



The Global Language of Business

GS1 Global Traceability Standard

GS1's framework for the design of interoperable traceability systems for supply chains

Release 2.0, Ratified, Aug 2017

Document Summary

Document Item	Current Value
Document Name	GS1 Global Traceability Standard
Document Date	Aug 2017
Document Version	2.0
Document Issue	
Document Status	Ratified
Document Description	GS1's framework for the design of interoperable traceability systems for supply chains

Log of Changes

Issue No	Date of Change	Changed By	Summary of Change
1.0	Sep 2007	John Ryu, Diane Taillard	Initial Version of the GS1 Global Traceability Standard
1.3.0	Nov 2012	John Ryu	eBallot approved WR 11-281 and update for publication
2.0	Aug 2017	Coen Janssen	WR17-000031 to enable trading partners to better understand how to leverage standards-based traceability solutions to address the requirements of multiple regulations.

Disclaimer

GS1®, under its IP Policy, seeks to avoid uncertainty regarding intellectual property claims by requiring the participants in the Work Group that developed this **GS1 Global Traceability Standard** to agree to grant to GS1 members a royalty-free licence or a RAND licence to Necessary Claims, as that term is defined in the GS1 IP Policy. Furthermore, attention is drawn to the possibility that an implementation of one or more features of this Specification may be the subject of a patent or other intellectual property right that does not involve a Necessary Claim. Any such patent or other intellectual property right is not subject to the licencing obligations of GS1. Moreover, the agreement to grant licences provided under the GS1 IP Policy does not include IP rights and any claims of third parties who were not participants in the Work Group.

Accordingly, GS1 recommends that any organisation developing an implementation designed to be in conformance with this Specification should determine whether there are any patents that may encompass a specific implementation that the organisation is developing in compliance with the Specification and whether a licence under a patent or other intellectual property right is needed. Such a determination of a need for licencing should be made in view of the details of the specific system designed by the organisation in consultation with their own patent counsel.

THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR PARTICULAR PURPOSE, OR ANY WARRANTY OTHER WISE ARISING OUT OF THIS SPECIFICATION. GS1 disclaims all liability for any damages arising from use or misuse of this Standard, 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 retains the right to make changes to this document at any time, without notice. GS1 makes no warranty for the use of this document and assumes no responsibility for any errors which may appear in the document, nor does it make a commitment to update the information contained herein.

GS1 and the GS1 logo are registered trademarks of GS1 AISBL.

Table of Contents

1	Introduction	6
1.1	Objective	6
1.2	Scope	6
1.3	About GTS version 2.....	7
1.4	How to use this document?	8
2	Traceability and the importance of standards.....	9
2.1	Business drivers.....	9
2.2	The need for unique identification	10
2.3	The need for traceability data	11
2.4	The need for interoperability and standards.....	12
2.5	GS1 standards – key enabler for interoperability.....	13
3	Traceability data and traceability systems.....	16
3.1	Traceability data within an organisation	16
3.2	Traceability data across supply chains	16
3.3	Managing traceability data	17
3.3.1	Sources of traceability data.....	18
3.3.2	Precision of traceability data	18
3.3.3	Sensitivity of traceability data	19
3.3.4	Quality of traceability data	20
3.3.5	Sharing of traceability data	20
3.4	Traceability systems.....	21
3.5	Traceability systems in action: An example	23
4	Key enablers for interoperable traceability systems	27
4.1	Identification of objects, parties and locations.....	27
4.1.1	Traceable objects.....	27
4.1.2	Traceability parties	30
4.1.3	Traceability locations.....	30
4.1.4	Transactions and documents	30
4.2	Automatic identification and data capture (AIDC)	30
4.2.1	Applying data carriers	31
4.2.2	Capturing data	32
4.3	Sharing traceability data	33
4.3.1	Separation of content and communication method.....	33
4.3.2	GS1 data sharing standards and services.....	33
4.3.3	Data discovery, trust and access control	34
4.3.4	Event data from devices & sensors and the Internet of Things (IoT)	36
4.4	The traceability solution ecosystem	37
5	Key requirements for interoperable traceability systems	38
5.1	Prerequisites	38
5.2	Identification requirements (including static data management).....	38
5.3	Automatic data capture and identification (AIDC) requirements	39
5.4	Data recording requirements (relation data and CTEs)	39
5.5	Data sharing requirements	40

5.6 Roles and responsibilities	41
6 Glossary.....	42
6.1 List of abbreviations	43
7 References.....	45
A Summary of interoperability requirements	46
B Data management responsibilities.....	47
C Getting started	48
C.1 Before you begin.....	48
C.2 Steps to take	48
C.3 Design the traceability system	49
C.4 Build the traceability system.....	50
C.5 Deploy and use the traceability system	50
D Sector examples	52
E Acknowledgements.....	55

1 Introduction

1.1 Objective

The objective of the GS1 Global Traceability Standard (GTS) is to assist organisations and industries in the design and implementation of traceability systems based on the GS1 system of standards. At a strategic level, this standard aims to provide key insights and knowledge for organisations or industries that are developing long-term traceability goals.

Traceability is the ability to trace the history, application or location of an object [ISO 9001:2015]. When considering a product or a service, traceability can relate to:

- origin of materials and parts;
- processing history;
- distribution and location of the product or service after delivery.

GS1's approach to enabling supply chain traceability is focused on the use of open standards to provide visibility of objects that are relevant to supply chains. This document is intended to help organisations and industries to achieve global supply chain traceability by:

- Providing a methodology for organisations to use when developing requirements for the design of traceability systems that fit their needs and objectives.
- Serving as the foundational starting point for sector-specific, regional and local standards and guidelines.
- Enabling successful and interoperable communication across supply chains by providing consistent ways to identify traceable objects and to create and share standards-based data about the movements or events of those objects over the course of their lifetime.
- Enabling scale and adoption by applying existing and proven standards, and so avoid fragmented approaches to use cases beyond traceability.

1.2 Scope

The GS1 Global Traceability Standard is intended for use across end-to-end supply chains and is relevant to all events that span the lifecycle of a traceable object, including:

- The transformation and processing of raw materials, ingredients, intermediate products, components and components into the product.
- Aggregation and disaggregation of products and linkage to assets (e.g., returnable assets).
- Transport and distribution, including cross-border trade.
- The maintenance, repair and overhaul operations across multiple cycles of usage or service of the product.
- Consumption of products, including dispensing and administering.
- The disposal and destruction of the product and the recycling of materials.

This document assumes that each individual organisation will have its own objectives when establishing the traceability systems and tools that drive their business. To succeed, each individual organisation will need to ensure that their systems are **interoperable** with systems of other organisations across their supply chains.

This document focuses on the **data management** aspects of traceability. It identifies and references the necessary requirements for capturing and sharing data using a simple model that works across known and trusted chains of custody or ownership. Traceability data is captured and shared across the “who, what, when, where and why” dimensions, in order to provide applications with sufficient **business context** to effectively use the data.

It also provides a foundation to enable data sharing across more complex supply chains, where parties need to find and retrieve information from companies that are not their direct trading partners and where trust may need to be established before data can be shared.

This document is **sector and product neutral**. The principles can be applied to supply chains across many sectors, including food and beverage, apparel, pharmaceuticals, medical devices, humanitarian logistics, technical equipment and components.

This document is also designed to be **technology neutral**. It is based on the foundational principles that are at the heart of the GS1 system of standards: Identify – Capture – Share. These foundational principles are used to explain how the GS1 system of standards can be used to enable traceability solutions. The document references a variety of data capture and data sharing technologies and related GS1 standards, including GS1 barcodes, EPC/RFID, GDSN, EDI and EPCIS.

The GS1 Global Traceability Standard does not aim to compete with other international standards that address traceability requirements such as those from ISO, those benchmarked by the Global Food Safety Initiative (GFSI) or other certification schemes but rather complements and completes them. Where these standards define “what” should be done, the GTS helps companies and organisations to understand “how to” meet these requirements using standardised traceability data.

1.3 About GTS version 2

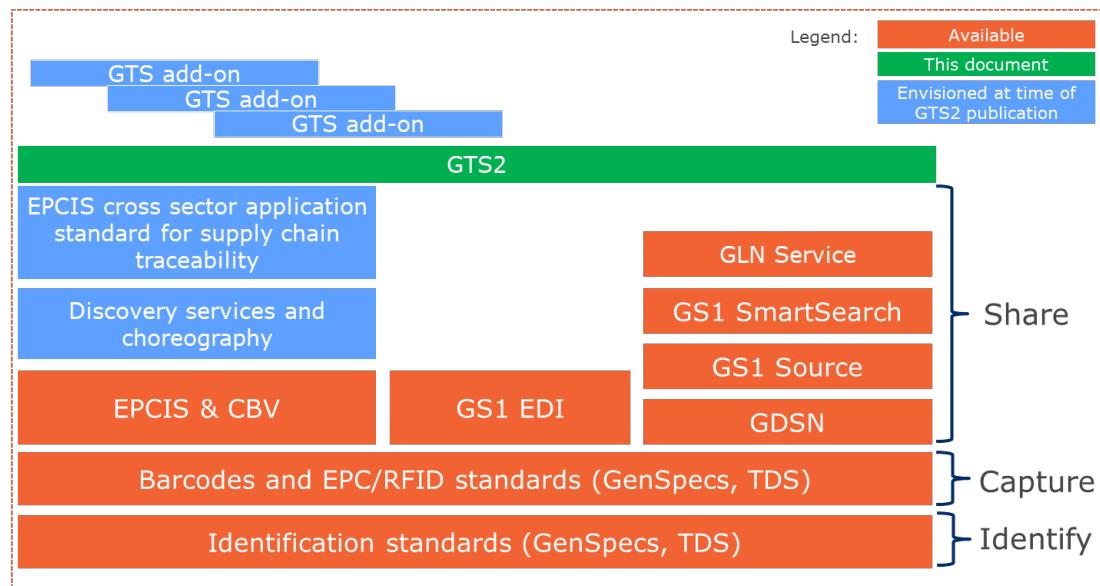
GTS version 1 established the foundation for standards-based traceability systems by addressing the needs for:

- globally unique identification of products, locations and parties;
- labelling of all products and levels of packaging;
- data capture and recording;
- enabling access to the data;

with clearly defined responsibilities along the entire value chain.

This second version of the GTS builds on the foundation established in version 1. In GTS version 2 a layered approach to traceability is introduced, in order to better suit the variety of traceability needs of increasingly dynamic supply chains and in order to embrace all capabilities offered by today's information technologies.

Figure 1-1 GTS version 2



GTS2 is a generic document that builds on the GS1 standards for identification, data capture and data sharing. As shown in the figure, it is expected that additional standards and guidelines will need to be developed to enhance the GS1 standards.

Furthermore, the figure illustrates that GTS2 is expected to serve as a foundational reference document that will be augmented by sector-, industry-, domain-, product- and region-specific

standards and guidelines. It is expected that this approach will ensure fast development of materials relevant to newly-identified business challenges.



Note: As a first step a GTS implementation guideline will be developed (see appendix C).

1.4 How to use this document?

This document is intended for use by organisations of any size and for all supply chain parties and stakeholders. If you or your organisation have a need to access or share traceability data, this document will be a relevant reference for you.

- Section 2 provides an overview of the GS1 traceability framework.
- Section 3 goes deeper into the traceability data management aspects, and provides a generic example.
- Section 4 explains how GS1 standards enable the creation of interoperable traceability systems.
- Section 5 defines the key requirements for interoperable traceability systems.
- Appendix A contains a summary of the interoperability requirements.
- Appendix B provides an overview of the data management responsibilities.
- Appendix C describes a step-by-step method for the design and implementation of traceability systems.
- Appendix D provides sectorial examples and references to GS1 resources.
- Appendix E contains a list of people and organisations that contributed to this document.

2 Traceability and the importance of standards

2.1 Business drivers

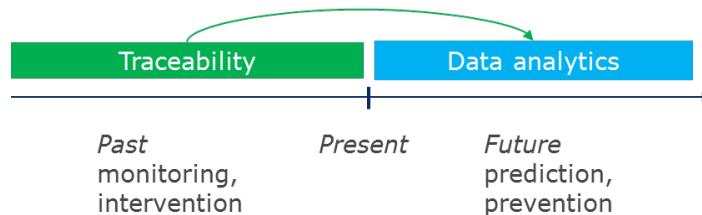
Traceability has become a strategic priority for organisations around the world. In addition to enabling increased supply chain quality, efficiency and transparency, the sharing and use of traceability data enables the development of solutions that enhance supply chain security and safety.

The importance of data

Traceability enables access to relevant data so that data can be analysed and decisions can be made. Data accessibility is key to drive speed of response and precision of analysis. It involves gathering, storing, and reporting detailed information about every important event throughout supply and production. That information can then be used in many different ways to improve operations or to resolve seemingly unrelated challenges.

Traceability data can be leveraged for much more than crisis-resolution. Data and related methods such as data analytics have become one of the most important ways for organisations to control and proactively monitor their supply chains.

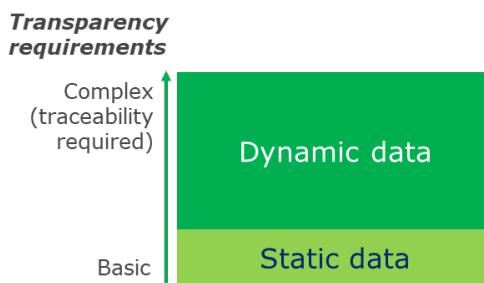
Figure 2-1 Traceability - enabling better decision making



Note: Traceability data will not be the only source for effective data analytics. Various other sources, such as weather information, geographic data, demographic data, will be applied.

Transparency, which refers to the need to ensure visibility and access to accurate information across supply chains (inclusive of consumers), is often an important driver for traceability projects. Some transparency requirements may be fulfilled by using static data about customers, suppliers, products and production conditions. Requirements that are more complex will require static data as well as dynamic data related to the actual supply chain events and transactions that occurred, i.e. traceability. See section [3.3](#) for more information on traceability data.

Figure 2-2 Transparency, traceability and required data



Market pressures and regulatory demands

The supply chains of today are long and complex. They often intersect with a multitude of other supply chains, making traceability a multi-party and multi-chain challenge.

Market pressures and emerging regulations are critical drivers of traceability. A complicating dimension to traceability is compliance with varying and evolving regulations. In today's global

economy, supply chain traceability involves complying with multiple jurisdictions for each country and region involved in the supply chain.

As a result, each organisation may face a multitude of internal and external traceability requirements. This document is designed to ensure that the basic data sharing needs of these complex and long supply chains are explained in a way that is relevant to all.

Cross-functional

Because the sharing and use of traceability data can impact so many aspects of business operations, it should be no surprise that traceability tools and solutions are relevant across many functions and departments in an organisation, including but not limited to:

- Quality & safety teams (risk management, recall readiness, audits, management of errors and incidents, expiry date management, stock rotation).
- Compliance teams that are concerned with regulation and organisational requirements.
- Consumer-facing teams that need to share relevant information.
- Internal teams that are tasked with fighting counterfeiting, enabling supply chain security or brand protection.
- Social responsibility teams focused on ethical and environmental topics.
- Product life cycle management teams.
- Teams responsible for transport and logistics.
- Systems development and management teams.

People responsible for such a variety of functions will often have different perspectives on the needs of traceability systems and tools. All of these different perspectives are important, and this document aims to build a common understanding of needs by:

- Creating a common language when talking about the data management aspects of traceability
- Defining principles for the creation of interoperable traceability systems that can serve the needs of all these stakeholders

2.2 The need for unique identification

At the heart of any traceability system is the identification of traceable objects.

A **traceable object** is a physical or digital object for which there is a need to retrieve information about its history, application, or location. Examples of traceable objects include products (e.g., consumer goods, medicines, electronic devices), logistic units (e.g., palletised goods, parcels) and assets (e.g., trucks, vessels, trains, fork lifts).

For the physical identification of traceable objects, generally three main levels of identification can be distinguished (see section [4.1.1](#) for more information):

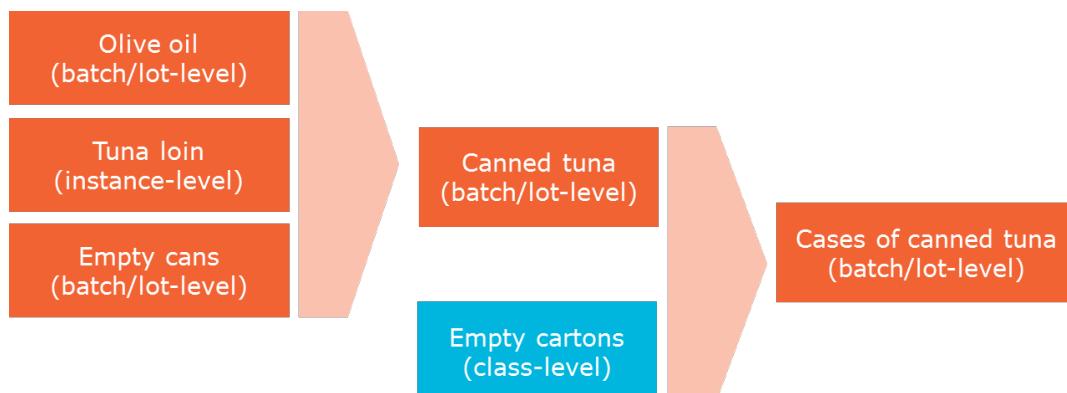
- **Class-level identification**, where the object is identifiable by its product / part ID, enabling it to be distinguished from different kinds of products or parts.
- **Batch/lot-level identification**, where the product / part ID is extended with a batch/lot number, limiting the number of traceable objects with the same ID to a smaller group of instances (for example, items produced at the same time).
- **Instance-level identification**, where the traceable object is identified with a serialised ID, limiting the number of traceable objects with the same ID to one individual instance.

The objectives of the traceability system and the supply chain itself are key criteria to determine the right level of identification. For example, products and ingredients associated with high risks will always be identified at batch/lot- or instance-level.

Companies will often apply a combination of identification levels. This is for example a common practice in transformation events arising in manufacturing, where the inputs in a manufacturing process include primary and secondary ingredients / materials. Taking the example of making canned tuna (see figure 2-3), primary ingredients / materials would comprise tuna loin, olive oil and

cans, whereas empty cartons (in which the cans are packed into) would belong to secondary materials.

Figure 2-3 Example of combination of identification levels



- ✓ **Note:** The empty cartons are shown in a different colour, since they are identified on class-level. This provides transparency but no real traceability. See also section [3.3.2](#).

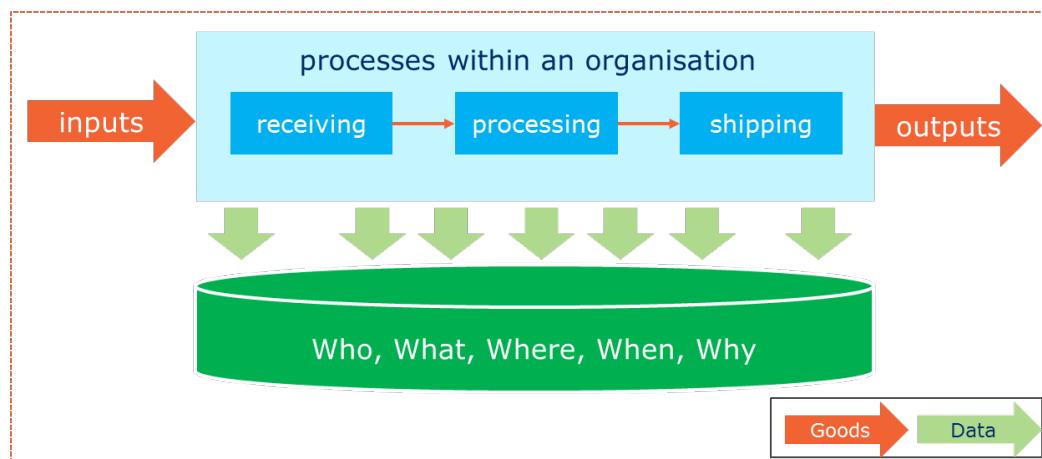
Another example is the combined use of instance-level and batch/lot level on the same product: Each individual product gets a serialised ID, but the distribution units (e.g. outer cases) are identified on batch/lot-level for use by the supply chain and logistics systems of supply chain partners.

The time and cost to implement will vary greatly for each identification level. There is no 'one size fits all', and coordination with supply chain partners is essential when defining the identification levels that your organisation (and your supply chains) will require.

2.3 The need for traceability data

Traceability systems are powered by traceability data. Traceability data is generated through execution of a variety of business processes carried out by each organisation.

Figure 2-4 Generation of traceability data - single company view



Each time a traceability-relevant process is executed in any organisation, traceability data is generated. This data provides business content to applications that use the data, and includes information that spans five important dimensions: Who, What, Where, When and Why.

- **Who:** Which parties are involved?

Uniquely identified entities involved in the handling, custody or ownership of the objects moving through the supply chain. Where there is a need to distinguish the entity and their role in the process, it is valuable to include this.

- **What:** What is the primary object being traced? Which related objects need to be traced?

Uniquely identifying objects that move through the supply chain is critical. These may be individual products as well as shipments of products. They may also include other physical or virtual objects such as transport means, equipment (including returnable transport items) and documents.

- **Where:** Where did these movements or events take place?

Uniquely identified locations are critical to understanding the path an object takes across a supply chain. It may be a manufacturing site, a specific production line, a warehouse, a field, an ocean, a point of sale, a hospital, ship or rail car.

- **When:** When did a movement or event that included that object occur?

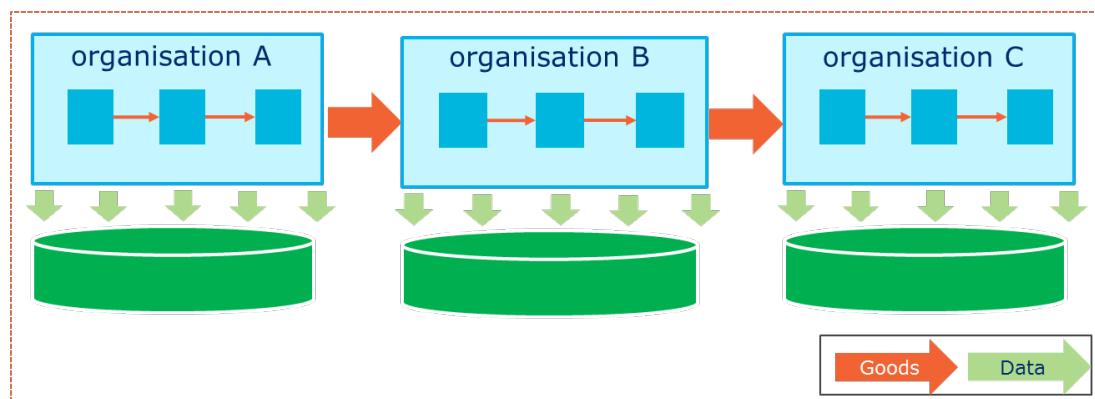
The date, time and timezone when a specific event occurred provides the timeline of an object's movement through the supply chain.

- **Why:** What happened? What business process was happening at the time the event took place? What business transactions were taking place? Why was the object at that location at that time?

This tells the story of the object. It provides the business context around the events that have occurred. Shipping and receiving events represent changes in a chain of custody or ownership, while a dispensing event may indicate that a particular medicine was given to a patient. In manufacturing, transformation events represent when one or more ingredients were irreversibly combined to create one or more new outputs or products.

When we extend the view to a full supply chain, it becomes clear that each organisation will manage its own set of traceability data. In order to achieve end-to-end supply chain traceability, it will be necessary to access and combine data from multiple organisations.

Figure 2-5 Generation of traceability data - supply chain view



2.4

The need for interoperability and standards

An organisation's traceability system will need to support a multitude of applications and use cases, from risk management to supply chain efficiency, regulations, sustainability, and consumer trust or brand integrity. It should be adaptable, because needs will evolve over time. It should leverage investments based on proven technologies and make use of what is already in place (e.g., logistic labels, barcode scanners) within each company and/or its trading partners as much as possible. Solutions should also enable easy integration with new system components.

A system that is implemented to meet internal traceability requirements may not be able to interoperate with systems of other parties in the supply chain. In order to ensure an appropriate level of interoperability, organisations will need to ensure that their systems are all built on a

common set of standards. This does not mean that all actors in the supply chain need to use the exactly the same systems, but their systems will need to be able to support standardised data.

Variety of objectives and requirements

Individual companies have different objectives and needs when implementing traceability solutions. These differences are attributable to many factors, including product, supply chain role, regulatory and business environments, cost/benefit strategies and available enabling technologies.

In addition, many products cross geographic borders at least once in their lifecycle, subjecting them to multiple regulations, which can include mutually inconsistent requirements.

In order to realise the ultimate goal of end-to-end supply chain traceability, all partners of a specific industry or supply chain must use a foundational set of standards.

Variety of solutions and tools

Various information technologies and tools are available on the market to support traceability implementations. Commonly, multiple system components need to work together to deliver an overall system. These may include a system for managing product identification and master data, one or more solutions for automatic identification and data capture (AIDC) and other systems to capture transactional or event data about a product's path through the supply chain.

Parties in a supply chain may also have different levels of technical maturity. They may have chosen different technologies, or may have implemented the same technology in different ways (using different software or platforms).

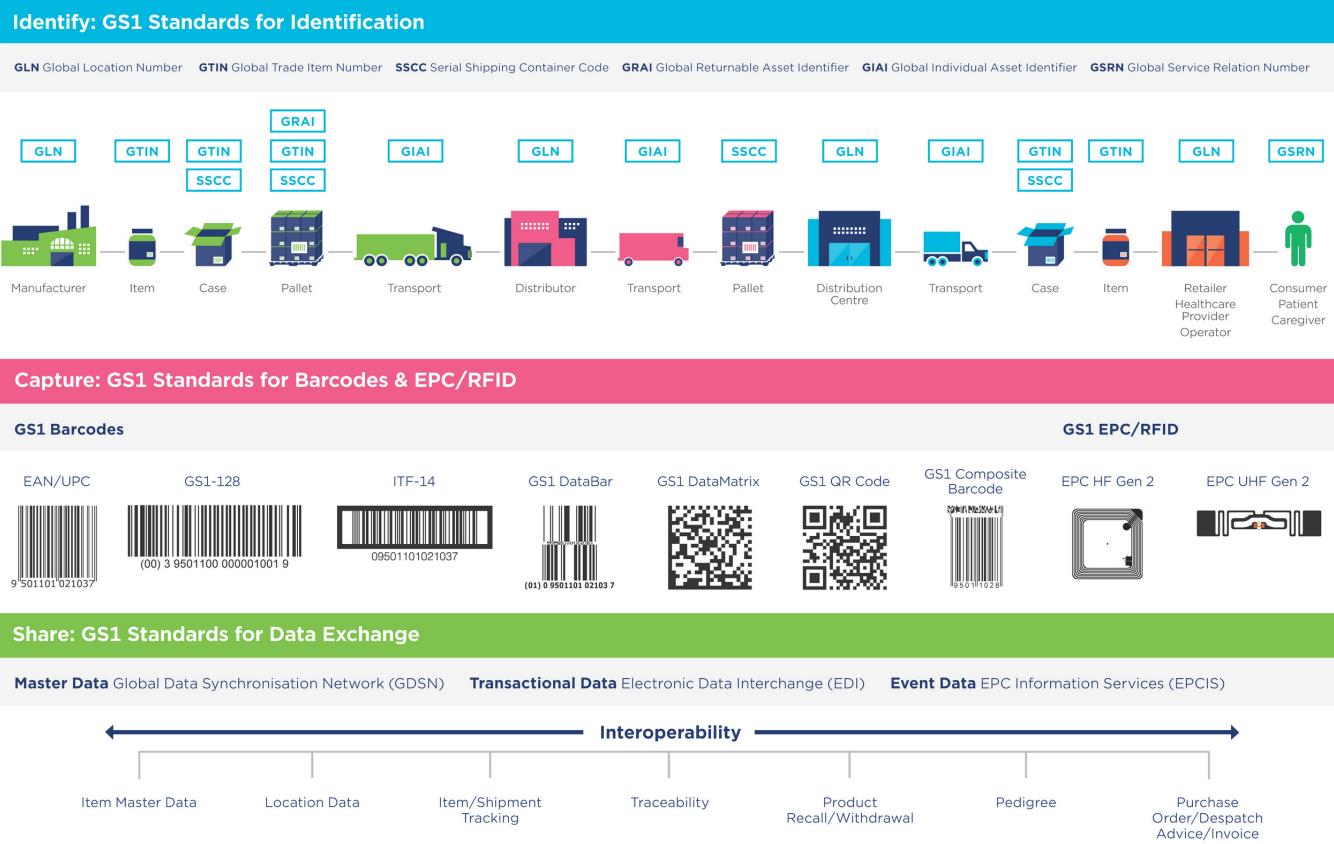
Standards-based systems and components are, to a certain level, naturally interoperable with other systems and components that conform to the same standards.

2.5 GS1 standards – key enabler for interoperability

GS1 system of standards

The GS1 system of standards provides a comprehensive set of standards to identify, capture and share information about objects throughout their lifecycle, providing the core foundation for interoperability:

1. Supply chain partners **identify** business objects and locations using standardised identifiers.
2. Supply chain partners **capture** an object's identity and any additional attributes (e.g. the expiry date) that have been encoded in a standard manner in a data carrier (barcodes, RFID). This ensures the object can be read automatically and consistently throughout the supply chain. Thereby, also the time (when), location (where) and other data (who and why) are recorded.
3. Once supply chain partners are using a common language for identification and data capture, the gathered data is refined and enhanced with business context, to transform it into data that can be **shared** using standardised semantics, in a standardised format, and using standard exchange protocols.

Figure 2-6 The GS1 system of standards


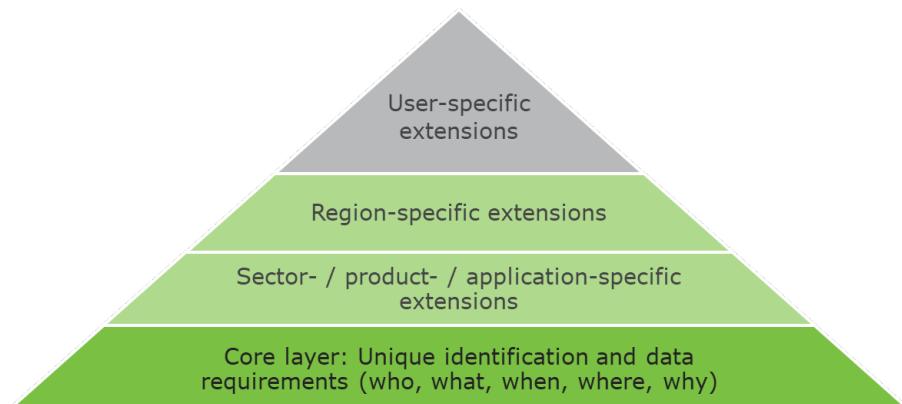
Note: See <http://www.gs1.org/standards> for more information.



Note: Not depicted in the diagram is the GS1 Global Product Classification (GPC) standard. GPC codes are static codes that are used to group similar products. The GPC can be used to aggregate data across suppliers, for example to show the origin of a certain type of crop by country. For more information see <http://www.gs1.org/gpc>.

Framework for interoperable traceability systems

This document provides a framework for the creation of interoperable traceability systems based on the GS1 system of standards. It defines the minimum elements that are needed to achieve interoperable traceability systems, and describes how additional elements can be added to address requirements of specific sectors, product categories, regions and application areas.

Figure 2-7 GTS framework for interoperable traceability systems


At the foundation, the core of the framework is designed to cover the base requirements of all sectors, regions, applications and trading partners.

The core can be extended to include sectorial and regional layers that are designed to address specific requirements, for example regulatory requirements.

On top of that, the system can be further tailored to address requirements based on supply chain partner relationships and agreements that may need to be considered.



Important: Whenever possible, user-specific (non-standard) extensions should be avoided, since they will add complexity and cost for other parties in the supply chain and reduce interoperability.

Besides fully GS1-based implementations, the GTS framework also supports hybrid implementation, where GS1 standards are combined with non-GS1 standards (e.g., ISO) or legacy solutions. Some examples:

- Animal identification (a regulator assigned ID may be mandatory)
- Intermodal container identification (the BIC code, covered by an ISO standard, is formally approved for use in the GS1 EPCIS standard)

The conditions and rules under which non-GS1 standards may be applied will need to be precisely defined, in order to prevent duplicate solutions for the same business need.

Finally, the GTS framework provides a path for organisations to increase the interoperability of their traceability system. Industry sectors may, for example, be progressing towards adoption of certain identifiers (i.e. GLNs) and data sharing standards, but may not yet have reached 100% adoption.

3 Traceability data and traceability systems

3.1 Traceability data within an organisation

When it comes to traceability data, an organisation should first look at its internal business processes. The organisation should identify which steps in those business processes are important from a traceability perspective. Subsequently, the organisation will need to establish processes to define and capture all of the relevant data about these business process steps, which will enable the effective use of the data within and outside of the organisation.

Business processes will extend across a variety of departments of the organisation, and therefore a common language is critical to implementations of data capture solutions. At the core of this are two concepts:

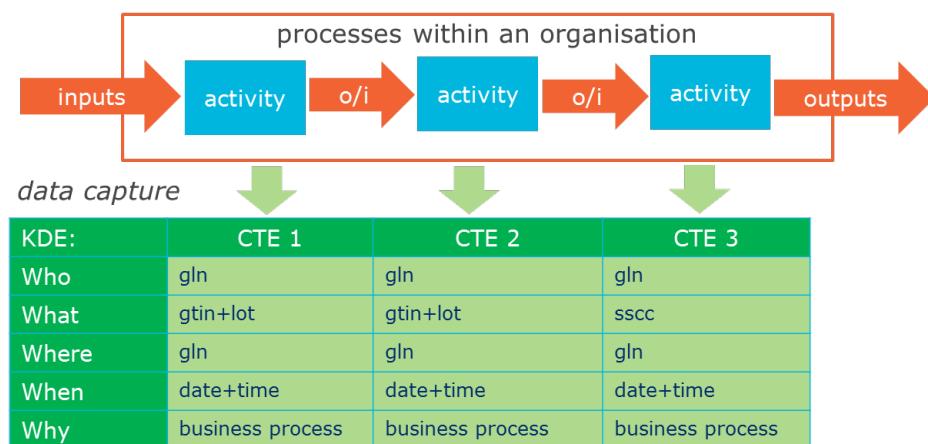
- Critical Tracking Events (CTEs)

These are the actual events that occur to the traceable objects during their lifecycle, such as receiving, transforming, packing, shipping, transporting.

- Key Data Elements (KDEs)

These are the pieces of data that describe the actual instances of the CTEs. The data will commonly cover the five dimensions (Who, What, Where, When, Why) described in section [2.3](#).

Figure 3-1 Critical Tracking Events (CTE) and Key Data Elements (KDE) - example



End-to-end supply chain traceability extends the responsibilities of the organisation to include the exchange of data outside of the walls of any one enterprise (see section [3.2](#)).

Each member of the supply chain should, at a minimum, be able to trace back to the direct suppliers of traceable objects and to track forward to the direct recipients of traceable objects (in some cases even including end-consumers). This enables the possibility for all parties to gain access to relevant data further upstream and downstream through queries of direct trading partners (often referred to as a “one-up, one-down” approach, described in more detail in section [3.3.5](#)).

3.2 Traceability data across supply chains

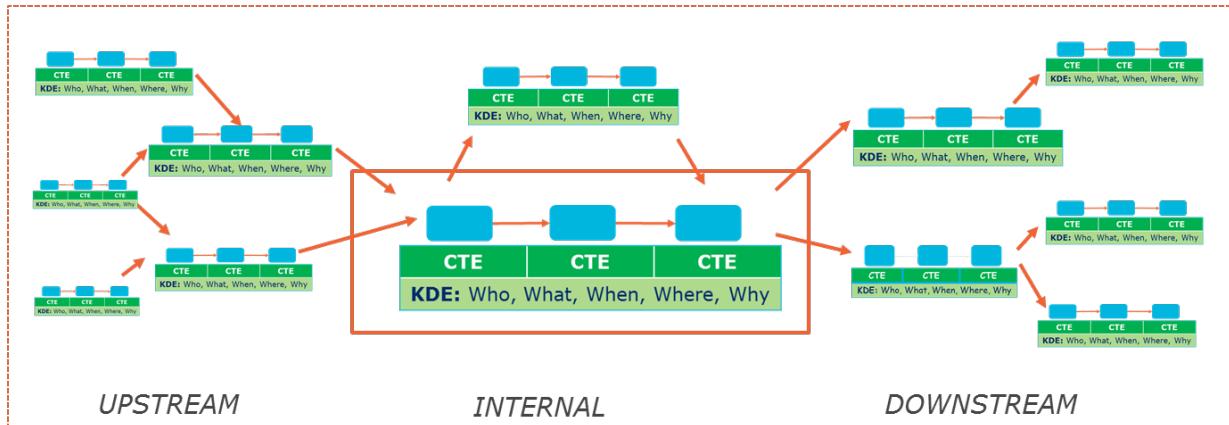
Supply chains involve multiple operators that are interdependent (in terms of traceability). Whether you are an upstream materials provider or a downstream retailer, all parties trading and/or handling traceable objects have a shared responsibility when it comes to achieving full-chain traceability.

Although each party will have its own traceability system, these solutions will need to understand each other and be able to exchange data with each other. This is even true in cases of shared traceability systems (such as vertically integrated retail operations). The design of each individual system will be based on the traceability responsibilities of each party in the end-to-end supply chain, and may be influenced by outside forces such as regulation.

End-to-end traceability refers to the ability to track and trace an object through its entire life cycle and through all parties involved in its production, custody, trade, transformation, use,

maintenance, recycling or destruction. Traceability requirements may extend from all the way upstream (suppliers of raw materials, ingredients and components) to all the way downstream (customers of finished goods including end-consumers).

Figure 3-2 Traceability data across supply chains



Because of the complexities inherent to most supply chains, each party will need to ensure traceability data can flow in two directions (upstream and downstream). Systems will need to support parties querying for data that may exist upstream or downstream from the organisation. As explained in section 2, standards for the identification, capture and sharing, are a key enabler in achieving the required interoperability to establish connections between the systems of the different parties.

Emergent supply chains

A significant challenge for traceability systems is that, for most products, the chain of custody and chain of ownership are not defined in advance. Instead, they are usually chains or paths through a supply chain network that emerge over time, during the course of normal supply chain operations. We call these supply chains "emergent".

For example, instances of a product that are manufactured and shipped together may ultimately reach different destinations, and the manufacturer or brand owner will typically have no knowledge of the routes taken by the individual instances of the product. Similarly, upstream, a party often does not know the identity of the suppliers of its suppliers (tier 2 suppliers and beyond). Such relationships may represent sensitive commercial information, and the further upstream one goes (tier 3, 4, 5 etc.), the less visibility there may be regarding the parties that were involved.

Because of these complexities, it is essential to be able to understand, through some means of discovery, which parties were participants in a supply chain activity and who may have relevant traceability data. Furthermore, when parties do not have a direct business relationship with one another, some means of establishing trust is critical, as commercially sensitive data may be included or derived.

See section [4.3.3 Data discovery, trust and access control](#) for more information.

3.3 Managing traceability data

Traceability data originates from a variety of functions and processes within companies, including design and quality control data for the product; production process data; procurement data and logistics and distribution data. Several departments may need to be involved and several internal systems may need to play a role. Some of the data can be commercially sensitive and may require special processing or partial redaction before being made available to third parties.

Some data will be more stable over time (e.g., master data) and can be communicated in advance of receipt of traceable objects. Other data will be added whenever relevant critical tracking events or transactions occur.

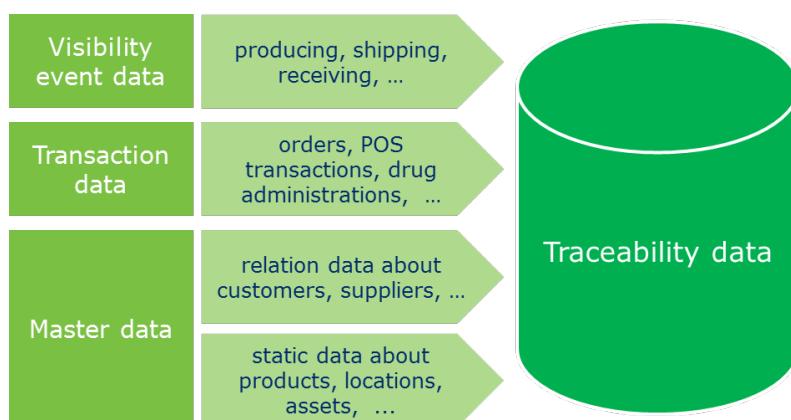
The volume of traceability data that is collected over time can be quite significant, creating challenges in terms of time and cost to collect, store and provide access to the data. Preparation for data retention should be considered to manage these challenges.

3.3.1 Sources of traceability data

There are four sources of data that contribute to what we define as "traceability data". These four data sources may be managed in different systems of an organisation, but together they provide the information that is critical in understanding the full context of traceability data.

- **Master data:** Master data are the single source of common business data used across all systems, applications, and processes for an entire organisation.
 - *Static master data* (referred to as "static data" throughout this document) typically exists to describe products, parties, locations, and assets.
 - *Master data about supply chain relations* (referred to as "relation data" throughout this document) typically exist to describe the supply chain partners of an organisation (i.e. its suppliers and customers), specified by product category and location. When relation data are linked across organisations, this enables the creation of a complete map of the supply chain (upstream and downstream). And, when relation data are enhanced with qualitative data such as certifications, this helps organisations to gain insight in environmental, ethical and safety aspects of the supply chain.
- **Transaction data:** Transaction data are recorded as a result of business transactions, such as the completion of a transfer of ownership (e.g. orders, invoices) or a transfer of custody (e.g. transport instruction, proof-of-delivery). Transaction data may be recorded with the aid of electronic data exchange (EDI) and AIDC techniques (e.g., POS scanning, bedside scanning).
- **Visibility event data:** Visibility event data are records of the completion of business process steps in which physical or digital entities are handled. Each visibility event captures what objects participated in the process, when the process took place, where the objects were and will be afterwards, and why (that is, what was the business context in which the process took place). Unlike the other types of data, visibility event data are often specifically recorded for visibility and traceability purposes. Visibility event data will often be captured using AIDC techniques such as barcodes or RFID.

Figure 3-3 Sources of traceability data



3.3.2 Precision of traceability data

The precision of traceability data is determined by two main dimensions:

1. The level of identification of the traceable objects (products and resources),
2. The granularity at which traceability data is recorded.

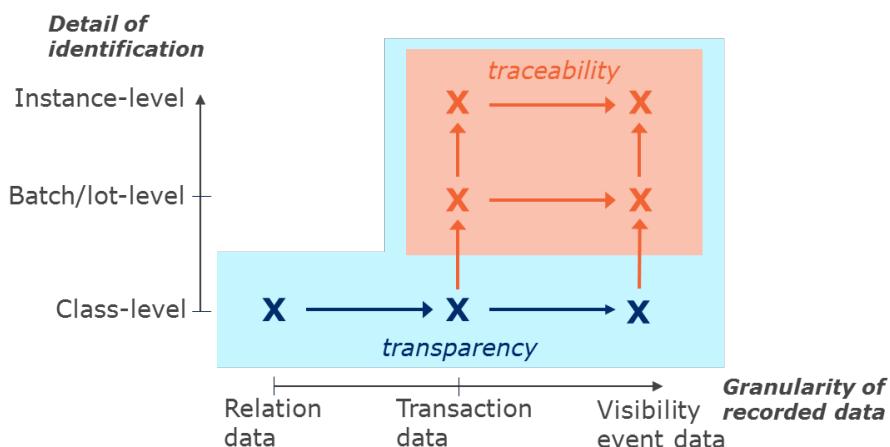
Together these two dimensions provide organisations a way to establish the optimal level of precision.

As illustrated in figure 3-4 the combinations with the lowest precision help to provide transparency, which is a basis for traceability. The combinations with the highest precision help to provide traceability, enabling organisations to locate specific traceable objects in a supply chain.

Visibility event data recorded at serial level provide the highest fidelity in the sense that:

1. Visibility event data record the completion of each business process step, including 'internal' processing steps that do not directly refer to specific transactions between trading parties.
2. A serialised object can only exist in one place at any point in time, so it makes a single unambiguous path through the supply chain network.

Figure 3-4 Precision of traceability data



The following example illustrates how these combinations apply to trade items:

- Trade items may be identified at class-level (GTIN), lot-level (GTIN + batch/lot ID) or instance-level (GTIN + serial ID).
- Data may be available about the relations, transactions and visibility events that involve the trade item.

This leads to the following possible levels of precision in the available traceability data:

Table 3-1 Precision of traceability data for trade items

Detail of identification	Master data about relations	Transaction data	Visibility event data
GTIN	The suppliers / customers per trade item.	The suppliers / customers and related transactions (such as orders and invoices) per trade item.	The suppliers / customers and related events (such as manufacturing, picking, packing, shipping) per trade item.
GTIN + batch/lot ID		Same as above, but specified at batch/lot-level.	Same as above, but specified at batch/lot-level.
GTIN + serial ID		Same as above, but specified at serial-level.	Same as above, but specified at serial-level.

3.3.3 Sensitivity of traceability data

An important aspect to consider is the potential sensitivity of the traceability data that an organisation may choose to share with other parties.

Generally, a distinction can be made between internal data —data not suitable for sharing with other parties, for example due to commercial or privacy reasons— and external data —data suitable for sharing with other parties if certain pre-defined conditions are met—. See [Table 3-2](#) for examples of data that may be treated as internal vs external by an organisation.



Note: The organisation will also need to consider access restrictions to any internal data that may be shared across organisational lines. Internal access restrictions vary widely across industries and regions.

Table 3-2 Example of internal vs external data of an organisation

Sensitivity of data	Master data		Transactional data	Visibility event data
External data	<i>Static data:</i> <ul style="list-style-type: none"> ▪ Locations ▪ Catalogue items ▪ Assets ▪ ... 	<i>Relation data:</i> <ul style="list-style-type: none"> ▪ Suppliers ▪ Customers ▪ 3rd party service providers ▪ ... 	<ul style="list-style-type: none"> ▪ Purchase orders ▪ Despatch notifications ▪ Transport instructions ▪ ... 	<ul style="list-style-type: none"> ▪ Producing ▪ Picking ▪ Packing ▪ Shipping ▪ Receiving ▪ ...
Internal data	<ul style="list-style-type: none"> ▪ Product design ▪ Production process ▪ Personnel ▪ ... 	<ul style="list-style-type: none"> ▪ Contracts ▪ ... 	<ul style="list-style-type: none"> ▪ Quality inspection data ▪ Lab analysis results ▪ .. 	<ul style="list-style-type: none"> ▪ Inspecting ▪ Collecting ▪ Holding ▪ ...

As such, this standard focuses mainly on the sharing of external traceability data.

3.3.4 Quality of traceability data

The quality of data provided by each trading partner is critical because inaccurate data which is shared between trading partners could affect other business processes like a trace request or recall activity.

Establishing and maintaining a good quality level of traceability data is a major challenge. Some important aspects are:

- Completeness: Are all relevant data recorded?
- Accuracy: Are the recorded data accurately reflecting what happened?
- Consistency: Are the data aligned across systems
- Validity: Are the data time-stamped, to ensure the validity timeframe of data is clear?

3.3.5 Sharing of traceability data

When it comes to providing access to traceability data to supply chain partners or other stakeholders, five main models (traceability choreographies) can be distinguished. They result from the different ways in which traceability data can be systematically stored and made available to other parties.

The following example illustrates how the five different traceability choreographies compare, based on a simple scenario that involves three different organisations:

Figure 3-5 Traceability choreographies



In the **one step up-one step down** model the parties keep the traceability data in their own local system. Information requests are exchanged between immediate trading partners upstream or downstream. This model enables traceability data to be exchanged and partially checked between each pair of trading partners, and further upstream or downstream one step at a time.



In the **centralised** model the parties share the traceability data in a central repository and send their information requests to it.

Note that some centralised repositories (e.g. those operated by a regulatory authority) may only provide a capture interface but might not make the query interface available to all contributing parties, instead preferring to limit query access to the owner of the repository. Other centralised repositories may support different access control policies, providing query access to all parties – or based on supply chain role – or whether the querying party can prove that they are on the chain of custody / ownership / transactions for the objects specified in their query.



In the **networked** model the parties keep the traceability data in their own local system and stage it in a way that enables all supply chain partners (not only immediate trading partners) to query the data.

Networked models may differ according to the access control permissions about who is allowed to retrieve the data. In some models, any member of the community or network of supply chain partners may be entitled to query and retrieve data. In other models, access may depend on supply chain role, e.g. to prevent one manufacturer from querying a rival manufacturer's data; or access may depend on whether the querying party can prove that they are on the actual chain of custody / ownership / transactions for the objects specified in their query.



The **cumulative** scenario is a push method where the traceability data is systematically enhanced and pushed forward to the next party in the chain in parallel of the product flow. It enables sharing of upstream data with parties further downstream, but not the opposite.

This approach results in highly asymmetric visibility across the supply chain, in which downstream parties receive a complete copy of all relevant upstream data, while the upstream parties have no visibility downstream beyond their immediate 1-down customer. This approach can also be quite challenging for downstream parties to receive and process large volumes of traceability data, especially if the processing involves checking of multiple nested digital signatures.



The fully **decentralised and replicated** scenario is a mix of the cumulative scenario and networked scenario, and typical for the blockchain technology. The traceability data is systematically enhanced and all supply chain partners involved in the network keep a local copy of all data.



See section [4.3](#) for more information on the way the GS1 data sharing standards relate to the traceability choreographies.

3.4 Traceability systems

When we use the term "traceability system", we are referring to *the set of methods, procedures and routines used by an individual party to manage traceability in its supply chains*.

Traceability systems are used by individual parties to increase visibility across their own organisation and then to share that visibility data with upstream and downstream parties to contribute to end-to-end supply chain traceability.

Each organisation bases its traceability system on a careful balance between costs, benefits and risks. They will need to do so by taking their role in the wider supply chain context into account, since the needs of direct customers and end-customers will be an important consideration.

All traceability systems should be designed to mitigate risk and, as a by-product, enable visibility of the product's life cycle.

Components

A complete traceability system will include components that manage:

1. Identification, marking and attribution of traceable objects, parties and locations.
2. Automatic capture (through a scan or read) of the movements or events involving an object.
3. Recording and sharing of the traceability data, either internally or with parties in a supply chain, so that visibility to what has occurred may be realised.

Depending on the size of the organisation, multiple IT components may be involved, and the organisation will need to embed the traceability capability into these components.

Figure 3-6 Traceability capability in IT system components



Interoperability is an important factor in ensuring the seamless interplay between the various system components of an organisation.

Scope

The scope of the traceability system of a party will depend on the role of the party and the traceability questions that need to be addressed. Some elements that define the scope of a traceability system are:

- How many tiers up and down your supply chains will you need to share data?
- Will you need to interact with only direct supply chain partners, or will your system require a broader scope?
- Will you track main ingredients only, or also packaging and indirect materials?
- Will your system need to integrate data sharing with final consumers / end customers?

3.5 Traceability systems in action: An example

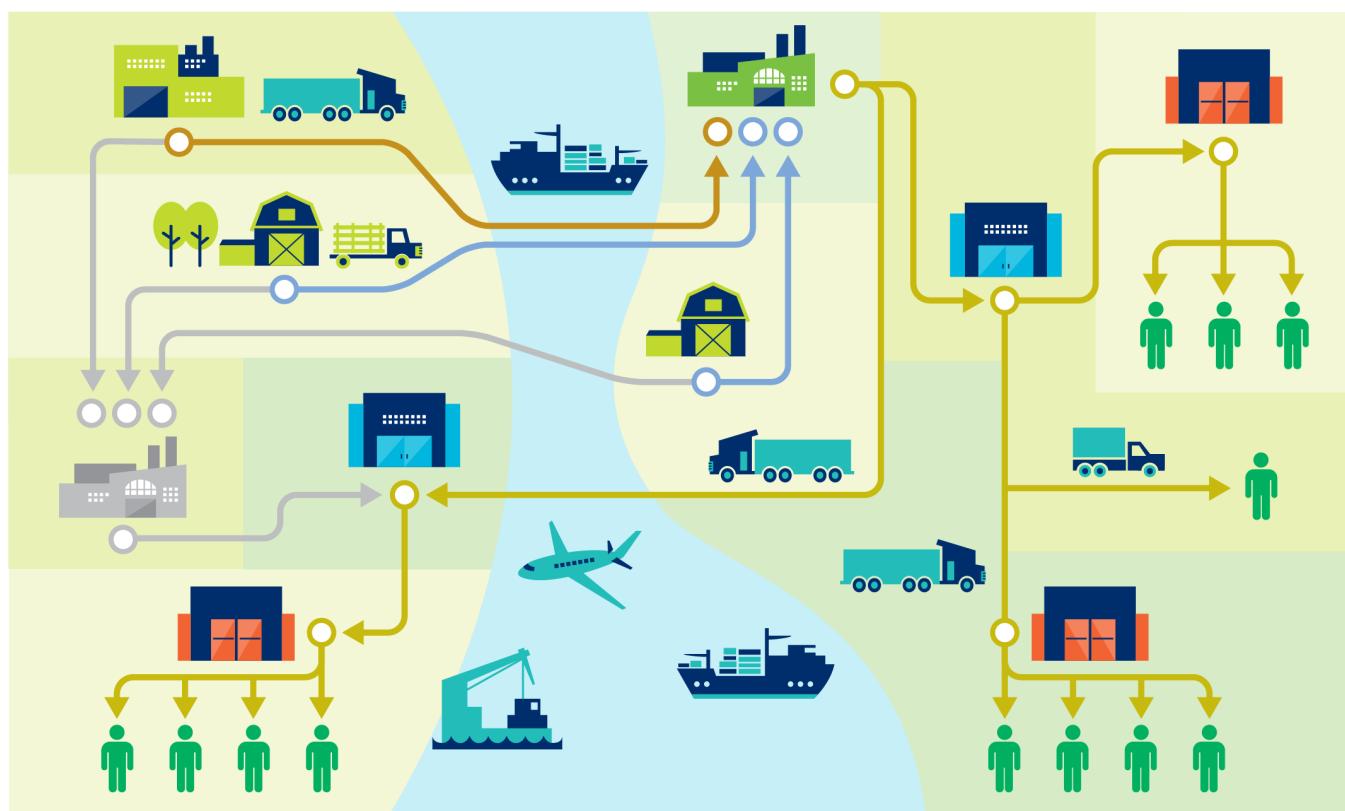
In this section a generic example is given that illustrates the functions of a standards based traceability system. In the example, globally unique identifiers are used for the trade items, logistic units, parties and locations. Automatic data capture techniques such as barcodes are used across the supply chain to gather the traceability data based on the activities in the supply chain.



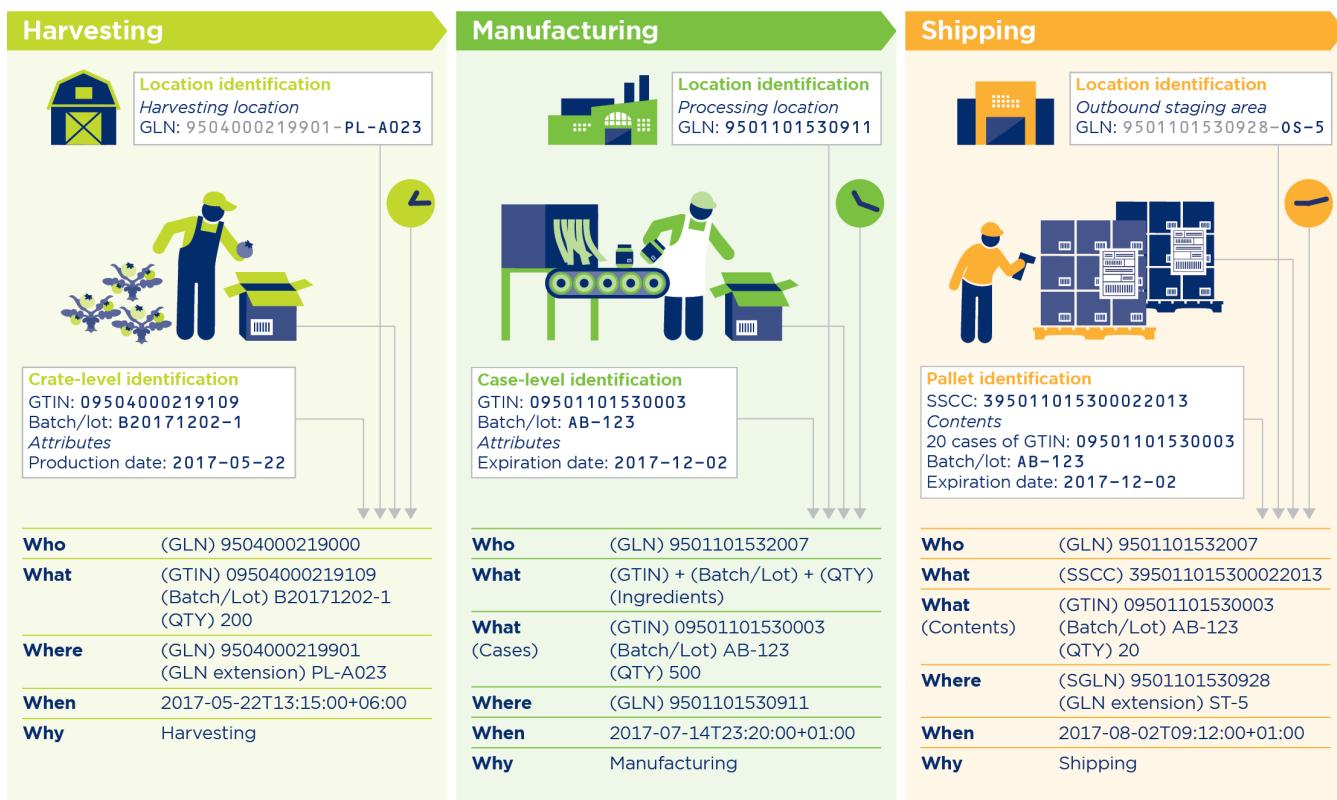
Note: See appendix D for sector-specific traceability examples

Figure 3-7 provides an overview of the supply chain. It illustrates how ingredients and packaging are supplied, transformed into products and distributed to the final customers.

Figure 3-7 Supply chain overview



On the next pages, figures 3-8 and figure 3-9 illustrate some of the business process steps that will occur at various points in the supply chain. Each step will lead to one or more critical tracking event (CTEs) for which key data elements (KDEs) need to be recorded.

Figure 3-8 Traceability data collection in business process steps (1)


Harvesting:

The producer harvests the crop and packs the products into in cases. Each of the cases gets a label with GTIN + batch/lot ID, and the related data are recorded.

Manufacturing:

The manufacturer transforms ingredients into final products. After that, the manufacturer packs the products into cases.

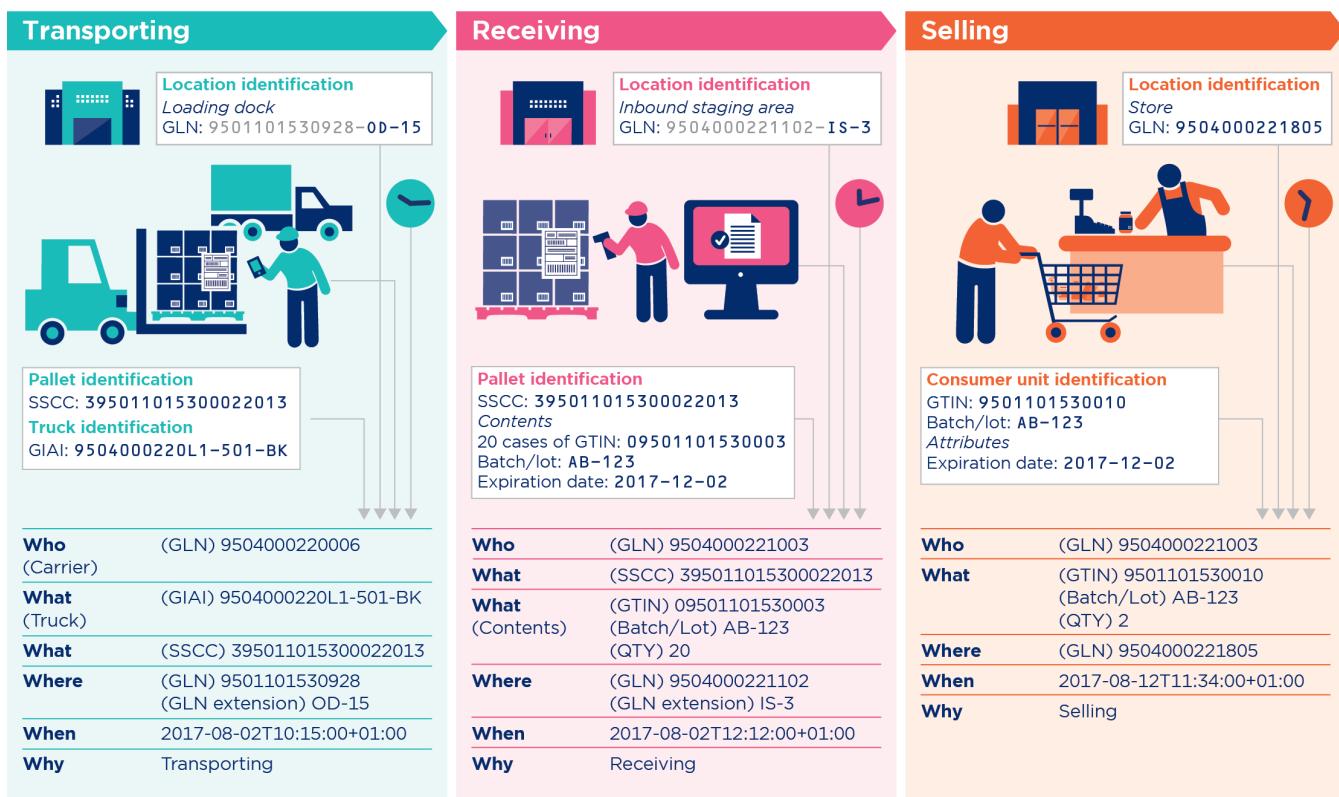
To maintain traceability the inputs and outputs of the process are recorded on batch/lot level.

Shipping:

The warehouse department picks the goods and packs them onto pallets.

To maintain traceability the warehouse records the links between product IDs (GTIN + batch/lot ID) and pallet IDs (SSCC).

Subsequently, the pallets are moved to the outbound staging area to be collected by the carrier.

Figure 3-9 Traceability data collection in business process steps (2)


Transporting:

The carrier arrives and loads the pallets onto the truck. The driver uses his mobile device to identify each of the pallets. The link between the pallets and the truck is recorded. Now, by tracking the truck also the pallets and goods can be tracked.

Receiving:

The pallets arrive in the retail distribution centre.

The incoming goods department inspects the received goods by scanning the SSCCs on the pallet label and comparing the data against the pre-registered information in the system.

When all checks are ok, the goods will be marked as available in the inventory management system.

Selling:

The products have arrived at the store and have been placed on the shelves.

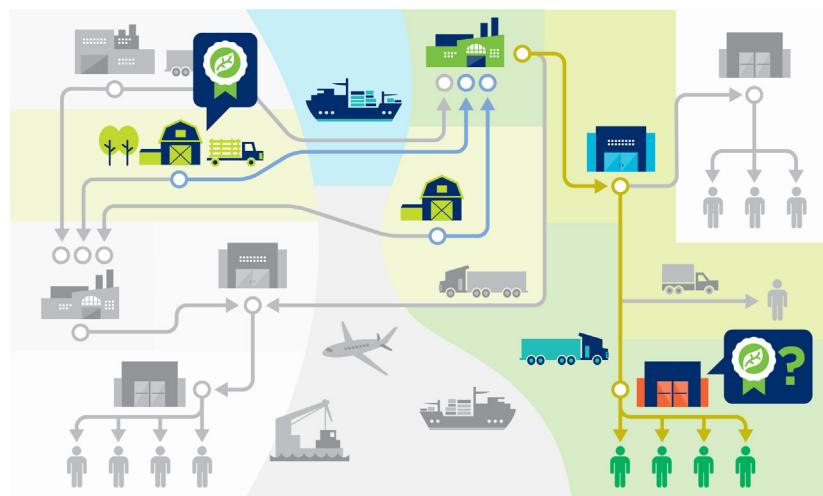
A consumer has decided to buy two products. At the checkout, the clerk scans the barcode on the products. The system automatically checks the expiry date.

The sales are recorded, in addition to the GTIN also the batch/lot ID is registered.

On this page, two examples are included that illustrate the way traceability data can be applied.

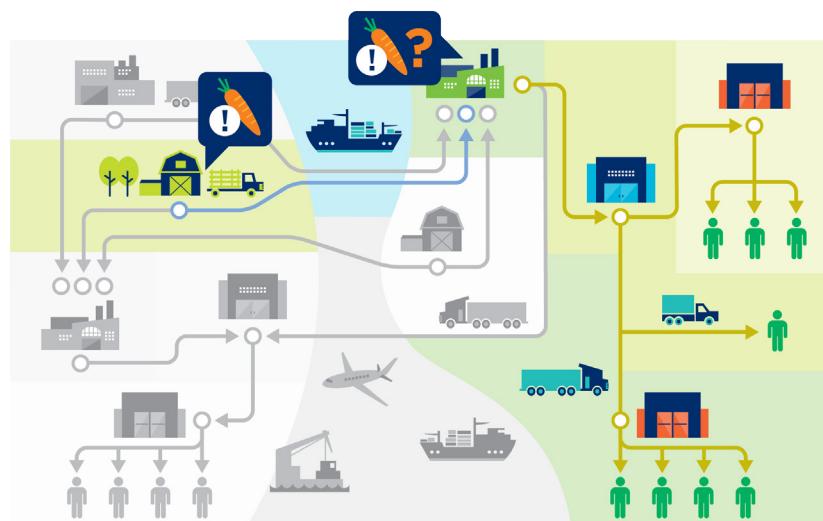
In the first example, figure 3-10, a retailer needs to find upstream information about the origin of a particular ingredient, which growers were involved and the quality certificates they have. By following the chain of custody upstream, the grower is located, and the required information is retrieved.

Figure 3-10 Data usage: Upstream query



In the second example in figure 3-11, a manufacturer needs to locate products of a specific batch/lot that need to be recalled from the distribution network. By following the chain of custody downstream all points in the distribution network where instances of the batch/lot were observed are identified, enabling a targeted recall.

Figure 3-11 Data usage: Downstream query



4 Key enablers for interoperable traceability systems

Traceability is a multi-party, multi-chain challenge. Therefore, alignment and collaboration with supply chain partners is essential. This is where standards come into play. Open supply chain standards enable interoperability between all parties by establishing a common set of rules for identification, data capture, data sharing and data usage.

The GS1 system is an integrated suite of global standards that provides supply chain visibility through the accurate identification, capturing, and sharing of information regarding products, parties, locations, assets, and services.

Using **GS1 identification keys**, companies and organisations around the world are able to globally and uniquely identify *physical things* like trade items, physical locations, assets, and logistic units as well as *intangible things* like corporations or a service relationship between distributor and operator. When this powerful identification system is combined with **data capture** and **data sharing** methods, connections can be made between these physical or logical things and the information that organisations across the supply chain need about them.

In summary, organisations can identify products and locations using a standardised product identification and standardised location identification method. Additionally, companies can capture the standardised identification in a common approach – barcodes and/or EPC/RFID tags. Finally, once companies are using a common language to identify and capture product data, the information can be shared in a standardised format, ensuring data completeness and accuracy.

4.1 Identification of objects, parties and locations

4.1.1 Traceable objects

A traceable object is a physical or digital object whose supply chain path can and needs to be determined. The table below lists the GS1 keys that are available for the identification of traceable objects.

Table 4-1 GS1 identification keys for traceable objects

Key	Full name	Type of objects being identified
GTIN	Global Trade Item Number	Types of products at any packaging level, e.g., consumer unit, inner pack, case, pallet.
SSCC	Serial Shipping Container Code	Logistic units, combination of trade items packaged together for storage and/or transport purposes; for example a case, pallet or parcel.
GSIN	Global Shipment Identification Number	Grouping of logistic units that need to be delivered together. Typically used by shippers to instruct transport providers or freight forwarders.
GINC	Global Identification Number for Consignment	Grouping of logistic units (that may belong to different shipments) that need to be transported together. Typically used by freight forwarders to instruct transport providers; for example, on a Master Airway Bill (MAWB) or a Master Bill of Lading (MBL).
GIAI	Global Individual Asset Identifier	Assets such as vehicles, transport equipment, warehouse equipment, spare parts.
GRAI	Global Returnable Asset Identifier	Returnable transport items such as pallets, crates, beer kegs, roll cages.
GDTI	Global Document Type Identifier	Physical documents such as invoices, tax forms, etc.
CPID	Component / Part Identifier	Components / parts that are produced and identified based on specifications of an Original Equipment Manufacturer (OEM), for example a car manufacturer.
GCN	Global Coupon Number	Paper and digital coupons.

Notes:

- GTIN and CPID only include a type reference, making these keys suitable for class-level identification. Only in combination with other attributes are they suitable for batch/lot-level or serial-level identification.
- GRAI, GDTI and GCN include a type reference and an optional serial component, which makes these keys suitable for class-level as well as instance-level identification.
- SSCC and GIAI only include a serial reference, and are instance-level identifiers.
- GINC and GSIN include a consignment or shipment reference and are used to identify groupings of logistic units.

Trade item identification

The GS1 system provides globally unambiguous identification keys to provide a common language for the communication of product information from company to company. The GS1 identification key for products is the GS1 Global Trade Item Number (GTIN). For decades, this GS1 identification key has facilitated the sharing and communication of product information among supply chain partners. Moreover, it has provided the foundation for innovative improvements in supply chain management for many industries.

GS1 standards provide a choice regarding the granularity of trade item identification, leading to varying degrees of precision as it pertains to traceability that can be achieved, as summarized in the following table.

Table 4-2 Trade item identification - precision levels

Granularity	GS1 identification key	Comments
Class-level	GTIN	<p>All products of a given type (e.g., 10 count cases of jars of jam) are marked identically.</p> <p>It is possible for an information system to tell one product from another (e.g., a 10 count case from a 24 count case), but not to distinguish two of the same product type (two separate 10 count cases of jars of jam).</p> <p>This is typically the least expensive kind of marking because the marking can be incorporated into package artwork that is printed in bulk.</p>
Batch/Lot-level	GTIN + batch/lot number	<p>All product of a given type (e.g., 10 count cases of jars of jam) within a given batch/lot are marked identically.</p> <p>It is possible for an information system to tell one product from another (e.g., a 10 count case from a 24 count case), and to distinguish two products of the same type from different lots/batches (a 10 count case of jars of jam from Lot #20100201 and a 10 count case of jars of jam from Lot #20100204), but not to distinguish two products of the same type within the same batch/lot.</p>
Instance-level (full serialisation)	GTIN + serial number (a combination also known as Serialised GTIN or SGTIN)	<p>Each specific occurrence of a given product (e.g., a specific 10 count case of jars of jam) is marked with a unique serial number, and so the combination of GTIN + serial number is a globally unique identifier for a single product instance, different from all other physical objects in the world.</p>

Reading from top to bottom, each choice gives increased ability to trace products in the supply chain, though at the cost of increased bookkeeping and cost of product marking.

Class-level identification (GTIN) provides the ability to see where different products are used in the supply chain, and to gather data based on counting products. This includes many inventory applications, sales analysis, etc. However, at this level, all instances of a given product are indistinguishable, which prevents real traceability.

Batch/lot-level identification (GTIN + batch/lot ID) provides the ability to distinguish products in one batch/lot from another batch/lot. This is especially useful in business processes that deal with quality issues that tend to occur on a batch-by-batch basis, such as a product recall of a contaminated batch/lot. Batch/lot-level traceability lets you identify all the places in the supply chain where a given batch/lot has reached, and confirm the quantity of items present from that batch/lot.

Instance-level, or fully serialised identification (GTIN + serial ID) provides the ability to identify each product instance individually. This allows each product instance to be tracked or traced individually, and therefore to precisely correlate observations at different times in the supply chain. This is for example useful for products with a long product lifecycle, where traceability requirements extend to business processes related to the use and maintenance of the product.

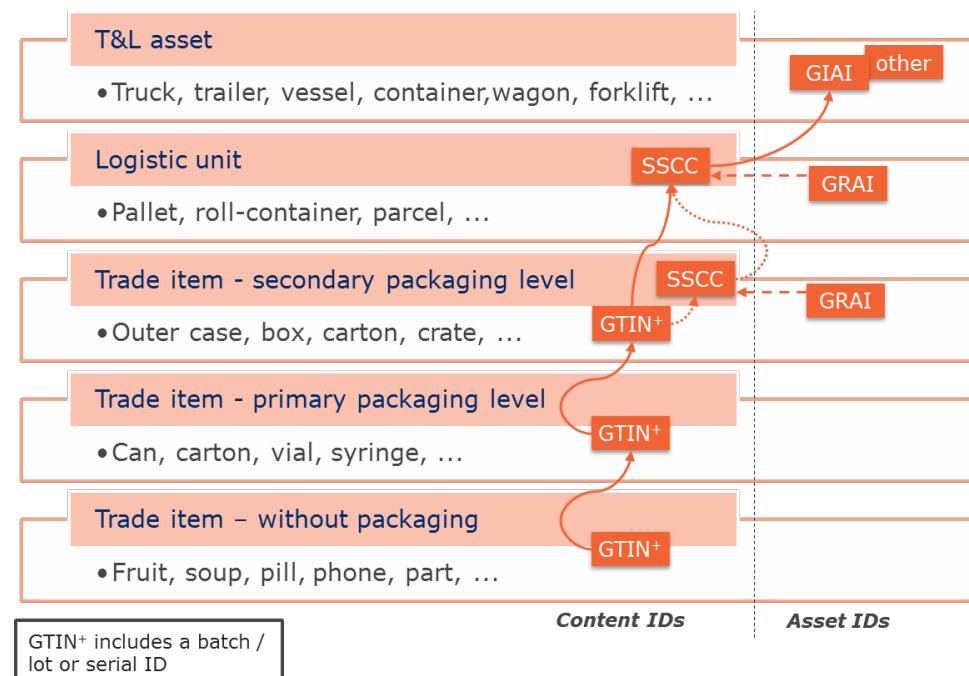
Instance-level identification has the unique advantage that the identifier represents one individual instance that can only exist in one location at a particular point in time. The other identification levels allow multiple instances or quantities (fixed or variable measure) with the same identifier to exist in multiple locations at a particular point in time, which limits the amount of knowledge about the instance(s). For example, the specific chain of custody of an object can be evaluated precisely if instance-level identifiers are used – but otherwise can only be estimated in a probabilistic manner.

- ✓ **Note:** Supply chain and logistics systems will often only support batch/lot-level traceability, since they are designed to concurrently handle a wide range of products. This means that even when each final product instance is assigned a serialised identifier during manufacturing, it may be advisable to also include a batch/lot identifier, both on the product as well as on the outer packaging.

Traceable objects in distribution and logistics

In distribution and logistics, trade items are often aggregated (grouped, packaged, loaded). This leads to other traceable objects needing to be tracked and traced, for example logistic units, containers, trucks and vessels. The diagram below illustrates how these types of objects relate to each other and how the GS1 identification keys can be applied.

Figure 4-1 Traceable object aggregation levels and identification keys



In order to preserve the relation between the higher aggregation levels and the contained trade items, the links between the various aggregation levels will need to be recorded. This is one of the essential elements of a traceability system, and key for establishing connections between the traceability systems of the various parties (including logistic service providers).

There is a difference in nature between the GTIN and SSCC on the one hand and GIAI and GRAI on the other hand. Whereas SSCC and GTIN identify goods or products including their packaging, the GIAI and GRAI identify the T&L asset independent of its contents. A special situation occurs when assets themselves are being distributed, for example empty pallets. In such cases asset IDs can also be used to identify the contents.



Note: Not depicted in figure 4-1 are the GSIN and GINC. These GS1 identification keys serve to identify groupings of logistic units and are used in combination with an SSCC.

4.1.2 Traceability parties

In any traceability system, it is important to distinguish the various actors who play a role in the chain of custody or ownership of a supply chain. Examples of parties in the supply chain might include a manufacturer, a broker, a distributor, a carrier, or a retailer. In order to understand the full context of traceability, understanding WHO played a role and sometimes their relationship to each other in the chain is essential. Identification of parties can be accomplished with the Global Location Number (GLN). In some cases, especially when identifying individuals involved, the Global Service Relation Number (GSRN) can also play a role.

Table 4-3 GS1 identification keys for traceability parties

Key	Full name	Type of supply chain information
GLN	Global Location Number	Trading partners (legal entities as well as functional entities such as a department)
GSRN	Global Service Relation Number	Service relationships (provider as well as recipient)

4.1.3 Traceability locations

A traceability location is a designated physical area that has been selected to be in scope of a traceability system.

Physical locations defined by an organisation for their business operations can be identified using the Global Location Number (GLN).

Table 4-4 GS1 identification keys for physical locations

Key	Full name	Type of supply chain information
GLN	Global Location Number	Locations
	Global Location Number + GLN extension component	(internal) Locations within a site

The GLN can be used to identify business locations as defined by a specific party. In traceability systems other locations can also be of importance. For this reason, the GS1 standards support additional ways to identify locations, such as geographic coordinates.

4.1.4 Transactions and documents

In cases where references to documents or transactions need to be shared across parties, globally unique identifiers enable unambiguous identification across systems of parties. For example, globally unique identifiers could be applied to quality certificates assigned by certification bodies.

Table 4-5 GS1 identification keys for documents and transactions

Key	Full name	Type of supply chain information
GDTI	Global Document Type Identifier	Physical documents such as certificates, driving licenses, and electronic documents such as digital images and EDI messages.

4.2 Automatic identification and data capture (AIDC)

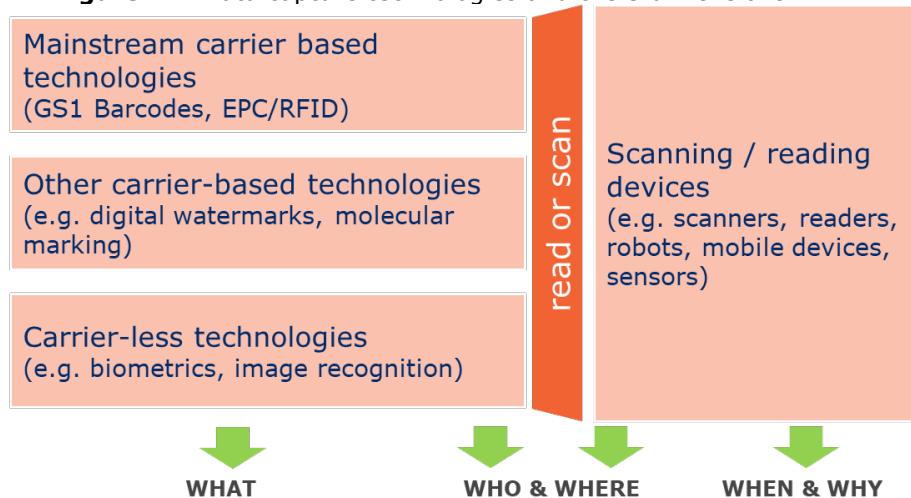
Traceable objects —and in some cases also parties, locations, transactions and documents— will need to be physically identified to enable traceability.

Traceability systems can use GS1-approved barcode symbologies and EPC/RFID tags to encode GS1 identification keys that uniquely identify products, trade items, logistic units, locations, assets, and service relations worldwide. Additional information such as best-before-dates, serial numbers, and lot numbers may also be encoded into barcodes or EPC/RFID.

Besides barcodes and EPC/RFID, other carrier-based technologies (such as digital watermarks) and carrier-less technologies (such as image recognition) may also play a role.

In addition to the data that is captured from objects, data provided by the equipment used to scan or read the data —such as date & time, read-point and user (operator)— will be important in determining the who, where, when and why dimensions.

Figure 4-2 Data capture technologies and the 5 dimensions



4.2.1 Applying data carriers

Barcodes

The marking of traceable objects is driven by the level of identification. Batch/lot-level or serialised identification are dynamic data and therefore cannot be included in the artwork of the packaging. This means that adding dynamic data in a barcode will have an impact on printing and packaging speeds.

Traditionally, barcodes on **consumer units** were used for POS scanning and only contained the Global Trade Item number (GTIN), also known as EAN or UPC. With evolving product safety regulations and product information requirements, other types of data are making their way to the barcodes on consumer products. Besides the batch/lot ID and/or serial ID these may also include the expiry date, best before date, etc. The proper linkage of the barcode, the related data and the produced instances of the trade item, is a key aspect.

Looking at **trade item groupings** such as outer cases, traditionally barcodes containing a GTIN were applied, in some cases pre-printed on the case, but also quite often included on a label. In recent years, dynamic data have made their way to case labels causing such barcodes to be increasingly printed inline.

For **logistic units** the barcodes have always been based on the SSCC, which is a serialised identifier. This means that logistics labels will be printed when the goods are packaged, and that the link between data and label will be secured that way.

Table 4-6 GS1-barcodes overview

	GS1 barcodes that support only a GTIN (no other keys, no attributes)	GS1 barcodes that support all GS1 identification keys as well as attributes
1D symbols	EAN/UPC, ITF-14, GS1 DataBar (non-expanded)	GS1-128, GS1 DataBar (expanded)
2D symbols		GS1 QR Code, GS1 DataMatrix



Note: Matrix symbols (2D) require image-based scanners. Linear symbols (1D) can be read by laser as well as image-based scanners.

EPC/RFID

EPC/RFID tags are by definition serialised. A special aspect is that EPC/RFID tags will often be pre-written, requiring the link between the issued serialised identifier and the associated data to be recorded afterwards.

Example

The example below illustrates the entities that need to be automatically identified in the healthcare sector, and which carrier techniques are applied.

Figure 4-3 Example of GS1 barcodes and EPC/RFID tags as applied in healthcare



4.2.2 Capturing data

When it comes to capturing the data, the main questions are:

1. Which process steps need to be captured?
2. What is the most cost effective way to capture the data?

Usually the first step will be scanning of logistic units upon receipt. For barcodes this is often done using handheld devices. For EPC/RFID tags, fixed readers can be used. Other process steps where data will be captured are storing, picking, packing, shipping, transporting, selling. Often a combination of fixed mounted scanners or readers and hand held devices will be applied to capture the critical tracking events.

The emergence of mobile devices deserves a special mention here, since it increases the availability of scanning capability (making scanning as pervasive as the barcode) and so may make it feasible to record additional events at limited additional cost.

4.3 Sharing traceability data

The collection of traceability data from other parties and the provision of data to other parties are essential components in distributed traceability systems. The five traceability choreographies (see section [3.3.5](#)) all pose different requirements when it comes to the standards-based exchange of data.

4.3.1 Separation of content and communication method

An important principle is the separation of data content from the way the data is exchanged (the communication method).

In terms of data content, GS1 standards for business data pertain to three categories of business data that are shared between end users:

- **Master data** that provide descriptive attributes of real-world entities identified by GS1 identification keys, including trade items, parties, and physical locations.
- **Transaction data** that consist of trade transactions, triggering or confirming the execution of a function within a business process as defined by an explicit business agreement (e.g., a supply contract) or an implicit one (e.g., customs processing), from the start of the business process (e.g., ordering the product) to the end of it (e.g., final settlement), also making use of GS1 identification keys.
- **Visibility event data** provide details about activity in the supply chain of products and other physical or digital assets, identified by keys, detailing where these objects are in time, and why; not just within one company's four walls, but throughout the supply chain. *It makes it possible to track and trace goods with live data along the process.*

The communication methods applied in the GS1 standards may be broadly classified in two groups:

- **Push** methods, where one party unilaterally transfers data to another in the absence of a prior request. Push methods may be further classified as:
 - **Bilateral** party-to-party push, where one party transfers data directly to another party.
 - **Publish/subscribe**, where one party transfers data to a data pool or repository, which in turn pushes the data to other parties who have previously expressed interest in that data by registering a subscription ("selective push").
 - **Broadcast**, where a party publishes business data in a well-known or publicly-accessible place such as a World Wide Web page, where it may be retrieved by any interested party. *Broadcast does not necessarily mean that the data is available to anyone; the data may be encrypted for a specific intended user or the broadcast channel (e.g. website) may require the receiving party to authenticate and may only grant access to the broadcast data according to specific access control policies.*
- **Pull** or query methods, where one party makes a request for specific data to another party, who in turn responds with the desired data. *Note that in the above classification of Push methods, the Broadcast method may also involve a Pull query, in order to retrieve the data from a publicly-accessible place (such as a website).*

See the GS1 System Architecture document [ARCH] for more information.

4.3.2 GS1 data sharing standards and services

GS1 offers several standards and services, based on the types of data and communication methods described above. All GS1 data exchange standards and services are based on the use of GS1 identification keys, rather than relying on internal identifiers or descriptive elements. The use of globally unique keys greatly simplifies implementations between trading partners, since they provide interoperability across the various systems.

Table 4-7 Overview of GS1 data sharing standards

Standard	Description	Communication method
Master data		
GS1 Global Data Synchronisation Network® (GDSN)	The GS1 Global Data Synchronisation Network® (GDSN) enables trading partners to automatically share their business data with each other. This means organisations can have confidence that when one of their suppliers updates their database, their own database is similarly updated as a result. Everyone has access to the same continuously refreshed data.	Publish / subscribe
GS1 Source	GS1 Source is a network of data aggregators who have all agreed to use GS1 standards. Data aggregators gather product data from brand owners and manufacturers, share it with each other on the cloud, and make it available to developers for their web and mobile applications.	Pull
GS1 SmartSearch	GS1 SmartSearch standard makes it possible to create structured data about objects and relate this data to its GS1 identification key. The structured data about the object (e.g. a product) can then be used by search engines, smartphone apps, etc. to deliver a richer experience to the user.	Broadcast
GLN Service	The GS1 GLN Service provides a single point of access to GS1 GLN master data via an interconnected network of local registries.	Pull
GS1 EDI	GS1 EDI provides some messages in support of bilateral master data exchange, in particular the EANCOM PRICAT, PRODAT & PARTIN messages and GS1 XML Item data notification.	Bilateral push
EPCIS	There are several ways to transmit master data via EPCIS: (1) Master data query (2) Instance/Lot Master Data (ILMD), (3) Header of EPCIS document (4) EPCIS master data document. See [EPCIS] for more information.	Pull (to support on-demand synchronous queries) as well as Push (publish/subscribe to standing query notifications).
Transactional data		
GS1 EDI	GS1 EDI provides trading partners with an efficient business tool for the automatic transmission of commercial data from one computer application directly to another. In EDI, all paper business documents sent previously between companies have been replaced by messages, suitable for exchange by electronic means between computer applications.	Bilateral push
Visibility event data		
EPC Information Services (EPCIS) and Core Business Vocabulary (CBV)	The GS1 EPCIS standard enables disparate applications to create and share visibility event data, both within and across enterprises. The GS1 CBV standard specifies the structure of vocabularies and specific values for the vocabulary elements to be used in conjunction with the GS1 EPCIS standard.	Pull (to support on-demand synchronous queries) as well as Push (publish/subscribe to standing query notifications).

4.3.3 Data discovery, trust and access control

The traceability choreographies mentioned in section [3.3.5](#) all apply to the three types of data content. However, each choreography applies a different mix of communication methods, as illustrated in the table below.

Table 4-8 Traceability choreography – applicable communication methods

Traceability choreography	Publishing / Contributing	On-demand selective query (synchronous)	Selective standing query (asynchronous)
One step up-one step down (e.g. bilateral EDI messages)	Push data to relevant trading partner (1-up or 1-down)	Pull (request, response)	
Centralised (e.g. centralised EPCIS repository)	Push data to centralised repository	Pull (request, response)	Publish & subscribe (receive pushed notifications matching previous standing query subscription)
Discovery of networked resources (*) (e.g. Discovery Service)	Push referral link to a Discovery Service	Pull (request, response)	
Networked (*) (e.g. distributed EPCIS repositories)	Push data to own repository	Pull (request, response)	
Cumulative (e.g. old GS1 Pedigree standard)	Push cumulative data to next 1-down party	Not applicable (downstream parties automatically receive all relevant upstream data; no need to support selective queries)	
Decentralised and replicated (e.g. blockchain ledger)	Push data to one node for validation then inclusion and replication in decentralised repository or ledger	Not applicable (All parties connected to the decentralised replicated ledger have read access to all data in the ledger, with automatic updating as new data is added to the ledger; each party can index and query their copy of the ledger and extract the data they need. Note that although the data in the decentralised replicated ledger is readable to all, it may not be understandable to all, if some sensitive data has been stored in a hashed or encrypted manner)	
(*) The Networked choreography may require an initial discovery phase (to find the relevant networked repositories), followed by direct interaction with each of the repositories.			

Access control

All of the choreographies are in principle capable of selectively restricting access to the meaning of the exchanged data on a need-to-know basis, although they differ in the mechanisms used and in the ability to control whether a receiving party shares the data with additional parties:

- Some of the choreographies involve bilateral communication between an information requesting party (querying party) and an information providing party, which may be the original contributor of the data or a shared repository holding the data. Privacy of such bilateral communications can be assured via mutual authentication, use of secure communication channels and potential encryption of the data payload or messages.
- Decentralised and replicated choreographies can involve a different approach to selectively restricting access to the meaning of the data. In the case of a blockchain ledger, trust in the ledger is assured if everyone is able to independently inspect the entire ledger including all of its data, in order to be assured that no historic transaction data has been subsequently altered. Although this openness necessarily means that anyone can read all the data in the ledger, it is still possible to hide the meaning of sensitive data either by encrypting such data or by storing a hash value in the ledger. If hash values are stored in a blockchain ledger, the original data is typically stored elsewhere and exchanged by another mechanism, while the hash value recorded in the blockchain ledger effectively archives a ‘tamper-evident seal’ that corresponds to what the data originally looked like.

Data discovery

It is sometimes desirable to share data between parties who have no direct relationship, but who are connected through a chain of custody, chain of ownership, chain of transactions, or some combination of these.

All traceability choreographies (see [3.3.5](#)) enable this in one way or another. The "data discovery problem" is applicable when going beyond the one step up-one step down scenario, and specifically in the case of the networked model. It is concerned with how to *directly* share data between parties that are connected in a chain but do not have a direct relationship.

Elements of the discovery problem include:

- **Chaining:** how does Company A find out which other companies are connected to it by a chain (and who therefore may have data of interest)?
- **Trust:** if Company A and Company C discover they are connected by a chain, but have no direct relationship, how can they establish the conditions of trust necessary to share data with each other? Are they able to do this in an automated manner, without human intervention by intermediate companies such as Company B?
- **Data transfer:** once companies have discovered each other and established trust, how do they accomplish the sharing of data?

GS1 technical standards to address the data discovery and trust aspects are currently being developed but are not yet ready for market. Much good work has been done to develop the concepts of discovery services (including basic data model and functional requirements). See also section [4.4](#).

 **Note:** Please contact GS1 for implementation advice on the topic of data discovery, trust and access control. <https://www.gs1.org/contact>

4.3.4 Event data from devices & sensors and the Internet of Things (IoT)

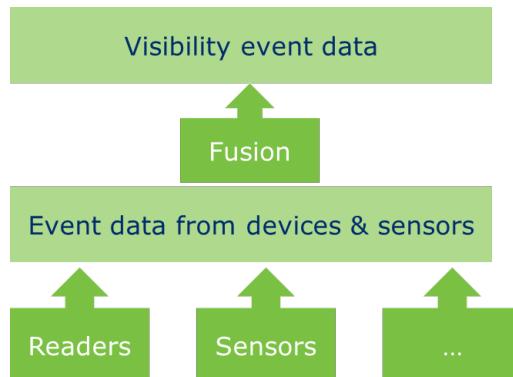
The enormous growth of sensors and actuators in physical devices, and the fact that these devices are increasingly connected to the internet (the Internet of Things) leads to a new category of timestamped event data that is much broader than the visibility event data currently handled by the GS1 ALE (Application Level Events) and EPCIS standards.

Sensors passively record changes in the state of the physical world and the objects contained within it, such as a food temperature sensor in a truck recording events outside an acceptable temperature range. Event data from actuators record a history of intentional changes, such as the opening of a valve for a water reservoir or gas pipeline or the locking/unlocking of a door.

GS1 has started to engage in IoT-related standardisation initiatives, in particular when it comes to the use of identifiers, the interpretation (semantics) and fusion (adding business context) of event data from devices and sensors.

Event data from devices and sensors are expected to be very similar in nature to visibility event data. The data will be enriched with business context —including the five dimensions that define the who, what, when, where and why— and shared using networked or decentralised choreographies (see section [3.3.5](#)).

Figure 4-4 Visibility event data and event data from devices and sensors



4.4 The traceability solution ecosystem

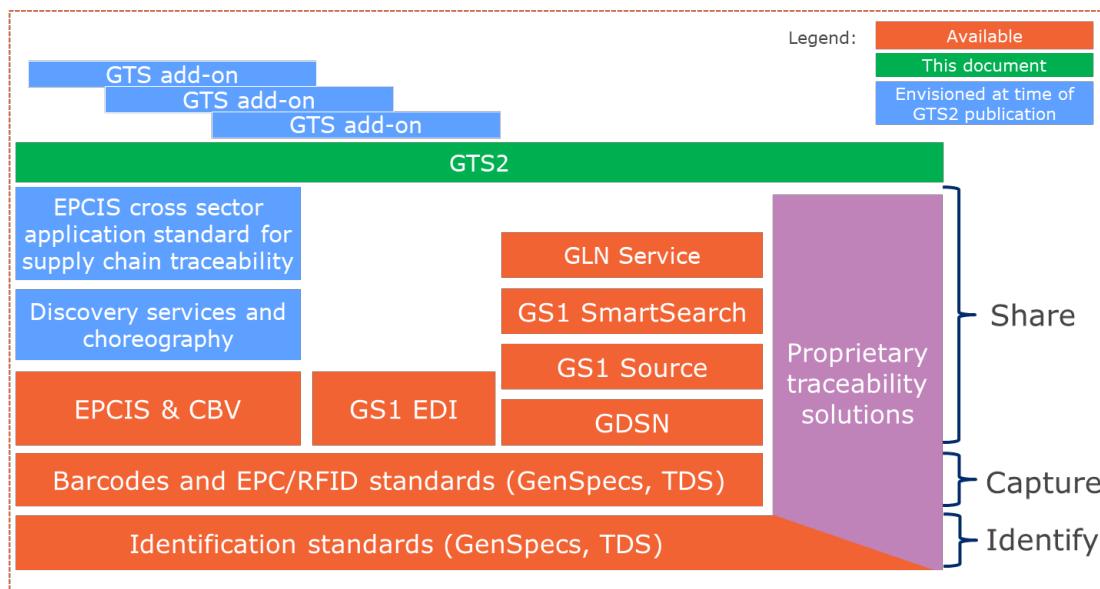
Various vendors offer plug-and-play solutions to address the traceability needs of organisations. Such solutions can be used by larger organisations to easily on-board numerous suppliers.

Transparency solutions tend to provide supply chain mapping capabilities, enabling the identification of connections between suppliers and customers by product type. These solutions often lack the ability to track or trace an individual object (with a globally unique serialised identifier) along a specific supply chain path, and their focus may instead be more on being able to say whether all upstream suppliers hold specific certifications or accreditations for organic / environmentally-friendly / ethical practices. **Traceability solutions** offer detailed levels of traceability, and often include event-based data repositories and the ability to logically link related events.

If vendor solutions apply a proprietary data model and closed ecosystem they are unlikely to be interoperable with competing solutions. Furthermore, interoperability with existing IT systems of the users may be limited. Applications that have certified compliance with relevant GS1 open standards such as GS1 barcodes, GDSN, EPCIS and CBV are much more likely to support a high level of interoperability for the exchange of traceability data. It is important to note that partial compliance with GS1 standards can provide benefits to the users. For example, adding support for the GTIN to a vendor solution can enhance interoperability.

In addition to turnkey traceability solutions, several **enabling services** exist. Services that provide access to data about certifications of a party are of particular interest to traceability systems. GS1 standards aim to support connectivity to such services by providing standard reference mechanisms and by promoting the use of GS1 keys to connect to such services (e.g., a GLN to identify the party).

Figure 4-5 GS1 standards and services in the traceability solution ecosystem



In the above graphic, the bottom layer represents the GS1 standards for **identification** of products, assets, locations, etc. It should be noted that many proprietary traceability solutions leverage some of these foundational standards for identification. The layer above this represents the GS1 **data capture** standards that exist to ensure consistent representation of identity in barcodes and RFID tags. In the next layer, the orange boxes represent the existing GS1 standards for the **sharing** of different kinds of data (master data, transaction data, visibility event data). The blue boxes represent future work related to data sharing standards.

Above all of these standards is where this **GTS2** document is intended to fit. It makes appropriate references to all of the standards below it, and is designed to show how all of these pieces fit together to enable standards-based traceability solutions. The blue boxes above GTS2 —the GTS add-ons— represent future work on sector and process application standards that is expected to be needed to complete the full ecosystem.

5 Key requirements for interoperable traceability systems

The interoperability requirements provide a way for companies to evaluate their traceability systems in a non-binary way.

For each requirement, one or more KPIs are included, and next to each KPI the applicable GS1 standards. Ultimately, these KPIs could serve to generate benchmarks per sector / product / region.

5.1 Prerequisites

In order to judge the degree to which the traceability system meets the requirements, the following elements will need to be clear:

- *Which of the traceable objects we create, manage or process are in scope of the system?*
- *What is the required precision level for the traceability data for each of the traceable objects we create, manage or process?*
- *Which locations that we manage are in scope of the system?*
- *Which suppliers and supplier locations are in scope of the system, including suppliers further upstream?*
- *Which customers and customer locations are in scope of the system, including customers further downstream?*
- *Which third parties and third party locations are in scope of the system?*

In the requirements below these variables are treated as a precondition. This means that KPIs need to be expressed relative to the intended scope of the traceability system.

5.2 Identification requirements (including static data management)

	Requirement	Applicable GS1 standards
R01	The traceability system of a party needs to apply globally unique identifiers for each traceable object created or managed by the party, and maintain a record with the associated master data. Exception: For intermediate products, an internal identifier MAY be applied.	
<i>a</i>	<i>How many of the trade items we produce and/or sell have a globally unique ID? (*)</i>	GTIN
<i>b</i>	<i>How many of the logistic units we ship have a globally unique ID? (*)</i>	SSCC, (GSIN, GINC)
<i>c</i>	<i>How many of the assets we produce and/or manage have a globally unique ID? (*)</i>	GRAI, GIAI
R02	A party may also handle traceable objects whose identifiers have been created and managed by other parties. Also in this situation, the traceability system of a party needs to record such identifiers in the traceability data it captures and retrieve any relevant master data associated with these identifiers, where appropriate.	
<i>a</i>	<i>How many of the trade items we buy / receive from our suppliers have a globally unique ID? (*)</i>	GTIN
<i>b</i>	<i>How many of the logistic units we receive from our suppliers have a globally unique ID? (*)</i>	SSCC, (GSIN, GINC)
<i>c</i>	<i>How many of the assets we use (but which are owned or managed by other parties) have a globally unique ID? (*)</i>	GRAI, GIAI
R03	The traceability system of a party needs to identify traceable objects that are produced, managed and/or sold by the party at the level required to meet the traceability requirements of all parties in the end-to-end supply chain.	
<i>a</i>	<i>How many of the trade items we produce and / or sell that require serialised identification have an appropriate ID? (*)</i>	GTIN + serial ID (SGTIN)
<i>b</i>	<i>How many of the trade items we produce and / or sell that require lot-level identification have an appropriate ID? (*)</i>	GTIN + batch/lot ID (LGTIN)
R04	The traceability system of a party needs to use globally unique identifiers for each traceability party that is managed by the party, and maintain a record with the associated master data.	

	Requirement	Applicable GS1 standards
a	<i>How many of the legal entities and functions that engage in processes and transactions with other parties have a globally unique ID? (*)</i>	GLN, GSRN
R05	The traceability system of a party needs to use globally unique identifiers for each physical location that is managed by the party, and maintain a record with the associated master data.	
a	<i>How many of the physical locations that engage in processes and transactions with other parties have a globally unique ID? (*)</i>	GLN or GLN + extension
R06	The traceability system of a party needs to apply globally unique identifiers for transactions or documents created by the party and shared with other parties, and in that case needs to maintain a record with the associated data.	
a	<i>How many of the transactions and documents we create and share with other parties have a globally unique ID? (*)</i>	GDTI
<i>(*) KPI needs to be expressed as percentage of the total quantity in scope.</i>		

5.3 Automatic data capture and identification (AIDC) requirements

	Requirement	Applicable GS1 standards
R10	For traceable objects that require automatic identification and are created or managed by the party, open standards should be applied.	
a	<i>How many of the traceable objects created or managed by us are marked at the right level of precision using an open AIDC standard? (*)</i>	GS1 barcodes, GS1 EPC/RFID
R11	For traceable objects that require automatic identification and are created or managed by other parties open standards should be applied.	
a	<i>How many of the traceable objects created or managed by other parties are marked at the right level of precision using an open AIDC standard? (*)</i>	GS1 barcodes, GS1 EPC/RFID
<i>(*) KPI need to be expressed as percentage of the total quantity in scope.</i>		

5.4 Data recording requirements (relation data and CTEs)

	Requirement	Applicable GS1 standards
R20	The traceability system of a party needs to keep a record of all supply chain partners per trade item. The relation data should contain: <ul style="list-style-type: none"> ▪ The category-level or class-level ID of the trade item ▪ The ID of the source / destination party ▪ The ID of the source / destination location ▪ The validity period 	
a	<i>For how many of our suppliers do we have relation data available? (*)</i>	GDSN, GS1 EDI, EPCIS
b	<i>For how many of our customers do we have relation data available? (*)</i>	GDSN, GS1 EDI, EPCIS
c	<i>For how many of our third party service providers do we have relation data available? (*)</i>	GDSN, GS1 EDI, EPCIS
d	<i>What is the average data quality (completeness and accuracy) of the relation data, on a scale of 1 to 5? (**)</i>	GDSN, GS1 EDI, EPCIS
R21	The traceability system of a party needs to keep record of all CTEs related to shipments and receipts, consisting of: <ul style="list-style-type: none"> ▪ The class-level, batch/lot-level or instance level ID of the traceable objects ▪ The ID of the source / destination party ▪ The ID of the source / destination location ▪ The despatch / receipt date 	
a	<i>How many of the shipments we receive are recorded? (*)</i>	GS1 EDI, EPCIS
b	<i>How many of the shipments we ship or despatch are recorded? (*)</i>	GS1 EDI, EPCIS

	Requirement	Applicable GS1 standards
R22	All CTEs in which traceable objects are initially created (e.g., commissioned) need to be recorded.	
a	<i>How many of the CTEs in which we create traceable objects are recorded? (*)</i>	EPCIS
R23	For each CTE the following data needs to be recorded at a minimum: <ul style="list-style-type: none"> ▪ Event date and time (including time zone and UTC time offset) ▪ ID of the traceable object at instance-level or batch/lot-level ▪ ID of the location where the event took place ▪ Business process step and disposition ▪ ID of the responsible party (in case it is different from the manager of the location) 	
a	<i>What is the average data quality (completeness and accuracy) of the recorded data for these events, on a scale of 1 to 5? (**)</i>	EPCIS, GS1 EDI
R24	For CTEs in which traceable objects are being transformed (e.g., produced) the relationship between the inputs and outputs needs to be recorded.	
a	<i>What is the average data quality (completeness and accuracy) of the recorded data for transformation events, on a scale of 1 to 5? (**)</i>	EPCIS
R25	For CTEs in which traceable objects are being aggregated (e.g., packed or assembled) or disaggregated (e.g., unpacked or disassembled) the relationship between the children and parent needs to be recorded for each containment level.	
a	<i>What is the average data quality (completeness and accuracy) of the recorded data for aggregation events, on a scale of 1 to 5? (**)</i>	EPCIS
R26	The traceability system of a party needs to keep a record of additional critical tracking events (CTEs) where applicable.	
a	<i>Which additional CTEs should we be recording? E.g., installation, disposal, ...</i>	EPCIS
b	<i>How many of these are we currently recording? (*)</i>	EPCIS

(*) KPI needs to be expressed as percentage of the total quantity in scope.

(**) KPI needs to be expressed as value on a scale of 1 to 5, as follows:

1. Quality is unknown.
2. Weak, the data do not serve our needs in most cases.
3. Average, the data serve our needs in most cases, but we do not apply regular quality assurance checks.
4. Good, the data serve our needs in most cases, and we do apply regular quality assurance checks.
5. Excellent, the data quality is continually monitored and used in our day-to-day decision making.

5.5 Data sharing requirements

	Requirement	Applicable GS1 standards
R30	The traceability system needs to enable traceability data to be provided to other parties and for traceability data to be received from other parties, within the time frame required and using effective and secure mechanisms..	
a	<i>Can we provide traceability data to our supply chain partners within the agreed timeframe?</i>	GDSN, GS1 EDI, GS1 EPCIS, CBV
b	<i>Can we gain access to traceability data of our supply chain partners within the agreed timeframe?</i>	GDSN, GS1 EDI, GS1 EPCIS, CBV
c	<i>Are authorisation mechanisms in place to help determine which parties have access to which data?</i>	GDSN, GS1 EDI, GS1 EPCIS, CBV
R31	Traceability data needs to be retained and remain accessible to authorised parties to meet the traceability requirements of all supply chain partners.	
a	<i>Do we have archiving procedures for the traceability data we create, with an adequate data retention period?</i>	GDSN, GS1 EDI, GS1 EPCIS, CBV
b	<i>Do our supply chain partners have archiving procedures for the traceability data we may require, with an adequate data retention period?</i>	GDSN, GS1 EDI, GS1 EPCIS, CBV
R32	Traceability data that is electronically exchanged between parties for automated processing needs to be exchanged using open data sharing standards.	

	Requirement	Applicable GS1 standards
a	<i>Is all traceability data exchanged using open data exchange standards?</i>	<i>GDSN, GS1 EDI, GS1 EPCIS, CBV</i>
b	<i>Are automated communication methods applied (push, pull)?</i>	<i>GDSN, GS1 EDI, GS1 EPCIS, CBV</i>

5.6 Roles and responsibilities

Another important element that needs to be taken into account when evaluating the degree to which the traceability system meets the requirements are the traceability data management responsibilities. These responsibilities follow from rules as defined in the various foundational GS1 standards (GS1 General Specifications, GTIN management rules, GDSN), application standards (Product Recall Management) and the requirements as defined in this document. See appendix [B](#) for a comprehensive overview.

6 Glossary



Note: See the GS1 glossary for other terms related to the GS1 system,
<http://www.gs1.org/glossary>

Chain of custody

A time-ordered sequence of parties who take physical custody of an object or collection of objects as it moves through a supply chain network.

Chain of ownership

A time-ordered sequence of parties who take legal possession of an object or collection of objects as it moves through a supply chain network.

Critical Tracking Event (CTE)

A record of completion of a step in the business process in a supply chain, that is critical to record and share, in order to ensure end-to-end traceability.

Key Data Element (KDE)

Those data required to be present in a CTE to accurately represent what occurred in the step of a business process, in order to ensure traceability.

Party

An organisation or individual acting as an entity in a supply chain. Parties may play multiple different roles in the supply chain.

Supply chain

A supply chain is a system of organisations and business processes that are involved in the manufacture, distribution and maintenance of a product or asset.

Supply chain visibility

The awareness of, and control over, specific information related to product orders and physical shipments, including transport and logistics activities and the statuses of events and milestones that occur prior to and in-transit. [Aberdeen Group]

Traceability

Traceability is the ability to trace the history, application or location of an object [ISO 9001:2015].

When considering a product or a service traceability can relate to:

- the origin of materials and parts;
- the processing history;
- the distribution and location of the product or service after delivery.

For practical reasons, "trace" or "track and trace" may be used as equivalent terms to designate the action of ensuring the traceability.

Traceability system

The system used by an individual party to manage traceability in its supply chain(s). A traceability system includes mechanisms for the identification of objects and for the capture of information about observations of those objects over time as they move between locations or participate in various business processes.

Traceability party

A party that has been selected to be in scope of a traceability system. Parties in scope of traceability systems may include those that take custody of traceable objects, those that take ownership of traceable objects, those that inspect traceable objects, those that insure traceable objects, etc.

End-customers (including consumers and patients) will often not be treated as traceability parties, since they do not necessarily carry a traceability responsibility and very often remain unknown to the other traceability parties.

Traceability location

A traceability location is a designated physical area that has been selected to be in scope of a traceability system.

Traceable object

A traceable object is a physical or digital object whose supply chain path can and needs to be determined.

Tracing

Tracing is the capability to identify the origin and characteristics or history of a particular traceable object upstream (through earlier observations) based on data recorded at defined points of the supply chain.

Trace or Tracing backward or ascending traceability

Tracking

Tracking is the capability to locate or follow the path of a particular traceable object downstream (through later observations) based on data recorded at defined points of the supply chain.

Track forward or descending traceability

Transparency

Transparency refers to the need to ensure visibility and access to accurate information across supply chains (inclusive of consumers), including the provision of relevant traceability data to trading partners and consumers in a spirit of openness.

Visibility

Visibility is the ability to know exactly where things are at any point in time, or where they have been, and why.

Visibility event data

Visibility event data are records of the completion of business process steps in which physical or digital entities are handled. [ARCH]

Each visibility event captures *what* objects participated in the process, *when* the process took place, *where* the objects were and will be afterwards, and *why* (that is, what was the business context in which the process took place).

6.1 List of abbreviations

Abbreviation	Full term
AI	GS1 Application Identifier
AIDC	Automatic Identification and Data Capture
API	Application Programming Interface
BIC	Bureau International des Containers et du Transport Intermodal
BOM	Bill Of Material

Abbreviation	Full term
CBV	Core Business Vocabulary
CTE	Critical Tracking Event
EDI	Electronic Data Interchange
EPC	Electronic Product Code
EPCIS	EPC Information Services
ERP	Enterprise Resource Planning
GDSN	Global Data Synchronisation Network
GIAI	Global Individual Asset Identifier
GLN	Global Location Number
GTIN	Global Trade Item Number
GTS	Global Traceability Standard
HRI	Human Readable Interpretation
ID	Identifier
IoT	Internet of Things
ISO	International Standards Organisation
IT	Information Technology
KDE	Key Data Element
MRO	Maintenance, Repair and Overhaul
OEM	Original Equipment Manufacturer
POS	Point-Of-Sale
RFID	Radio Frequency identification
SKU	Stock Keeping Unit
T&L	Transport and Logistics
TDS	Tag Data Standard
UTC	Coordinated Universal Time

7 References

Table 7-1 Normative references

Abbreviation	Document	Author / Year
ARCH	GS1 System Architecture, http://www.gs1.org/docs/architecture/	GS1, 2017
CBV	Core Business Vocabulary Standard version 1.2.1, http://www.gs1.org/epcis	GS1, 2017
DCM	Digital Coupon Management standard, version 1, http://www.gs1.org/digital-coupons/digital-coupon-standard/1	GS1, 2012
EDI	GS1 has currently three sets of complementary EDI standards: ▪ GS1 EANCOM® ▪ GS1 XML ▪ GS1 UN/CEFACT XML See https://www.gs1.org/edi for more information.	GS1
EPCIS	EPC Information Services Standard version 1.2, http://www.gs1.org/epcis	GS1, 2016
EPCIS-IG	EPCIS and CBV Implementation Guideline version 1.2, http://www.gs1.org/epcis	GS1, 2017
GENSPECs	GS1 General Specifications, version 17, http://www.gs1.org/genspecs	GS1, 2017
GLN-ALL	GLN Allocation Rules, http://www.gs1.org/1/glrules/en/	GS1, 2016
GTIN-MAN	GTIN Management Rules, http://www.gs1.org/1/qtinrules/en/	GS1, 2016
ISODIR2	ISO/IEC Directives part 2; Rules for the structure and drafting of International Standards – 7th edition, 2016	ISO, 2016
LOG-LAB	GS1 Logistics Label guideline, version 1.2, http://www.gs1.org/shipping-and-receiving	GS1, 2017
RECALL	Product Recall Business Message Standard, version 3.3, http://www.gs1.org/edi-xml-recall/xml-product-recall/3-3	GS1, 2017
TDS	GS1 Tag Data Standard (TDS), version 1.10, http://www.gs1.org/epc-rfid	GS1, 2017

Table 7-2 Non-normative references

Abbreviation	Document	Author / Year
GTS-v1.3	GS1 Global Traceability Standard, version 1.3	GS1, 2012
GTC	GS1 Global Traceability Compliance Criteria for Food Application Standard, version 4.0	GS1, 2015
GLN-SER	GLN Service	GS1, 2017
GS1US-CTE	How GS1 Standards support Product Tracing, Critical Tracking Events and Key Data Elements	GS1 US, 2011
LIM	GS1 Logistics Interoperability Model, http://www.gs1.org/lim	GS1, 2007

A Summary of interoperability requirements

The table below provides a summary of the requirements and related GS1 standards, as listed in section [5](#).

Main topic	Subtopic	GS1 standards
IDENTIFICATION REQUIREMENTS		
Traceable objects	Trade items	GTIN, GTIN + lot ID, GTIN + serial ID
	Assets	GIAI, GRAI
	Logistic units	SSCC, GSIN, GINC
	Coupons	GCN
Parties		GLN, GSRN
Locations		GLN, GLN + GLN extension component
Transactions / documents		GDTI
AIDC REQUIREMENTS		
Barcodes	Trade items (GTIN-only)	(GTIN-only) EAN/UPC, ITF-14, GS1 DataBar non-expanded
	Trade items, assets, logistic units, parties, locations, transactions / documents	(GS1 identification key + attributes) GS1-128, GS1 DataMatrix, GS1 QR Code, GS1 DataBar expanded
RFID	Trade items, assets, logistic units, parties, locations, transactions / documents	EPC/RFID
DATA RECORDING REQUIREMENTS		
Relation data	Suppliers, customers, 3 rd parties	Internal, using GS1 identification keys
Critical Tracking Events	Observations	EPCIS: Object Event CBV business steps: commissioning, shipping, receiving, transporting, storing, ...
	Transformations	EPCIS: Transformation Event CBV business steps: commissioning
	Aggregations	EPCIS: Aggregation Event CBV business steps: packing, installing, ...
DATA SHARING REQUIREMENTS		
Master data	Trade items	GDSN, GS1 SmartSearch, GS1 EDI, EPCIS
	Parties and locations	GLN Service, GS1 EDI, EPCIS
	Assets	EPCIS
	Relation data	Bilateral, no standard
Transaction data	Shipments, receipts	GS1 EDI Despatch Advice (DESADV), Receiving Advice (RECADV), GS1 Transport Status Notification (IFTSTA)
	Recalls	GS1 EDI Product Recall standard
Visibility event data	Critical Tracking Events	ECPIS, CBV

B Data management responsibilities

The table below aims to provide a summary of the main data management responsibilities by role.

Data management responsibility	Primary party (data source, initiator)	Secondary parties (data recipients, others)	Responsibilities defined in	
(IDENTIFICATION) GS1 identification key management				
GTIN	Brand owner (*)	n/a	[GENSPES] [GTIN-MAN]	
GLN	Location owner, location primary user (**)	n/a	[GENSPECs] [GLN-ALL]	
GCN	Coupon offer issuer	n/a	[GENSPECs] [DCM]	
SSCC	Physical builder or brand owner	n/a	[GENSPECs] [LOG_LAB]	
GINC	Carrier or freight forwarder	n/a		
GSIN	Shipper, consignor	n/a		
GIAI, GRAI	Asset owner or manager	n/a	[GENSPECs]	
GSRN	Organisation offering the service	n/a		
GDTI	Document issuer	n/a		
CPID	Buyer (OEM)	n/a		
(DATA SHARING) Master data				
Trade item master data	Data source (brand owner (*), see GTIN)	Any party that fulfils the conditions under which these data are to be shared.	[GDSN], [GENSPECs]	
Party & location master data	Data source (location owner or manager, see GLN)		[GLN-SER], [GENSPECs]	
Other master data (related to assets, service relations, ...)	Party that assigned the identification key, see above.		[GENSPECs]	
(DATA RECORDING & SHARING) Capturing, recording and sharing of visibility event data				
Object events	Any party that is engaged in any of the following business steps: commissioning, shipping, receiving, transporting ...	Any party that fulfils the conditions under which these data are to be shared, for example based on chain of custody or chain of ownership relations.	[GTS2]	
Transformation events	Any party that is engaged in any of the following business steps: commissioning, processing, ...			
Aggregation events	Any party that is engaged in any of the following business steps: packing, loading, unloading ...			
(DATA SHARING) Transaction data sharing				
Despatch advice	Shipper, consignor, seller	Receiver, consignee, buyer	[GS1-EDI] [LIM]	
Receiving advice	Receiver, consignee, buyer	Shipper, consignor, seller	[GS1-EDI] [LIM]	
Transport status notification	Logistics service provider, carrier	Receiver, consignee, buyer	[GS1-EDI] [LIM]	
(DATA SHARING) Product recall				
Product recall notification	Product recall initiator	Product recall recipient	[GS1-EDI] [RECALL]	
Product removal confirmation	Product recall recipient	Product recall initiator		
Product recall closeout notif.	Product recall initiator	Product recall recipient		
Notes:				
(*) see [GENSPECs] section 4 for non-branded items and exceptions.				
(**) See [GENSPECs] section 4 for exceptions.				

C Getting started

This section provides an overview of a step-by-step methodology for the design of traceability systems. The methodology is intended for use by individual companies as well as by organisations or working groups that wish to establish sectorial and/or regional guidelines.



Note: Subsequent to the publication of GTS2, a GTS implementation guideline will be developed, which will provide more information on traceability processes, roles, responsibilities, traceability data models, etc.

C.1 Before you begin

Before you start designing your traceability system, it will be important to gather information about available guidelines and ongoing initiatives in your sector. Many industry organisations have established working groups in order to define best practices and establish a coordinated approach. GS1 is often a partner in such initiatives and can provide more information.

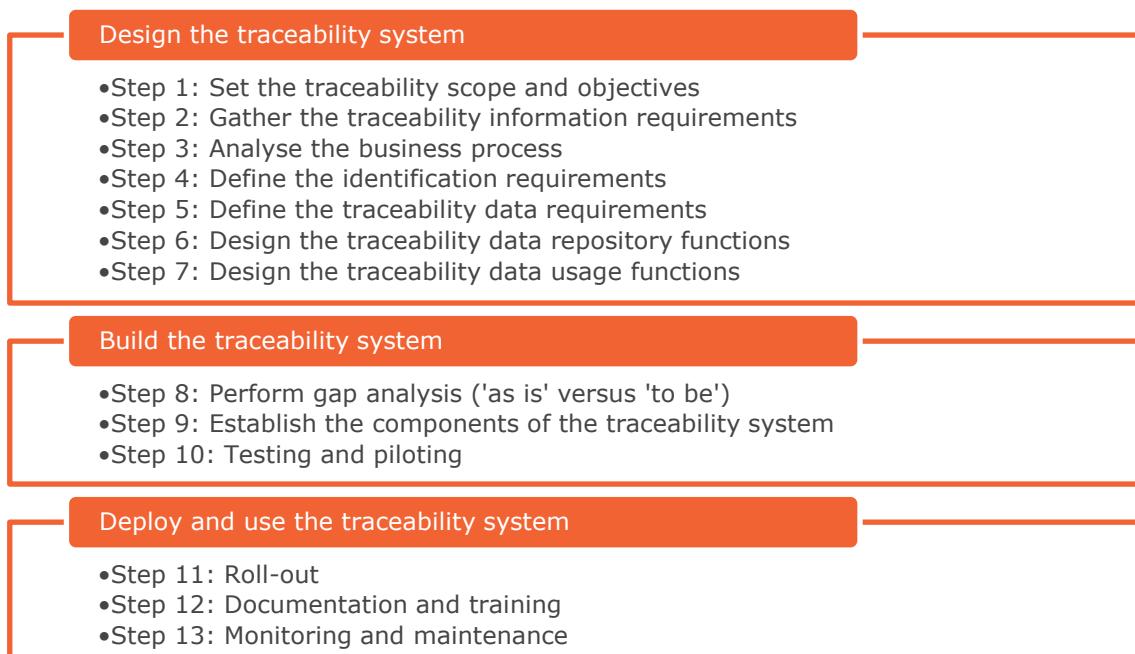
Examples of sectors where GS1 is involved or is facilitating traceability initiatives:

- Fresh foods (fruits and vegetables, fish and seafood, ...)
- Healthcare
- Rail manufacturing and MRO

C.2 Steps to take

This section provides a step-by-step methodology to accomplish traceability in value networks, for use by individual companies, but that can also be adapted by organisations in establishing sector / product guidelines.

Figure C-1 GS1 Traceability Methodology



C.3 Design the traceability system

Step 1: Set the traceability goals and objectives

Traceability is a shared responsibility of all actors in a value network. This means that in order to establish the traceability goals, each actor will need to consider its own strategy as well as the strategy of the other actors in the network. Often there are forces in play that help to define the direction, such as legal requirements or commercial requirements of dominant players. The request for greater transparency by end consumers is also an increasingly important driver.

As further requirements are placed on organisations to track and trace the movement of things through the supply chain, it is important to place an emphasis on the overall goals and objectives of deploying a traceability system. "What problem are we trying to solve"?

Step 2: Gather the traceability information requirements

In this step, the traceability objectives are transformed into concrete information requests that need to be fulfilled by the traceability system.

Step 3: Analyse the business process

The next step is to analyse the business process in a level of detail that is sufficient to understand the traceability aspects related to the goals and information requirements.

The analysis should include:

- Supply chain stakeholders and their interactions
- Traceability roles and responsibilities per stakeholder
- Process flows that depict the state changes and movements of the traceable objects.

Step 4: Define the identification requirements

Based on the analysis of the business process flows, it will have become clear which entities will require identifiers. The next step is to determine the right level of identification for each of those entities.

Determination of the level of trade item identification is a crucial decision with far-reaching consequences. Also for other entities, such as locations and documents, it is important to consider the method and level of identification.

Step 5: Define the traceability data requirements

The traceability data requirements first of all depend on the precision level that will be required.

A good way to proceed is to consider the Who, What, When, Where, and Why dimensions of each relation, transaction and event.

Step 6: Design the traceability data repository functions

To understand the required data capture and recording functions, it helps to approach these as being functions of a traceability data repository. In some cases, the repository will be physically implemented; in other cases, the repository will remain a virtual concept that dynamically integrates various data sources together as needed.

Three main functions need to be fulfilled:

- Data capture

- Data storage, including archiving procedures that define how traceability data is recorded, stored and/or administered, taking into account the minimum retention period required from legal and commercial perspectives.
- Data sharing

Step 7: Design the traceability data usage functions

Specific functions will be needed to detect exceptions and prevent incidents. Such functions may range from simple queries to advanced data analytics.

Examples:

- Expired certificate
- Temperature exception during transport
- Counterfeit detection

Furthermore, functions will be needed to manage interventions. Interventions procedures may be simple (limited to internal) or complex (involving a large number of external parties).

Examples:

- Recall notification, execution and closeout
- Quarantine
- Counterfeit remediation

C.4 Build the traceability system

Step 8: Perform gap analysis ('as is' versus 'to be')

Based on the design phase it will have become clear where there are gaps between the 'as is' and 'to be' situation.

Step 9: Establish the components of the traceability system

The next step is to evaluate whether it is possible to adjust existing hardware and software, or if it will be necessary to buy new components.

Step 10: Testing and piloting

Find trading partner(s) to pilot / test the traceability system.

C.5 Deploy and use the traceability system

Step 11: Roll-out

Establish an implementation plan by product/facility.

Prioritise based on identified quick wins, in order to build stakeholder confidence.

Step 12: Documentation and training

Besides designing the traceability system, the responsible parties will also need to address the implementation and maintenance of their traceability systems, such as:

- Making specific people accountable
- Having written procedures
- List of internal and external traceability parties that need to be contacted.
- List of key personnel for crisis management with defined responsibilities, e.g., separation of roles for initiation and approval in events such as recalls
- Communication plan for internal and external trace requests

Step 13: Monitoring and maintenance

It will be essential to include a monitoring and maintenance procedure, defining how the current operation will be verified and how the traceability system will be kept in line with the actual production and distribution process. The procedure could include:

- Regular audits to check if the system is still meeting the traceability goals
- Checks to assure and maintain the availability and quality of the traceability data

D Sector examples

The examples in this section illustrate how the GS1 standards can be used to accomplish traceability in a variety of supply chains.



Note: The examples provide a high-level overview. Details on critical tracking events, master data and roles and responsibilities are or will be included in sector-, product- or application-specific add-ons.

Retail CPG

Improved supply chain visibility, accurate product information, product traceability and food safety-made possible by GS1 standards- are enabling the seamless, omni-channel shopping experience that trading partners, regulators and consumers are demanding from the CPG/Grocery sector.

Figure D-1 Retail CPG example



Some important aspects of traceability in retail CPG supply chains:

- Transformation on batch / lot level (changing the GTIN)
- Transparency to consumers
- Product quality / recall
- Counterfeit products
- Online sales / e-commerce



Note: For more information on traceability in retail CPG: <https://www.gs1.org/cpggrocery>

Fresh foods

GS1 standards help to trace fresh foods from farm to fork. Information can be shared throughout the supply chain to support your business needs and vouch for food safety. You can retrieve data to satisfy safety regulations, use as a baseline for replenishment strategies and ensure overall quality while eliminating waste.

Figure D-2 Fresh foods example



Some important aspects of traceability in fresh foods supply chains:

- No or few transformations of the product, except for sorting, washing, cleaning, freezing
- Perishable products

- Specific regulations, quality requirements and certifications per product category (e.g. for meat, fish, fresh produce).
- Waste management



Note: For more information on traceability in fresh foods supply chains:
<https://www.gs1.org/fresh-foods>

Healthcare

Traceability is a foundation to many healthcare clinical and supply processes. Amongst other things, it helps to prevent counterfeit medicines and medical devices entering the supply chain, provides surety that products reach the intended end recipients, creates the ability to execute more effective and targeted recalls, and enables accurate recording of medical product information in both patient records and clinical registries. Ultimately, traceability is essential to ensure the patient rights – administration of the right medical product, in the right quantity, at the right time, to the right patient, by an authorised caregiver.

Figure D-3 Healthcare example



Some important aspects of traceability in healthcare supply chains:

- The patient and caregiver are key stakeholders.
- There are a range of countries/regions with regulatory requirements for traceability of pharmaceuticals and medical devices.
- The scope of items traced can vary from medical records and moveable assets, to healthcare products and surgical instruments.
- Traceability is being implemented extensively both within hospitals and between supply chain partners.



Note: GS1 standards are the most used system of standards for traceability in healthcare – from the manufacturer to the patient. For more information on traceability in healthcare:
<https://www.gs1.org/healthcare>

Technical industries

Defence, engineering, energy, mass transit and mining—all are technical industries that currently face many of the same challenges such as cost pressures, counterfeiting and the race to digitise their physical worlds. They share a mutual need for transparent processes to optimise their supply chains as parts and raw materials enter production environments; are processed, assembled and packaged; exit as finished products bound for customer locations; and then go through multiple usage and maintenance cycles.

Figure D-4 Technical industries example



Some important aspects of traceability in technical industries:

- Cyclical nature
- Long product lifetimes
- Product authentication
- Direct marking of the GS1 identification key on the traceable object
- Assembly of components and sub-systems into fully operational systems, requiring to keep track of complex product hierarchies, often using serialised identifiers (serialised bill of material of the product 'as-built').



Note: For more information on traceability in technical industries:
<https://www.gs1.org/technical-industries>

Transport & logistics

Traceability and visibility are of the utmost importance in transport and logistics processes.

Figure D-5 Transport and logistics example



Some unique aspects of traceability in transport and logistics:

- End-to-end traceability across multiple transport modes, with various changes in the chain of custody
- Piece level tracking of items contained in transport means and equipment
- Tracking of parcels in delivery process to final customer (including end-consumer)
- Tracking of empty assets



Note: For more information on traceability in transport and logistics:
<https://www.gs1.org/transport-and-logistics>

E Acknowledgements

GS1 would like to thank everyone who contributed to the various stages of this project.

First name	Last name	Organisation	Project role
Albert	Ang	GS1 Malaysia	
Koji	Asano	GS1 Japan	
Jonas	Batt	GS1 Switzerland	Editorial team
Wolfgang	Becha	Mondelez International, Inc.	Editorial team
Robert	Beideman	GS1 Global Office	GS1 project team (lead)
Chuck	Biss	GS1 Global Office	
Mats	Bjorkqvist	GS1 Sweden	
Enzo	Blonk	GS1 Global Office	
Gary	Bond	Dental Directory	
David	Buckley	GS1 Global Office	
Jaewook	Byun	Auto-ID Labs at KAIST	
Emanuela	Casalini	GS1 Italy	
Maria Madalena	Centeno	GS1 Portugal	
Madalina	Cernat	GS1 Romania	
Peter	Chambers	GS1 Australia	
Patrick	Chanez	INEXTO SA	
Jeffrey	Corthell	DoD Logistics AIT Standards Office	
Flavia	Costa	GS1 Brasil	
Luiz	Costa	GS1 Brasil	
Marco	Da Forno	GS1 Switzerland	
Brian	Daleiden	TraceLink	
Tim	Daly	GS1 Ireland	
Owen	Dance	GS1 New Zealand	
Guilherme	de França	GS1 Brasil	
Kevin	Dean	GS1 Canada	
Jeffery	Denton	Amerisource Bergen Corporation	
Christopher	Devins	Adents High-Tech International	
Véra	Feuerstein	Nestle	Editorial team
Richard	Fisher	DoD Logistics AIT Standards Office	
Frederique	Fremont	C.H.I Robert Ballanger	
Britta	Gallus	METRO Wholesale & Food Specialist AG	
Nilson	Gasconi	GS1 Brasil	
Stefan	Gathmann	GS1 Ireland	
Joseph	Germanos	GS1 Lebanon	
Alan	Gormley	GS1 Ireland	
Sudu	Gupta	ITradeNetwork.com, Inc.	
Rami	Habbal	GS1 UAE	
Ruediger	Hagedorn	The Consumer Goods Forum	

First name	Last name	Organisation	Project role
Mark	Harrison	Milecastle Media Limited	Editorial team
Karolin	Harsanji	GS1 Sweden	
Dave	Harty	Adents High-Tech International	
Heidi	Ho	GS1 Hong Kong, China	
Bernie	Hogan	GS1 US	
Martin	Hörberg	ICA AB	
Yoshihiko	Iwasaki	GS1 Japan	
Coen	Janssen	GS1 Global Office	GS1 project team / lead editor
jia	jianhua	GS1 China	
Sungkwan	Jung	Auto-ID Labs at KAIST	
Nora	Kaci	GS1 Global Office	GS1 project team
Andrew	Kennedy	FoodLogiQ	
Sangtae	Kim	Auto-ID Labs at KAIST	Editorial team
Sabine	Klaeser	GS1 Germany	Editorial team
Ulrike	Kreysa	GS1 Global Office	
Freddy	Ladino Perdomo	GS1 Colombia	
Earl	Lappen	GS1 Australia	
Carolyn	Lee	GS1 Global Office	Editorial team
Piergiorgio	Licciardello	Di.Tech S.p.A.	
Mikko	Luokkamäki	GS1 Finland	
Feargal	Mc Groarty	St. James's Hospital	
Timothy	Marsh	GS1 Global Office	GS1 project team
Doug	Migliori	ControlBEAM Digital Automation / ADC Technologies Group	Editorial team
Paula	Montanari	Jumbo Retail Argentina	
Gena	Morgan	GS1 Global Office	GS1 project team
Naoko	Mori	GS1 Japan	
Reiko	Moritani	GS1 Japan	
Hirokazu	Nagai	Japan Pallet Rental Corporation	
Giada	Necci	GS1 Italy	
Denis	O'Brien	GS1 Ireland	Co-chair, editorial team
Benjamin	Östman	GS1 Finland	
James	O'Sullivan	GS1 UK	
Michel	Ottiker	GS1 Switzerland	
Fany	Palafox	GS1 Mexico	
Edward	Pang	GS1 Hong Kong, China	
Rachel Ann	Paran	GS1 Singapore	
Nicolas	Pauvre	GS1 France	
Raphael	Pfarrer	GS1 Switzerland	
Sarina	Pielaat	GS1 Netherlands	
Neil	Piper	GS1 UK	

First name	Last name	Organisation	Project role
Francesca	Poggiali	GS1 Global Office	
Jane	Proctor	Canadian Produce Marketing Association	
ABHIJIT	PURADKAR	GS1 India	
Halim	Recham	GS1 Algeria	
Christopher	Reed	Johnson & Johnson	
Paul	Reid	GS1 UK	
Craig Alan	Repec	GS1 Global Office	
Ryan	Richard	GS1 US	
Rich	Richardson	GS1 US	
Patrice	RIGOLLE	GS1 France	
Dirk	Rodgers	Systech International	
Sylvia	Rubio Alegren	ICA AB	
Bonnie	Ryan	GS1 Australia	
John	Ryu	GS1 Global Office	GSMP Group Facilitator
Yamineth	Samudio	GS1 Panama	
Roxana	Saravia	GS1 Argentina	
Ulrich	Schäfer	GS1 Germany	
Rosalie	Schill	ipiit	
Sue	Schmid	GS1 Australia	
Eugen	Sehorz	GS1 Austria	
Faye	Shih	GS1 Chinese Taipei (formally known as GS1 Taiwan)	
Kim	Simonalle	Qliktag Software (formally Zeebric LLC)	
Steven	Simske	HP Inc	Editorial team
Andy	Siow	GS1 Singapore	
Michele	Southall	GS1 US	
Peter	Sturtevant	GS1 US	
Tania	Snioch	GS1 Global Office	
John	Szabo	GS1 Australia	
Diane	Taillard	GS1 Global Office	GS1 project team
Hiromitsu	Takai	GS1 Japan	
Sue	Thompson	National Council for Prescription Drug Programs	
Elena	Tomanovich	GS1 Global Office	
Ken	Traub	Ken Traub Consulting LLC	Editorial team
Ed	Treacy	Produce Marketing Association (PMA)	
Ralph	Troeger	GS1 Germany	Editorial team
Vivian	Underwood	GS1 US	
Regan	Van Tassel	Ecolab	
Krisztina	Vatai	GS1 Hungary	
Linda	Vezzani	GS1 Italy	
Elizabeth	Waldorf	TraceLink	Co-chair, editorial team

First name	Last name	Organisation	Project role
Ian	Walters	GS1 UK	
Qian	WANG	GS1 France	
Yi	Wang	GS1 China	
David	Weatherby	GS1 Uk	
Tomas	Wennebo	GS1 Sweden	
wang	wenyu	GS1 China	
Joachim	Wilkens	C & A SCS	
Sophia	Wu	GS1 Chinese Taipei (formerly known as GS1 Taiwan)	
Xinmin	Wu	GS1 China	
Belle	Yang	GS1 Chinese Taipei (formerly known as GS1 Taiwan)	
Cindy	Yin	GS1 Hong Kong, China	
Tony	Zhang	FSE, Inc.	
H.P.	Zwinkels	Floricode	