licence Credential
Subject
Issuer
GS1 Key Credential
GS1 Global Office
GS1 Utopia
Distributor
Issuer
Authorisation
Party Data Credential
Subject
Subject
Pharmaceutical products regulator
Issuer
Pharmaceutical Products Handling Credential

Figure 6-2 Multiple Verifiable Credentials to satisfy a use case

With every starburst as a Verifiable Credential shown in Figure 6-2, the distributor can make a single presentation to the pharmaceutical manufacturer:

- The DIDs of the regional business registry, the pharmaceutical products regulator, and GS1 Global Office are well known.
- The issuer of the business registration credential matches the DID of the regional business registry and the digital signature is valid, so the business registration is valid.
- The issuer of the pharmaceutical products handling credential matches the DID of the pharmaceutical products regulator and the digital signature is valid, so the pharmaceutical products handling is valid.
- The issuer of the GS1 Prefix licence credential matches the DID of GS1 Global Office and the digital signature is valid, so the GS1 Prefix licence is valid.
- The issuer of the GS1 Company Prefix licence credential matches the subject of the GS1 Prefix licence credential, the digital signature is valid, and the GS1 Company Prefix is within the range of the GS1 Prefix, so the GS1 Company Prefix licence is valid.
- The issuer of the GS1 identifier and party data credentials matches the subject of the GS1 Company Prefix licence credential, the digital signature is valid, and the GLN is within the range of the GS1 Company Prefix, so the GS1 identifier and party data are valid.

- The subjects of the business registration credential, pharmaceutical products handling credential, and GS1 Company Prefix licence credential are identical and are the same party that digitally signed the presentation, so the manufacturer authenticates the distributor and adds them to their trading partner list.

The GS1 licensing and identification ecosystem of Verifiable Credentials is already well defined and continues to evolve as it is tested with the GS1 community. Support for Verifiable Credentials is part of GS1 Vision 2030, and technical details (subject to change) may be found in the GS1 Digital Licenses document.

It's important to note that no party makes any claim about anything outside of its domain. For example, GS1 makes no claim about the authenticity of a business. That is the responsibility of various business registries around the world, and GS1 relies on those registries just like anyone else. Although it's conceivable for there to be a single trust anchor (e.g., a pharmaceutical industry group that validates all the above and presents a consolidated assertion), it's unlikely simply because of the multitude of use cases and the corresponding number of assertion consolidations required. Every use case can be broken down into one or more component parts, each with its own trust anchor.

Properly implemented, trust systems are self-assembling, and the whole is greater than the sum of its parts.

6.4 Digital signatures

A cryptographic digital signature is a well-known means of securing a document by attesting to the author and by assuring its integrity. GS1 provides significant support for digital signatures in the GS1 Web Vocabulary entry for gs1:AuthenticityDetails as well as, in rare circumstances (e.g., high value, high risk), the encoding of a barcode or RFID tag using DigSig AI (8030) which implements ISO/IEC 20248: Information technology — Automatic identification and data capture techniques — Digital signature data structure schema.

6.4.1 Digital signatures in traceability

While most often applied to the entire document, there are ways to generate and apply a signature so that parts of the document may be redacted without compromising the signature. Selective data can then be disclosed to downstream parties without sharing parts of data to which they are not entitled.

A typical example of this is age verification for purchasing restricted products (e.g., alcohol). If a driver's license is presented, the only information a retailer truly needs is the picture to confirm that the person presenting it is the person purchasing the product and either the date of birth or an attestation that the person is of age. The rest of the data (e.g., license class, address, etc.) is irrelevant to the transaction. In digital form, the presentation of selective data, without compromising the integrity of the digital signature, is an important consideration in the design of the digital signature process.

In supply chain applications, the distributed nature of EPCIS is such that data can come from multiple sources, and it may be necessary to provide non-repudiable proof as to which party is responsible for which data. It may also be necessary for data provided by one party (e.g., the event information itself) to be supplemented by data from another party (e.g., product master data) while ensuring that the integrity of the other party's data is maintained.

Although not explicitly called out in the EPCIS standard, EPCIS documents may be digitally signed using standard protocols for XML and JSON/JSON-LD. Several resources have been developed on this subject and may be explored in more detail:

- EPCIS Signing
- Verifiable Credentials and end-to-end traceability
- A solution approach for the anonymous sharing of sensitive supply chain traceability data
- EPCIS sanitisation

7 Additional questions

The number and variety of use cases around integrity and security make it impossible to define a one-size-fits-all approach. When evaluating requirements and solutions, it may be helpful to prepare a set of questions that need to be answered, alongside a metric of importance (e.g., data mandated by regulation may be considered critical, whereas marketing data is not). These are some of the considerations and questions that may apply.

- Is the identification authentic?
  - Has the identifier been issued by a party authorised to do so?
  - Has the identifier been allocated by a party authorised to do so?
- Is the data authentic?
  - Has the data been published by a party authorised to do so?
    - Not necessarily the same as the party authorised to allocate the identifier, e.g., third-party product certification.
    - Multiple authorisation chains may exist, e.g., brand owner authorises solution provider to provide planogram data and solution provider is certified against the GS1 Package and Product Measurement Standard by their local GS1 Member Organisation.
  - Generically, how do we account for third party agents and what credential grants and privileges should they have given their service agreements with the credential holder?
- What makes data associated with a GS1 identifier authentic?
  - Who provided it?
  - Has it been tampered with?
- What safeguards can be applied to the content of the data to ensure it hasn't been tampered with?

7.1 Identification

- What rights are granted to a user with a GS1 Company Prefix or individual GS1 identifier license?
- What makes a GS1 identifier authentic?

7.2 Master data

- Usually broadly distributed with little concern about who sees it.
- Exceptions for sensitive information (e.g., pricing, lead time).
- How is data declared at a later stage in the supply chain (e.g., local distributor adding data required by local regulation) handled?

7.3 Instance/group data

- Subset of master data, applying to a specific instance (serial) or sub-class (batch/lot).
- A subtle point that could be noted regarding master data is that in addition to master data asserted by the original brand owner / ID originator, there might be modifications to that master data (possibly at finer granularity, such as for an individual product instance) that might be asserted at a later stage in the lifecycle, e.g., by a third-party user / reseller. Some simple examples of such a change might be to note that the capacity of a built-in rechargeable battery is now different from the original capacity specified by the brand owner, or that a camera now has a specific number of shutter cycles or that a vehicle has a specific number of miles or kilometres on its odometer (distance "clock").

7.4 Transactional data

- Typically delivered through a trusted channel, with sender and receiver having a trusted relationship prior to any data exchange.
  - Data trusted by virtue of that relationship.
- Some situations where there is no prior relationship.
  - Drop shipment, buyer asks supplier to ship product to the buyer's customer.
  - Subsequently, buyer's customer requests supplier to verify the product.
  - No direct relationship between supplier and end customer.
- Emerging use cases in EDI include ensuring data integrity in the transaction documents themselves, not just in the connection between trading partners over which the documents are shared.

7.5 Event data

- Who has the authority to declare an event?
- Who has the authority to ask for it?
  - Querying party is either known to the information providing party or has sufficient "static" credentials to be granted access, without needing to evaluate any chain of connectedness between the querying party and the information providing party in the context of a specific product instance or individual shipment / logistics unit.
  - Querying party may be able to prove "right of access" using chain of credentials.
  - Not every party involved in an exchange has the right to see non-immediate/non-adjacent upstream or downstream party.
  - For example, in a manufacturer to distributor to retailer supply chain scenario, the manufacturer is not privy to whom the distributor transferred the product.
- Different products may have different security requirements.
  - Should we consider security levels and corresponding security mechanisms?
  - For example, some medicinal products (e.g., narcotics, controlled substances, psychotropic drugs, radioactive drugs) have much higher security requirements than other products.

8 Recommendations

The GS1 Architecture Group recommends:

1. Targeted analysis and publication of artefacts that strengthen integrity and security for GS1 identification and data. This would enhance existing documents by:
   a. providing formalised guidance for GS1 Member Organisations on implementing trust chains in practice; and
   b. further detailing the roadmap, steps, and processes to support GS1 Vision 2030.
2. Encouragement of pilots and research initiatives (e.g., via GS1's Auto-ID Lab network) to explore:
   a. mechanisms for partial data disclosure without compromising integrity in scenarios such as pharmaceutical EPCIS event sharing;
   b. application of the GS1 Web Vocabulary for product certifications (organic, fair trade), regulatory compliance, and similar use cases; and
   c. the added value of Verifiable Credentials in marketplace onboarding, including insights for enhancing Verified by GS1 capabilities.
3. Reaching out to external trust anchors (e.g., government registries, certification agencies) to validate and demonstrate multi-domain claim verification.
4. Review of GSMP to ensure that its approach to new technologies and standards that are expected to have an impact on GS1 standards in the medium- to long-term future are suitable for the present day.
5. Review of the GS1 Digital Signatures Technical Implementation Guide to educate industry and regulators on the consequence of encoding security features in data carriers.
6. Engagement of the GS1 Global Office Industry Engagement and Public Policy teams to promote the work on the GS1 Digital Signatures Technical Implementation Guide and the 2D Program tools on quishing (the use of malicious or spoofed QR codes to trick people into visiting fake websites, downloading malware, or revealing sensitive information) within the GS1 MO Interest Groups.