



The Global Language of Business

GS1 System Architecture

How GS1 standards fit together

Release 12.0, Oct 2024

Document Summary

Document Item	Current Value
Document Name	GS1 System Architecture
Document Date	Oct 2024
Document Version	12.0
Document Issue	
Document Status	Approved
Document Description	How GS1 standards fit together

Log of Changes

Release	Date of Change	Summary of Change
1.0	14 February 2012	Initial release
2.0	February 2013	Update based upon recent standard changes
3.0	14 April 2014	Update based upon recent standard changes
4.0	May 2015	Applied new GS1 branding and clarifications in the classes of keys (section 4.3) and approved following GSMP Community Review.
5.0	April 2016	Updates based upon recent standard changes
6.0	Feb 2017	Updates based upon recent standard changes
7.0	Feb 2018	Updates based upon recent standard changes
8.0	Feb 2019	Updates based upon recent standard changes
9.0	Feb 2020	Major review based upon simplification effort, new GS1 Data Services Strategy & recent standard changes.
10.0	Jun 2021	Major review and revision to AIDC (Capture) section (based on Data Carriers & GS1 RfF and GS1 Digital Link introduction), GS1 Data Services section, references to Technical Bulletin on Semantics and to accommodate recent standard changes.
11.0	Jun 2022	Material changes to Identification (key tiers), AIDC (RFID examples), Share (introduction of state data within visibility data, and Glossary (resolving overloaded terms such as object, attribute) sections
11.1	Mar 2023	Minor release to support alignment with the GS1 Digital Signature standard.
12.0	Oct 2024	Material changes based on deprecation of GEPIR and other updates to the Data Services section

Disclaimer

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 DOCUMENT. GS1 disclaims all liability for any damages arising from use or misuse of this document, whether special, indirect, consequential, or compensatory damages, and including liability for infringement of any intellectual property rights, relating to use of information in or reliance upon this document.

GS1 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 5**
- 2 Overview of the GS1 System Architecture 5**
 - 2.1 The role of standards 5
 - 2.2 Open value networks 6
 - 2.3 GS1 standards: Identify, Capture, Share, Use..... 7
 - 2.4 Digital value networks 10
- 3 General considerations 11**
 - 3.1 Standards, guidelines, data services, solutions..... 11
 - 3.2 GS1 System Architecture vs. End user system architecture 13
 - 3.3 Scope of standards..... 14
 - 3.4 Consistency across data standards 15
- 4 Identify – GS1 identification keys..... 15**
 - 4.1 Data modelling terms 15
 - 4.1.1 Entities 15
 - 4.1.2 Data elements 16
 - 4.1.3 Keys 16
 - 4.1.4 Terms relating to construction of GS1 identification keys 16
 - 4.2 GS1 identification keys (simple or compound) and AIDC data 17
 - 4.3 GS1 tiers of identification keys..... 18
 - 4.3.1 Tier 1 keys..... 19
 - 4.3.2 Tier 2 keys..... 19
 - 4.3.3 Tier 3 keys..... 19
 - 4.3.4 Tier 4 keys..... 20
 - 4.3.5 Summary..... 20
 - 4.4 Identifier Syntax: Plain syntax, GS1 element string, EPC URI, GS1 Digital Link URI..... 21
- 5 Capture – Automatic Identification & Data Capture (AIDC) 22**
 - 5.1 Automatic Identification & Data Capture (AIDC) architecture 23
 - 5.2 Automatic Identification and Data Capture Workflow 24
 - 5.2.1 Generic AIDC Workflow Functions 25
 - 5.2.2 GS1 Barcode-Specific Workflow 25
 - 5.2.3 2D Symbol (GS1 Digital Link URI) Specific Workflow 26
 - 5.2.4 GS1 EPC/RFID-Specific Workflow 28
 - 5.2.5 Sensor Device-Specific Workflow 29
 - 5.3 AIDC data carrier independence of data 30
 - 5.4 Types of AIDC data carriers 31
- 6 Share – Business data and communication 33**
 - 6.1 Content of standardised business data 33
 - 6.1.1 Master data..... 34
 - 6.1.2 Transaction data..... 35
 - 6.1.3 Visibility data 36
 - 6.1.4 Data flow 37
 - 6.2 Communication of business data 38



- 6.3 Data and service discovery 39
 - 6.3.1 Originating Party Service Lookup 39
 - 6.3.2 Identifier Resolution 40
 - 6.3.3 Event Data Discovery 40
- 6.4 Worldwide federation 40
- 6.5 Layering of interface standards – Content vs. Syntax vs. Transport 41
- 7 GS1 Data Services 42**
 - 7.1 Services offered by GS1 Global Office to GS1 Member Organisations 43
 - 7.1.1 Core Data Services 43
 - 7.1.2 SaaS Component Services 44
 - 7.2 Services offered by GS1 Global Office to Public 44
 - 7.2.1 Verified by GS1 on gs1.org 44
 - 7.2.2 GS1 Resolver Query Service 44
 - 7.3 Standards Support Resources offered by GS1 Global Office to Public 45
 - 7.3.1 Global Product Classification (GPC) Browser 45
 - 7.3.2 GS1 Navigator 45
 - 7.3.3 Check Digit and Check Character Pair Calculator 45
 - 7.3.4 GS1 GitHub Site 45
 - 7.3.5 Tools for EPC and EPCIS 45
 - 7.3.6 GS1 Web Vocabulary 46
 - 7.3.7 GS1 Application Identifier Browser 47
 - 7.3.8 GS1 Barcode Syntax Resource (BSR) 47
 - 7.3.9 GS1 TraceWay 47
 - 7.4 Services offered for the GDSN 47
- 8 Glossary 48**
- 9 References 52**

1 Introduction

This document defines and describes the architecture of the GS1 system of standards. The GS1 system is the collection of standards, guidelines, solutions, and services created by the GS1 community.

The primary audience for the *GS1 System Architecture* includes end users, solution providers, GS1 Member Organisations, and others engaged in the definition and implementation of the GS1 system.

This document has several aims:

- To introduce each of the components that are part of the GS1 system and to show how they are related. It also shows the relation between GS1 standard components and standards published by other organisations such as ISO, UN/CEFACT or W3C.
- To explain the underlying technical foundations that guide the design of individual standards and service components within the GS1 system.
- To provide architectural guidance to end users and solution providers who want to use the GS1 system and to set expectations as to how these elements function.

Other resources provide the technical details required to implement the GS1 system. Specifically:

- Individual data, software and hardware interfaces, as well as their use in open value network applications. These interfaces are defined by GS1 standards developed by the GS1 Community through the Global Standards Management Process (GSMP).
- Hardware and software components that implement GS1 standards. Implementers are free to innovate in the design of components, so long as they implement the interface between components in accordance with GS1 standards.
- GS1 Data Services that are operated and deployed by GS1 itself, by other organisations to which GS1 delegates responsibility or by third parties.

Many parts of the GS1 system are well-established and covered by GS1 standards. Other parts of the GS1 system are evolving to meet needs that are determined by industry-prioritised use cases. For those elements of the system that are evolving, architectural analysis may be underway within the GS1 Architecture Group for the purpose of ensuring that the GS1 system remains cohesive.

This document identifies which parts of the GS1 system are well-established architecturally and which parts are expected in the near future.

2 Overview of the GS1 System Architecture

2.1 The role of standards

The GS1 system is based on globally unique identification and digital information. GS1 standards have the following objectives:

- *To facilitate interoperability in open value networks*

Parties exchanging information must have agreement on the structure, meaning and mechanism of data exchange. The GS1 system includes technical standards for identification, automatic identification and data capture (AIDC) (i.e., barcodes and RFID tags), master data standards (e.g. product catalogue), and information exchange standards (e.g. Electronic Data Interchange), visibility event data (e.g., EPCIS). They also include application standards that determine a normative use of technical standards for a specific business use case.

- *To foster the existence of a competitive marketplace for interoperable system components*

GS1 standards define interfaces between system components that may be produced by different vendors or by different organisations' in-house development teams. This enables choice and leads to economies of scale that reduces costs for end users.

- *To encourage innovation built upon a standards foundation.*

GS1 standards define interfaces. Interface standards ensure interoperability between competing systems. By building value-added features or functions upon a standard foundation, implementers can have greater confidence in the eventual adoption of their products and systems and, therefore, increased confidence to invest in innovation.

GS1’s structure and processes enable it to engage a community of users who collaborate to develop standards and specifications based on business use cases and scenarios within open value networks. The developments are done in line with the GS1 architecture principles, which ensures consistency and integrity in the GS1 system of standards. As the community of users grows, the benefits to each user multiply.

2.2 Open value networks

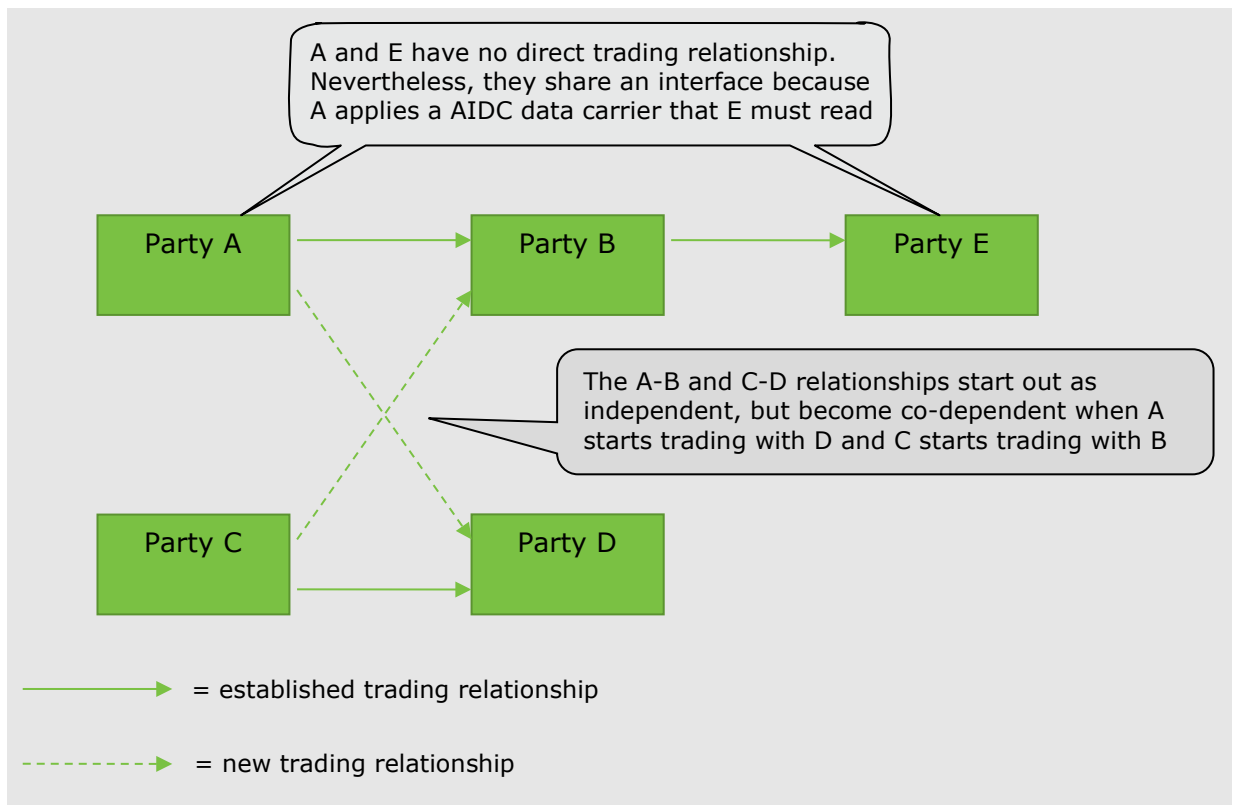
An *open* value network is one where the complete set of trading partners is not known in advance and changes over time and where, to a certain degree, trading partners are interchangeable. This has great significance for the architecture and design of information systems. Interfaces between different system components form the basis of interoperability. In a value network, the most important interfaces are those that exist *between* different organisations.

GS1 standards are designed for open value networks where collaboration takes place across industry, regulation, and processes. GS1 operates in an area where this collaboration makes sense and where competition law requirements are met, the reason why GS1 was established.

Closed/proprietary networks exist either within a company, within a consortium of companies or across an industry domain and have established networks to support their trade and transport operations. The challenge is when a closed interface no longer remains within the specified domain and incorporates other parties not originally subject to the requirements then the parties need to collaborate on changes to the network.

Open value networks need standards-based interfaces. However, standards-based interfaces are generally a good approach for closed value networks as well because they may extend over time and involve parties that were not involved initially. GS1 standards, designed via collaboration with and across industry, can bridge the gap between a closed and open network.

Figure 2-1 Open value network



The open nature of value network interfaces manifests itself in two ways, as illustrated in [Figure 2-1](#).

Firstly, an interface may exist between two companies that do not have a direct business relationship. For example, a manufacturer may mark a product with machine-readable data in a barcode, the product may then be sold to retailers through distributors. In this case, the barcode can be read by all retailers who receive the product (because of the use of a common standard). In this example, the barcode is an interface between the manufacturer and the retailers (and increasingly with consumers via initiatives such as GS1 Digital Link), but the manufacturer's only direct business relationship is with their distributors.

Secondly, a company may find over time that it needs to extend an existing interface to communicate data to new companies. For example, suppose that Companies A and B are in a trading relationship and utilise an electronic interface for exchanging purchase order and invoicing information. Companies C and D are in a similar relationship. Sometime later, Company A may find that it needs to trade with Company D, and likewise C may find that it needs to trade with B. The fact that all four companies already use common data interface standards enables Company A to use the identical interfaces and supporting information systems to trade with D as it does to trade with B, and likewise for C as it trades with B and D.

To ensure that standards are broadly adopted, interface definitions need to be negotiated and implemented *outside* the context of any trading relationship. Then, they need to be adhered to by all parties to ensure interoperability. For a standard to be adopted broadly, it must enable interoperability and be maximally applicable to a broad range of business contexts. These are precisely the foundation that underlie GS1 standards.

2.3 GS1 standards: Identify, Capture, Share, Use

GS1 standards support the information needs of end users that interact with each other in value networks. The subjects of such information are the entities that are part of those business processes. Entities include things traded between companies, such as products, raw materials, packaging, and so on; equipment needed to carry out the business processes such as containers, transport, machinery; physical locations where business processes are carried out; legal entities such as companies; service relationships; business transactions and documents; and others.

Entities may exist in the physical world (such entities are generically called *physical objects* in this document) or may be digital or conceptual. Examples of physical objects include a consumer electronics product, a transport container, and a manufacturing site (location entity). Examples of digital objects include an electronic music download, an eBook, and an electronic coupon. Examples of conceptual entities include a trade item class, a product category and a legal entity.

GS1 standards may be divided into the following groups, according to their role in supporting information needs related to entities in value network business processes:

- **Identification Standards:** These provide the means to **Identify** entities so that electronic information may be stored and/or communicated about them among end users. GS1 identification keys (simple or compound) may be used by an information system to refer unambiguously to an entity such as a trade item, logistics unit, asset, party, physical location, document or service relationship.
- **Capture Standards:** These provide the means to automatically **Capture** identifiers and/or data that is carried directly on physical objects, bridging physical and digital worlds, the world of physical things and the world of electronic information. GS1 data capture standards currently include specifications for barcode and radio-frequency identification (RFID) data carriers. Capture standards also specify consistent interfaces to readers, printers, and other hardware and software components that read the content of AIDC data carriers and connect this data to relevant business applications. The industry term Automatic Identification and Data Capture (AIDC) is sometimes used to refer to the standards in this group, though in the GS1 System Architecture a clear distinction is maintained between identification and automatic identification and data capture (AIDC) because not all identification is automated and not all data capture is identification.
- **Share Standards:** These standards provide the means to **Share** information, both between organisations and internally, providing the foundation for electronic business transactions, electronic visibility of the physical and digital world, and other applications. GS1 standards for

information sharing include standards for master data, business transaction data, and visibility event data, as well as communication standards for sharing this data between applications and trading partners. Other information sharing standards include standards such as those that define the resolver infrastructure for GS1 Digital Link, which help to locate where relevant data resides across a network.

- **Use of Standards:** GS1 Application Standards provide a normative selection of technology and data to meet business or regulatory requirements. These standards establish definitions, rules, and/or conformance specifications that shall be followed by all trading parties to establish a critical mass for implementation and the confidence of solution providers supporting that implementation.
- While GS1 standards may be used in any combination, the “Identify, Capture, Share” paradigm is pervasive in situations where GS1 standards apply, and most business application standards employ GS1 standards from all three groups. For example, consider the business processes that “Use” GS1 standards to support the retail sale of consumer goods. GS1 standards are commonly used as follows:
 - **Identify:** Each class of trade item is assigned a Global Trade Item Number (GTIN) following GS1 identification standards. Because of this, any retailer/marketplace is assured of having a unique way to refer to a given trade item in its information systems, regardless of which trade items it chooses to carry. Each product brand owner need only assign a single identifier to its trade item for use globally.
 - **Capture:** Each trade item carries its GTIN directly on the product package using a barcode that complies with GS1 barcode standards, possibly also using a GS1-compliant RFID tag. Automated identification is used to retrieve information about the item scanned or read or record events as physical objects as they move through the value network, from shipping to receipt to point-of-sale.
 - **Share:** Brand owners may share product master data with retailers through GS1 master data standards. GS1 Electronic Data Interchange (EDI) standards may be used by the retailer to reorder products from the manufacturer when supplies run low. GS1 visibility event data standards may be used to provide detailed information about the movements of goods, such as what products entered and exited each store.

The relationship between GS1 standards for identification, capture, and share is depicted below.

Figure 2-2 Identify, Capture, Share, and Use relationships



When discussing the Technical Standards, the key relationships between Identify, Capture, and Share layers are as follows:

- Both capture and share standards make use of unique identifiers for entities. There is a dependency between the capture/share standards and the identification standards.

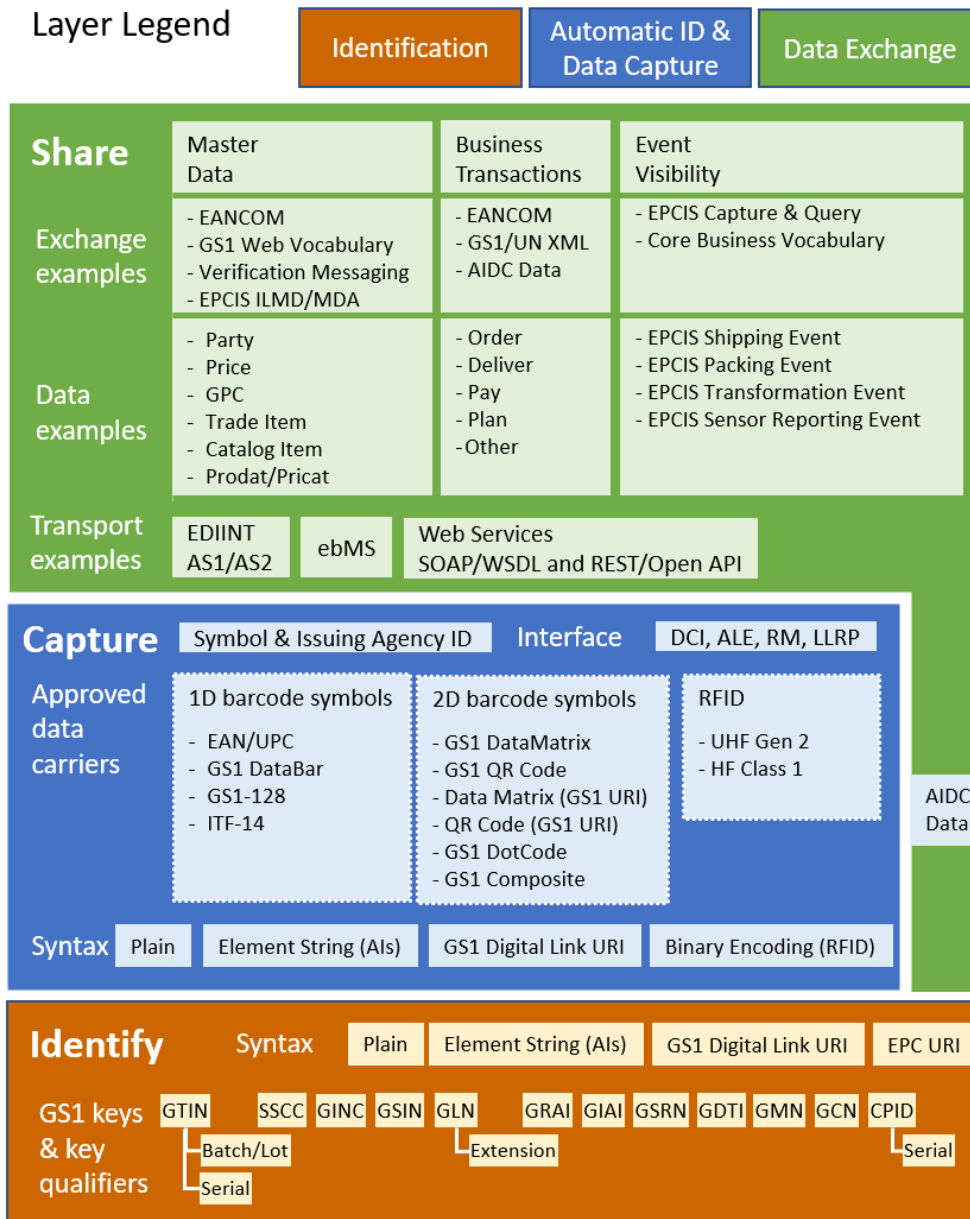
- Where an entity exists in the physical world, AIDC data carriers are used to bridge the physical and digital worlds. In such situations, GS1 capture standards come into play, and sit between the identification standards and the sharing standards.
- There are other situations in which identification is used directly by sharing standards without any AIDC data capture. For example, master data describing a trade item may be shared between trading partners without any physical product having been produced yet. There are also cases where the capture layer provides business data through an AIDC data carrier such as the weight of an item in a barcode at retail point-of-sale (POS).

Within each broad category of standards for identification, capture, and share, there are many individual standards that may be classified into subcategories. The following figure illustrates various GS1 system components and how they fit into this framework. They are discussed at greater length in the following sections.



Note: [Figure 2-3](#) is not exhaustive in its details. For example, the number of EDI message standards in GS1 would fill the Figure and the identification layer does not contain all examples for the use of GTIN, such as count of GTINs contained within a Logistic Unit, ITIP, GTIN with Third Party Serial Number. For a more comprehensive list of GS1 standards, visit <https://www.gs1.org/standards/log>

Figure 2-3 Visual representation of the Identification, Automatic Identification & Data Capture, and Data Exchange Standards (Services covered in Section 7)



2.4 Digital value networks

The central idea of a digital value network is that all information exchange is carried out electronically, through network pathways that effectively parallel the physical path taken by goods. In a fully realised digital value network, physical objects carry only a globally unique GS1 identification key, and all other information is communicated digitally using the unique identifiers to link the information to the physical objects unless there is a compelling reason to do otherwise. Changes in information needs may be accommodated without the need to re-engineer the business processes for marking and scanning physical objects. The use of global standards facilitates the rapid integration of new partners into the overall open value network.

The digital value network is based on the following principles:

- **Globally unique identification:** All objects of interest, whether identified at the class or instance level, in the value network should be identified with a globally unique identifier.

- **Affixing as few AIDC data carriers as possible:** If an object is physically handled, ideally only one AIDC data carrier should be affixed to carry the object's unique identification.
- **Use master data to express static / quasi-static data about entities:** All relevant descriptive data elements of an entity should be as master data associated with the entity's unique identification and communicated between parties using synchronisation or other means.
- **Use common data definitions in business documents, internal and external:** Business data exchanged between applications within a company and between companies should refer to objects using their unique identification. Descriptive information about those objects needed to process the data may then be obtained through master data.

This approach is directly supported by GS1 Identification, Automatic Identification & Data Capture, and Data Exchange standards. .

3 General considerations

The term "GS1 system" refers broadly to all the artefacts created by the GS1 community, including GS1 standards, GS1 guidelines, GS1 solutions, and GS1 data services. This section defines more precisely what is meant by each of these terms and makes some general statements about how they are used.

3.1 Standards, guidelines, data services, solutions

There are four types of artefacts that make up the GS1 system:

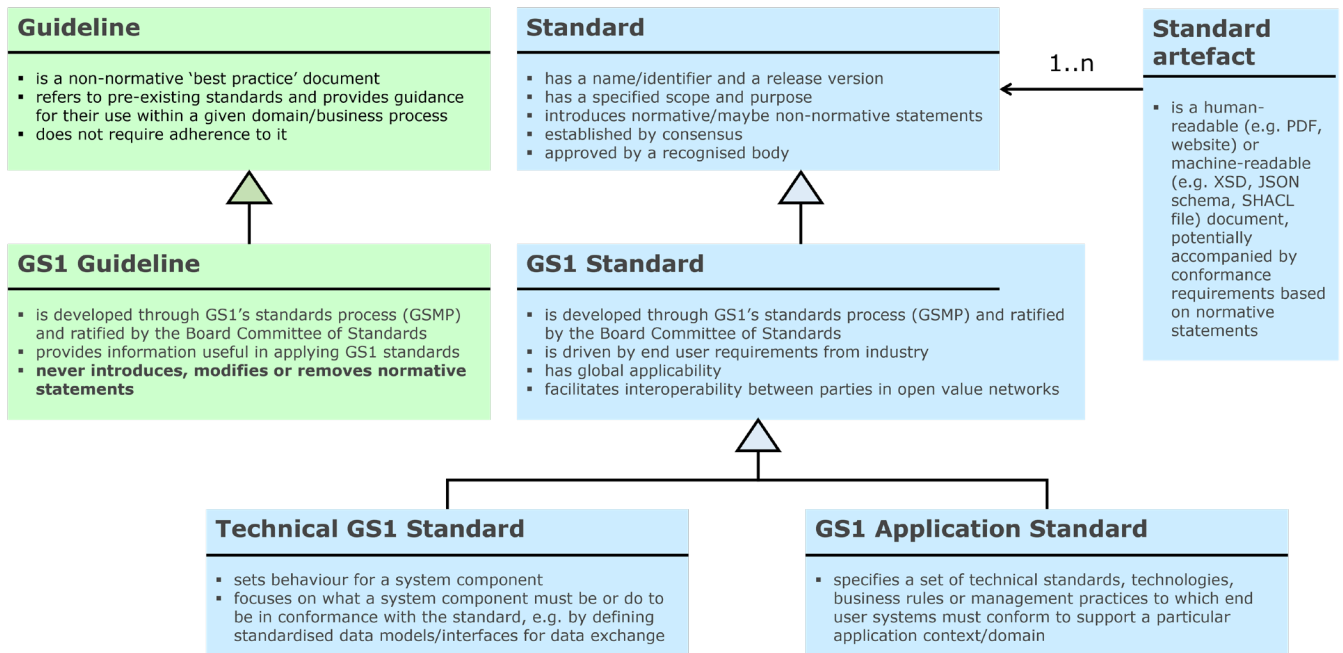
- **GS1 standard:** One or more documents that (a) provide normative specifications and rules developed with a balance of stakeholders represented via transparent due process (Global Standards Management Process) and (b) establish conformance requirements for the structure, meaning, and mechanism of data exchange between parties to facilitate efficiency and interoperability in open value networks.
- **GS1 guideline:** Best practice document which provides information considered useful in implementing one or more GS1 standards, developed with a balance of stakeholders represented via transparent due process (Global Standards Management Process) and which never introduces, modifies or removes normative content beyond the standard(s) to which it refers.
- **GS1 data service:** GS1 standards-based applications offered to industry to address a specific business need. A GS1 data service may be static (e.g., the Global Product Classification browser, which offers a simplified way to navigate the GPC schema) or dynamic (e.g., Verified by GS1, which is a lookup service coordinated by GS1 GO that provides all end users with the ability to lookup licence information and data about GS1 identification keys).
- **GS1 solution:** GS1 offering to industry that combines GS1 standards, services, guidelines, and/or other activities to address a specific business need. An example of a GS1 solution is GS1 traceability which includes standards, data services, training, certification, guidelines, etc.

GS1 standards may be further distinguished according to the type of normative content they contain, as follows:

- **Technical standards:** Defines a set of behaviours for a system component. Technical standards focus on "what" a system component must be or do to be in conformance with the standard. Technical standards may define standardised data models and/or standardised interfaces for the exchange of data. Technical standards are typically written to be as broadly applicable as possible across business sectors and geographic regions.
- **Application standards:** Specifies a set of technical standards to which end user systems must conform to support a particular business process application. Application standards provide a convenient way for different end users to express their agreement to follow certain standards to achieve mutually agreed interoperability goals in a given application context.

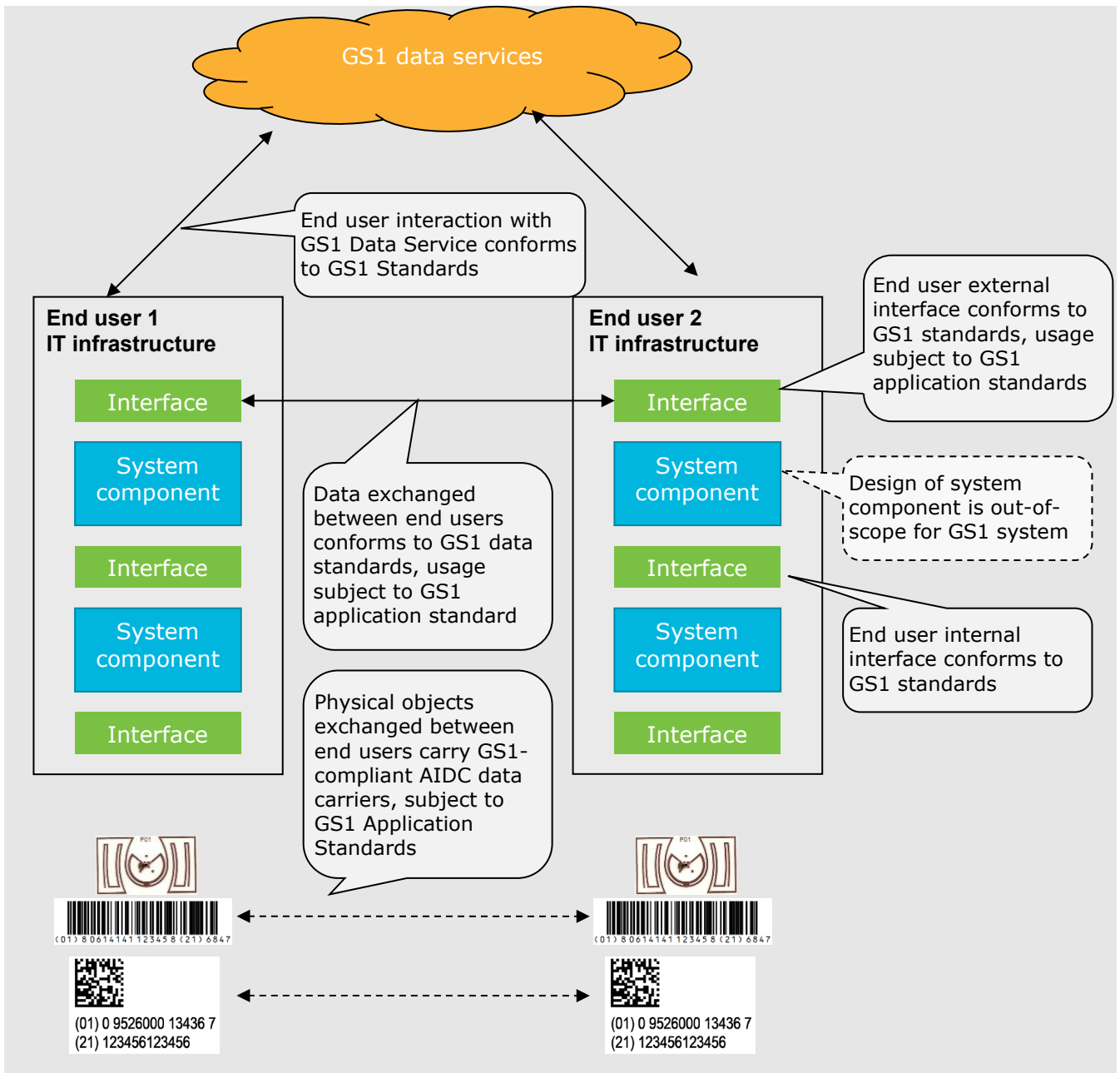
The following figure summarises the terminology for standards and guidelines.

Figure 3-1 Summary of Standards and Guidelines terms and characteristics



The following diagram illustrates how systems deployed by end users make use of GS1 system artefacts.

Figure 3-2 Use of GS1 standard components in End user systems



3.2 GS1 System Architecture vs. End user system architecture

The GS1 system is a collection of interrelated standards, guidelines, services, and solutions. End users deploy systems that make use of elements of the GS1 system. Each end user will have a system architecture for their deployment that includes various hardware and software components. These components may use GS1 standards to communicate with each other and with external systems. They may also make use of GS1 data services to support certain tasks. An end user's system architecture may also use alternative or additional standards, including data and interfaces beyond those defined by GS1.

The *GS1 System Architecture* is a conceptual model of the GS1 system. It does not define a system architecture that end users must implement, nor does it dictate hardware or software components an end user must deploy. GS1 standards only define data and interfaces that the end user's components may implement. An end user system architecture may need to employ only a subset of the GS1 standards and GS1 data services. The mapping between hardware and software

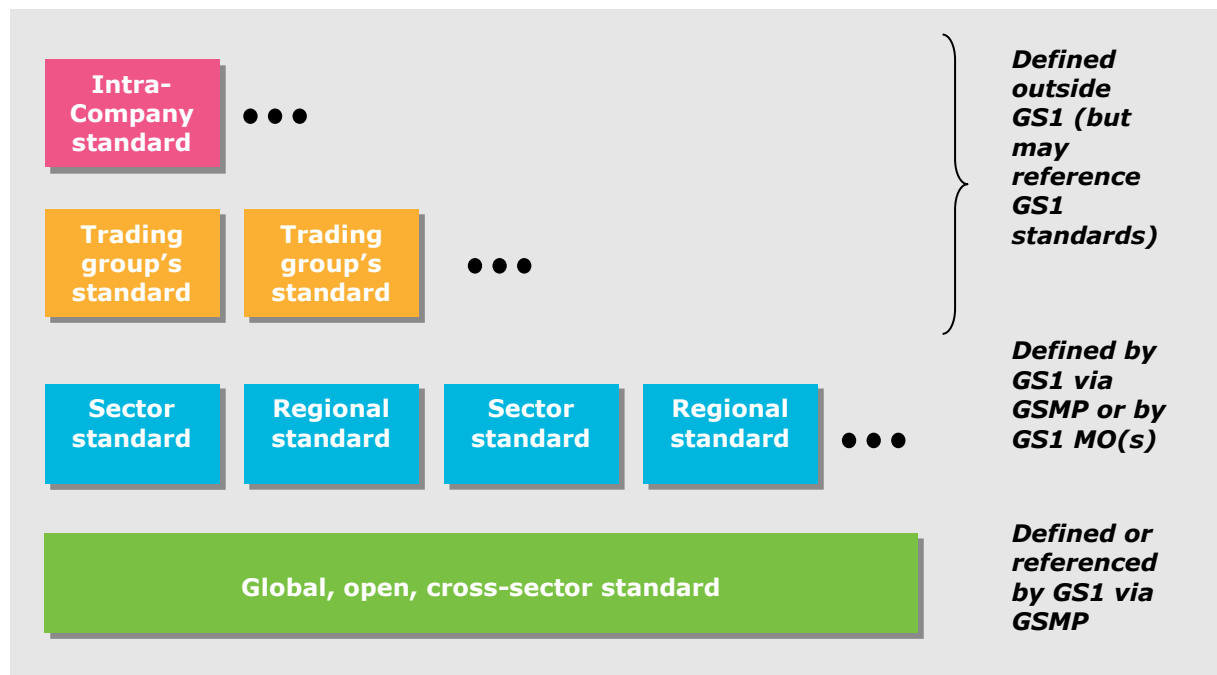
components depicted in this document and actual hardware or software components deployed by an end user may not necessarily be one-to-one. The roles depicted in this document may be carried out by end user system components that may have additional responsibilities outside the scope of the *GS1 System Architecture*.

3.3 Scope of standards

To the greatest extent possible, the components of the GS1 system are designed to be broadly applicable across all industry sectors and geographical regions. However, there are often needs that exist only within a sector. A similar pattern sometimes arises among smaller groups of trading partners within an industry and even among the divisions of a single company.

This leads to a hierarchy of standards, illustrated below:

Figure 3-3 Scope of standards



The hierarchy is as follows:

- **Global, cross-sector:** At the core of any implementation are the components of the GS1 system that have broad applicability across industry sectors and geographical regions. Most of the GS1 technical standards fall into this foundational layer. Some GS1 Application Standards are global and cross-sector.
- **Sector / Regional:** An industry sector may develop GS1 Application Standards for use within that industry and/or region. There are also certain GS1 data standards that are sector specific. Sector-specific standards apply to all geographical regions and are developed globally via GSMP. Regional requirements may be addressed via GS1 Application Standards or by other normative documents created by GS1 Member Organisations to serve their respective geographical regions. Such documents may also be sector-specific, or they may be cross-sector. Both sector and regional standards should always be designed to be used seamlessly with the global standards. It is essential that users who do not use sector or regional standards are not disrupted by others' use of them.
- **Trading group:** A trading group within an industry sector or region may establish specific rules for use among themselves, building upon the GS1 system. Such rules may be developed outside of GS1, but can reference GS1 standards, guidelines and/or services.
- **Company:** Individual companies are encouraged to develop their own internal architectural standards to drive the consistent use of GS1 standards across the enterprise.

Great care must be taken so that sector, regional, trading group, or company standards do not inadvertently create problems. A sector, regional, or trading group standard can create problems if some companies find themselves having to operate within two or more such sectors, regions, or trading groups that have mutually incompatible requirements. Ideally, requirements are pushed to the global level (and into global standards) whenever possible.

3.4 Consistency across data standards

Many GS1 standards include normative definitions of data. These include definitions of individual data elements, definitions of “documents” or data structures comprised of many individual data elements, and definitions of messages that are exchanged between system components as well as definitions of interfaces / APIs through which data can be exchanged or retrieved.

Each GS1 standard that defines data is designed to be self-contained and so includes a normative definition of each data element; however, many data elements recur across different GS1 standards and so some means of achieving consistency is required.

Today, data elements and their definitions within GS1 are published in the GS1 Navigator and to some extent, in the GS1 Web Vocabulary (WebVoc).

The scope of the GS1 Navigator is the GS1 Business Message Standards (BMS) and their components with definitions for GDSN, GS1 XML for EDI, and links to the GPC browser and the GS1 Web Vocabulary, as used by the GS1 Registry Platform (GRP). The GS1 Navigator is not a GS1 standard itself, but is a tool that helps to promote consistency across the GS1 standards within its scope.

The GS1 Web Vocabulary is an external extension to schema.org, enabling products, organisations, locations etc. to be described in greater detail and expressed as Linked Data.

Harmonisation work on GS1 data standards is underway to address conflicts and inconsistencies within and between them, to reduce duplication, and to document divergences which are either intentional or where alignment efforts are in progress. Both the GS1 Navigator and the GS1 Web Vocabulary aim to integrate data models from other standards not included in either. GS1 is working on a plan to develop a true “Single Semantic Model”. This approach will ensure full interoperability between implementations of different standards because they will all be based on the same definitions and process models.

4 Identify – GS1 identification keys

This section discusses the architectural foundations that support GS1 standards for identification. For more details and examples, please refer to Semantic Data Modelling Technical Bulletin [here](#).

4.1 Data modelling terms

This section defines common data modelling terms that apply to GS1 standards for identification.

4.1.1 Entities

An entity is something that is the subject of information in an information system. An entity may be:

- **Physical:** A physical object to which an AIDC data carrier (barcode or RFID tag) may be physically affixed.
- **Digital:** An artefact that exists in information systems and which has a recognisable lifecycle. Examples include a music download, an eBook and a digital coupon.
- **Abstract:** A virtual object or process, including legal abstractions (e.g., a party), business abstractions (e.g., a class of trade item), intangible items which forms part of a trading relationship (e.g., repair of an item or a haircut).

4.1.2 Data elements

Information systems are concerned with associating information with entities. The items of associated information are called data elements.

- **Data element:** One piece of information or one identification component associated with a specific thing, transaction, or event. A data element may be recognised if one can construct a sentence of the following form: "The [data element name] of [entity] is [data element value]."

Data elements can be classified based on how frequently they change.

- **Static data element:** A data element whose value does not change over the life of the entity. E.g., the load capacity of a specific forklift.
- **Dynamic data element:** A data element whose value changes frequently over the life of the entity. E.g., the price of a product.

4.1.3 Keys

Information systems refer to an entity by means of a key.

- **Key:** A data element or group of data elements of an entity that serves to uniquely identify that entity. An information system uses a key as a proxy for the entity itself.

Often a single data element is usable as a key, but sometimes a group of data elements is required. In data modelling terminology, these are called simple keys and compound keys, respectively.

- **Simple GS1 identification key:** A single data element that serves as a key. (E.g., a Global Service Relation Number assigned by a hospital to a patient).
- **Compound GS1 identification key:** Two or more data elements that together serve as a key. (E.g., the combination of a GTIN and serial number identifies an individual instance of a trade item).

To be usable as a key, a data element or set of data elements must have certain properties:

- **Uniqueness:** A given key value corresponds to one and only one entity within the specified domain; two different entities within the specified domain must have different values of their keys.
- **Completeness:** There exists a key value for every entity within the specified domain.
- **Persistence:** The same key value denotes a given entity throughout the entity's life, including its representation in digital form.

4.1.4 Terms relating to construction of GS1 identification keys

In many applications, and in the case of GS1 identification, keys are designed specifically for the purpose of being a key. When developing GS1 identification keys, some design considerations apply:

- **Syntax:** Common syntax rules include a choice of character set, limits on length, specifying fixed or variable length, having a grammar that supports a hierarchical structure.
- **Capacity:** The uniqueness and completeness requirements for being a key are affected by the capacity that is implied by the syntax rules.
- **Assignment methodology:** Keys can be assigned centrally from one single coordinating body or in a distributed manner. When intended to be assigned in a distributed manner, a hierarchical structure is often used, where some portion of the key is assigned by a central party and the assignment of the remainder is delegated to other parties, who may in turn delegate a portion of their portion, etc. This is the way GS1 has organised the assignment of GS1 identification keys, in a three-level hierarchy: GS1 Global Office, GS1 Member Organisation, GS1 licensee.
- **Resolution:** The ability to locate data related to a specific value of a key, or at least to determine an entry point to locate such data.
- **Non-significance:** A key is non-significant to the extent that it does not embed business information about the entity it identifies; such information is instead *associated* with the key. Components within compound GS1 identification keys (such as serial numbers or batch/ lot

numbers) may contain significance internal to a company (e.g., shift, production line) but no other company in an open value network shall be expected to interpret or use this significance.

4.2 GS1 identification keys (simple or compound) and AIDC data

GS1 standards enable unique, global identification of entity and enable standardised exchange of data related to the identified entity.

- **GS1 identification key (simple or compound):** The term "GS1 identification key" refers to those identifiers which are simple GS1 identification keys (GTIN, SSCC, etc.), and the term "key qualifier" refers to additional data elements that are designated for use as part of a compound key (e.g., GTIN + serial number is a compound GS1 identification key, with GTIN and the serial number being a key qualifier for the GTIN).
- **AIDC data:** Descriptive data elements of entities defined by GS1 standards, other than GS1 identification keys, which are capable of being directly affixed to an entity using an AIDC data carrier, e.g., best before date. While these are architecturally part of the Share layer, the Capture layer defines the syntax for including them in AIDC data carriers.
- **Other business data:** Any data element that is not an GS1 identification key (simple or compound), e.g., product description. These are part of the Share layer of the *GS1 System Architecture*.

GS1 identification keys (simple or compound) and AIDC data are themselves identified using *GS1 Application Identifiers (AIs)*. An AI is a short string (2, 3, or 4 characters) that identifies the data element, its brevity is particularly suited to identifying data elements when encoded into AIDC data carriers.

The following table summarises the GS1 identification keys in relation to the definitions in section [4.1.3](#). The column with the most relevant GS1 identification key (simple or compound) in the table below indicates which GS1 identification key may serve as a "key" (in the data modelling sense) for the entity listed in the first column.

Table 4-1 Entities identified by GS1 identification keys (simple or compound)

Entity	Physical / Digital / Abstract	Simple or Compound GS1 Key	Applicable to Digital Signatures
Trade item class	Abstract	GTIN	
Trade item batch or lot	Physical	GTIN + AI 10 (Batch or lot number)	
Trade item instance	Physical or Digital	GTIN + AI 21 (Serial number)	Yes
Unit pack Unique Identifier	Physical or Digital	GTIN + AI 235 TPX (Third Party Controlled, Serialised Extension of GTIN)	Yes
Individual trade item piece	Abstract	ITIP	
Individual trade item piece instance	Physical or Digital	ITIP + AI 21 (serial Number)	Yes
Logistic unit	Physical	SSCC	Yes
Legal entity (Party)	Abstract	GLN (AI 417, Party GLN)	Yes
Physical location	Physical	GLN (AI 414, Id of a physical location)	Yes
Physical location + extension	Physical	GLN + AI 254 (GLN extension component)	Yes
Digital location	Digital	GLN	Yes
Function	Physical or Abstract	GLN	Yes
Returnable asset class	Abstract	GRAI without optional serial number	
Returnable asset instance	Physical	GRAI with serial number	Yes

Entity	Physical / Digital / Abstract	Simple or Compound GS1 Key	Applicable to Digital Signatures
Individual asset	Physical or Digital	GIAI	Yes
Document type	Abstract	GDTI without optional serial number	
Document instance	Physical or Digital	GDTI with serial number	Yes
Service relation provider	Physical or Abstract	GSRN (AI 8017)	Yes
Service relation provider instance	Physical or Abstract	GSRN (AI 8017) + AI 8019 (Service Relation Instance Number)	Yes
Service relation recipient	Physical or Abstract	GSRN (AI 8018)	Yes
Service relation recipient instance	Physical or Abstract	GSRN (AI 8018) + AI 8019 (Service Relation Instance Number)	Yes
Consignment	Abstract	GINC	
Shipment	Abstract	GSIN	
Payment slip	Physical or Digital	GLN + AI 8020 (Payment slip reference number)	Yes
Coupon	Physical or Digital	GCN without optional serial number	
Coupon instance	Physical or Digital	GCN with serial number	Yes
Component / part class	Abstract	CPID	
Component / part instance	Physical	CPID + AI 8011 (CPID serial number)	Yes
Product model	Abstract	GMN	

4.3 GS1 tiers of identification keys

The GS1 identification keys are the foundation of the GS1 system. However, some GS1 standards make provision for the use of other systems of identification for which organisations other than GS1 are the issuing authorities. For this reason, enumeration of the tiers of keys, drawn from a GS1 perspective, clarifies the relationship between a GS1 identification key and others that may be incorporated into the GS1 system.

The following tiers of keys are defined:

- **Tier 1:** Keys controlled and administered entirely by GS1.
- **Tier 2:** Keys whose framework is controlled by GS1 and for which a portion of the identification capacity is allocated to an identification scheme administered by an external agency.
- **Tier 3:** Keys fully administered and controlled outside GS1 and which are explicitly supported as primary identifiers in some parts of the GS1 system.
- **Tier 4:** Keys fully administered and controlled outside of GS1, and which may be implicitly supported as primary identifiers in some parts of the GS1 system.

These tiers are described in more detail in sections [4.3.1](#) through [4.3.4](#) then summarised in section [4.3.5](#).



Note: The tier enumerations apply only to keys that are used as primary identifiers. The GS1 system makes provision for external keys as secondary identifiers, both explicitly and implicitly, in various ways. Some examples:

- Additional Party IDs are supported in the Global Data Dictionary.
- The GS1 Web Vocabulary supports secondary identifiers in multiple classes.
- AI 90 (Information mutually agreed between trading partners) can be used, by agreement, for any additional data.

- GS1 Digital Link supports any query parameter as long as the client and server agree on its definition.

4.3.1 Tier 1 keys

The structure, usage, and lifecycle rules of a GS1 tier 1 key are defined, administered, and managed entirely by GS1. A tier 1 key always incorporates a GS1 Prefix. A tier 1 key may incorporate a GS1 Company Prefix issued to a user company, who then issues the key, or it may be issued in its entirety as an individual key. Tier 1 keys are subject to allocation rules defined in GS1 standards, and their association with descriptive data elements is governed by validation rules also defined in GS1 standards.

The tier 1 keys are GTIN, GLN, SSCC, GRAI, GIAI, GSRN, GDTI, GINC, GSIN, GCN, CPID and GMN.

4.3.2 Tier 2 keys

The structure of a GS1 tier 2 key is defined by GS1 as a GS1 tier 1 key, but its usage and lifecycle rules are defined, administered, and managed by an external organisation.

A tier 2 key exists within the range of a GS1 Prefix or a GS1 Company Prefix, incorporates additional characters administered by an external organisation, and includes a check digit or a check character pair if required by its corresponding tier 1 key format. Tier 2 keys are unique with respect to tier 1 keys of the same type and can be used in most or all applications that support the corresponding tier 1 key type. Their allocation and lifecycle rules, however, are defined by an organisation external to GS1. The degree to which the usage and lifecycle rules are compatible with those of the corresponding tier 1 keys is specific to each tier 2 key.

Examples of tier 2 keys include:

- The International Standard Serial Number (ISSN) under GS1 Prefix 977 to form keys compatible with GTIN-13.
- The International Standard Book Number (ISBN) under GS1 Prefixes 978 and 979 to form keys compatible with GTIN-13.
 - A subset of ISBNs starting with 9790 are reserved for the International Standard Music Number (ISMN).
- Club Inter Pharmaceutique (CIP) codes for pharmaceuticals in France under GS1 Prefix 34 to form keys compatible with GTIN-13.
- Produce Electronic Identification Board (PEIB) codes in North America under U.P.C. Company Prefix 033383 (GS1 Company Prefix 0033383) issued by GS1 US, combined with a commodity code issued by the Produce Manufacturers Association, to form keys compatible with GTIN-12.

The arrangements leading to the existence of tier 2 keys are exceptional and subject to accreditation agreements between the MO or GO and the third party. The GS1 Policy on the Licensing of GS1 Identification Keys by or with the Assistance of Third Parties governs the establishment of such arrangements.

4.3.3 Tier 3 keys

The structure, usage, and its lifecycle rules of a GS1 tier 3 key are defined, administered, and managed entirely by an organisation external to GS1. This organisation enters into an agreement with GS1 that enables its keys to be supported in selected GS1 standards (e.g., within an EPC header). This organisation enters into an agreement with GS1 that enables its keys to be supported in selected GS1 standards (e.g., within an EPC header).

Tier 3 keys are supported in selected GS1 standards without disrupting users of tier 1 and tier 2 keys, but:

- GS1 gives no assurance that tier 3 keys will be recognised by users of tier 1 and tier 2 keys.
- GS1 has no expectation that systems relying upon tier 3 keys should recognise keys from tier 1 or tier 2.

- GS1 has no expectation that systems relying upon one type of tier 3 key should recognise other types of tier 3 keys.

Companies can take advantage of GS1 technology, network, and communications standards for tier 1, 2, and 3 keys, but should not expect the same level of interoperability between keys in tiers 1 and 2 and keys in tier 3 with the rest of the GS1 system. Tier 3 keys may be usable only within a subset of the GS1 system (e.g., within EPCIS but not GS1 EDI), the limitations being defined on an individual basis for each tier 3 key.

Keys in tier 3 at the present time are:

- Keys compliant with US Department of Defence (USDoD) and Airline Transport Association (ATA) standards (ADI-var) that are based on the Commercial and Government Entity (CAGE) and Department of Defense Activity Address Code (DoDAAC) identification standards.
- Bureau International des Containers (BIC) codes.
- International Maritime Organization Vessel Number (IMO).
- EPC General Identifier (GID)**.
- NATO Stock Number

These keys are supported in the *GS1 EPC Tag Data Standard* and, consequently, have EPC URIs that can be used in EPCIS.

4.3.4 Tier 4 keys

The structure and, usage, and lifecycle rules of a GS1 tier 4 key are defined, administered, and managed entirely by an organisation or entity external to GS1.

A tier 4 key has no explicit support within the GS1 system, but it may have some implicit support. For example, the EPCIS standard supports any URI as an object identifier and trading partners could, by mutual agreement, agree to use URIs for geographic locations as a ReadPointID for certain events.

GS1 gives no assurance that any tier 4 key will be recognised by any user.

4.3.5 Summary

The following table summarises the key classification discussed above.

Table 4-2 Tiers of GS1 Identification keys characteristics

Tier	Managed	Contract	GS1 Prefix	Interoperability*
1	By GS1	N/A	Yes	Full
2	Externally	Required	Yes	Variable
3	Externally	Required	No**	Limited
4	Externally	No	No	None

* Interoperability is the ability to use the GS1 identification key within the context of business processes supported by GS1 standards.

** One exception is GID GS1 Prefix 951. While the key itself does not contain a GS1 Prefix, the portion of the key that semantically corresponds to the GS1 Prefix is 951, and this GS1 Prefix is reserved for that use to avoid confusion with tier 1 and 2 GS1 identification keys. The General Manager Number, required for new GID issuers, has not been issued by GS1 GO since 2012.

4.4 Identifier Syntax: Plain syntax, GS1 element string, EPC URI, GS1 Digital Link URI

When a GS1 identification key or other identifier is used in an information system, it is necessarily represented using a specific syntax. The syntax that is used may depend on the medium in which the identifier exists; for example, when GS1 identifiers are exchanged via information systems, text-oriented representations are used, even though the identifier may have been encoded in a binary representation within the data carrier (e.g. RFID tag, 2D barcode).

GS1 standards provide various syntaxes for identifiers:

- **Plain (physical, digital) syntax:** This syntax is just the GS1 identification key with no additional characters or syntactic features. For example, a Global Location Number (GLN) is represented as a 13-character string, each character being a digit. The plain syntax is usable in a context where only a single type of GS1 identification key is expected. Examples of such single-key contexts include: a barcode symbology that is defined to only hold one type of GS1 identification key (e.g., ITF-14 which can only hold a GTIN), a column in a database table that is intended to hold only a single GS1 identification key.
- **GS1 element string (physical):** This syntax consists of a short (2-4 character) "application identifier" that indicates what GS1 identification key (simple or compound) or AIDC data follows, followed by the key or data value itself. This allows one type of GS1 identification key or AIDC data to be distinguished. Related to the GS1 element string is the "concatenated element string", in which two or more AI-value pairs are concatenated into a single string (with delimiters, if needed). This provides a syntax for compound keys such as GTIN + serial number or keys and AIDC data such as GTIN + weight + expiry date.
- **Electronic Product Code (EPC) URI (physical, digital):** This syntax is a Uniform Resource Identifier (URI), specifically a Uniform Resource Name (URN) beginning with `urn:epc:id:...` and the remainder having a syntax defined by the *GS1 EPC Tag Data Standard*. This provides a syntax for any GS1 identification key that identifies a specific physical or digital object, including some tier 3 keys as defined in section 4.3.3. Objects that are not identified at the instance-level are either expressed as an EPC Class URI (`urn:epc:class:...`) or an EPC Pattern URI (`urn:epc:idpat:...`).
- **GS1 Digital Link URI (physical, digital):** The GS1 Digital Link URI provides a syntax for expressing GS1 identification keys (simple or compound) AIDC data in a format that can be used on the Web in an intuitive manner (via a straightforward Web request) to enable direct access to relevant information and services about products, assets, locations, etc.

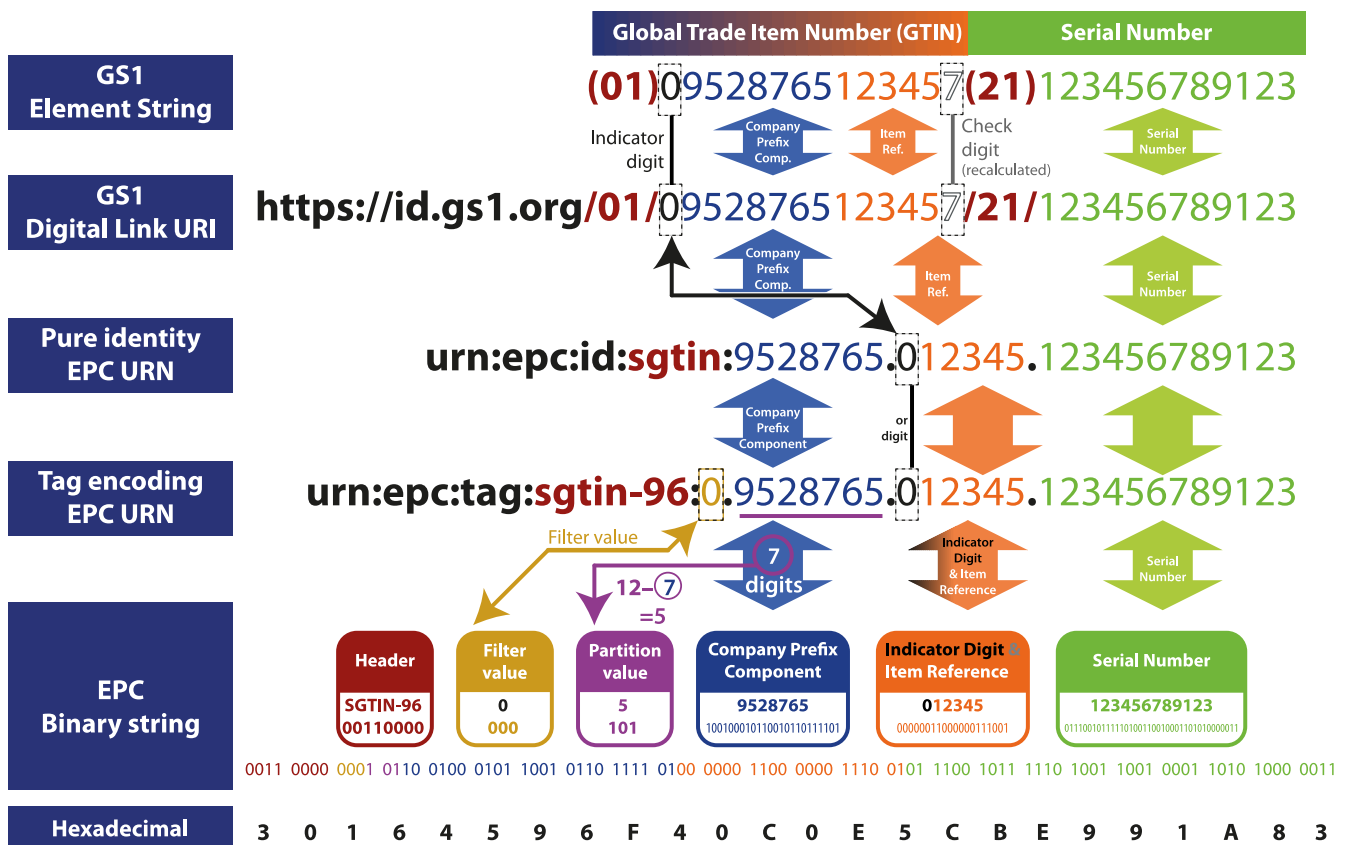
While any given GS1 identification key may be represented in more than one of the above four syntaxes, its *meaning* is always the same regardless of syntax. The following table illustrates a GS1 Global Returnable Asset Identifier (GRAI) in each of the four syntaxes:

Table 4-3 Example of GS1 identification key representation in identifier syntaxes

Syntax	Example	Remarks
Plain	9524141234564789	A GRAI composed from GS1 Company Prefix 9524141, asset type 23456, check digit 4, and serial component 789.
GS1 element string	(8003) 09524141234564789	The GS1 Application Identifier 8003 indicates the following GS1 identification key is a GRAI. The GS1 element string for GRAI also includes an extra "0" padding digit immediately following the GS1 Application Identifier. The remainder of the element string is the same as the plain syntax.
EPC URI	urn:epc:id:grai:9524141.23456.789	The "urn:epc:id:grai:" header specifies that this EPC URI corresponds to a GRAI. The GS1 Company Prefix, asset type, and serial component are separated by dot (".") characters. The check digit is not included in this syntax.

Syntax	Example	Remarks
	urn:epc:tag:grai-96:0.9524141.23456.789	Corresponding EPC Tag URI, which includes filter value and the indication of the number of bits. This corresponds one to one with the hexadecimal representation of the EPC binary encoding below.
EPC Binary	3316454EB416E80000000315	Hexadecimal representation of the EPC binary encoding 001100110001011001000101010011101011010000010110111010000000000000000000000001100010101
GS1 Digital Link URI	https://id.gs1.org/8003/09524141234564789	GS1 Digital Link URI on the id.gs1.org domain
	https://example.com/some/path/8003/09524141234564789	GS1 Digital Link URI using a custom domain name and permitting additional URI path information
	http://id.gs1.org/gAMRUwYcMwgHio	Compressed GS1 Digital Link URI on the id.gs1.org domain

Figure 4-1 Example of equivalence between different identifier representations



5 Capture – Automatic Identification & Data Capture (AIDC)

The "Capture" standards in the GS1 system are standards for automatically identifying a physical entity or for capturing other data that is associated with a physical entity. At the ISO/IEC SC31 JTC1 level, this area of technology standards is called Automatic Identification and Data Capture (AIDC). An AIDC data carrier is a representation of data in a format that is designed to be machine-readable. AIDC data carriers range in capability, from the simplest barcodes whose only function is to deliver a GS1 identification key when read, to complex 2D symbols capable of holding multiple

data elements with error correction, to the most sophisticated RFID tags which are themselves small computing devices. Interaction with RFID tags may include more than only “data capture,” though the term “capturing” is still used for the process of encoding and/or decoding data into/from AIDC data carriers. The processes involved in putting data into AIDC data carriers, including printing of barcodes and programming of RFID tags, are also included under the label of “data capture.”

This section outlines the general foundations of GS1 AIDC standards.

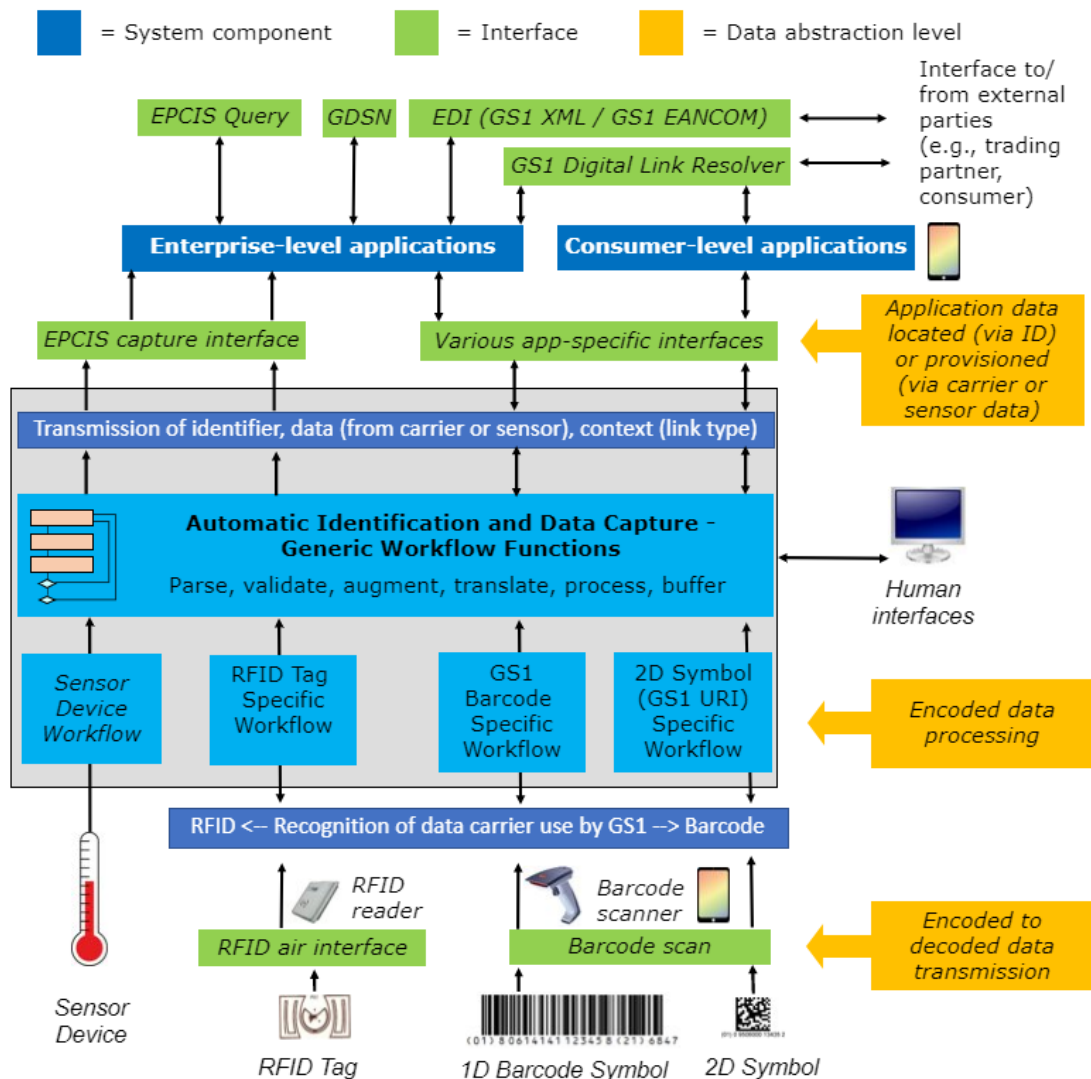
5.1 Automatic Identification & Data Capture (AIDC) architecture

The purpose of AIDC data carriers in the GS1 system is to provide a reliable way to automatically capture a GS1 identification key to link to the data held on computer systems as part of a workflow. In addition to the GS1 identification key, AIDC data (e.g., expiration date, weight, sensory data) may also be a part of the workflow. In a GS1 compliant application of AIDC data carriers, a GS1 identification key must always be present.

Within a given data capture workflow, there may be many individual interactions with AIDC data carriers. A data capture workflow may also involve interaction with humans, sensor devices, as well as with “back end” information systems such as an Enterprise Resource Planning (ERP) or Warehouse Management System (WMS). All these processes/systems combine to create the AIDC workflow, and this workflow gives meaning to the act of capturing the identifier or data from the AIDC data carrier.

For example, at a point-of-sale (POS) terminal, the business context is usually such that scanning a barcode containing a GTIN means that one instance of a product whose class is identified by the GTIN has just been purchased by the customer engaged in the checkout process. However, at the returns desk, scanning the same barcode may instead mean that the product is being returned rather than purchased. In each case, the business context gives meaning to each barcode scan.

[Figure 5-1](#) shows the elements of a typical AIDC application architecture. The exact architecture for any given AIDC application will vary from case to case. For example, not all AIDC applications use both barcodes and RFID. [Figure 5-1](#) shows commonly occurring relationships between components and how GS1 standard interfaces fit in from scan/read to application use.

Figure 5-1 Overview of the elements of a typical AIDC application architecture


5.2 Automatic Identification and Data Capture Workflow

GS1 automatic identification and data capture (AIDC) applications originates when a device (e.g., scanner, RFID reader) determines that an AIDC data carrier is carrying GS1 identifiers or AIDC data. This workflow occurs between the scan or read of the AIDC data carrier and the use of the scan/read of the GS1 identification key or AIDC by the application.

Section [5.2.1](#) describes functions that are common (independent of carrier type) within the AIDC workflow (e.g., parsing, validation, augmentation, translation, processing, buffering).

Sections [5.2.2](#) through [5.2.5](#) describe workflow functions which are specific to a particular AIDC data carrier technology, AIDC data carrier technology use of different syntax, or for sensor devices.

- Section [5.2.2](#), GS1 Barcodes with GS1 Element String syntax
- Section [5.2.3](#), 2D symbol with GS1 Digital Link URI syntax
- Section [5.2.4](#), EPC RFID
- Section [5.2.5](#), Sensor systems (e.g., monitor temperature exposure)

Each of these four sections describe the infrastructure or interfaces required, the method of determining that the data carried is encoded according to GS1 standards and provides common application examples.

5.2.1 Generic AIDC Workflow Functions

There are several functions which are utilised independently of the AIDC data carrier type. How, when, or even if they occur depend on the application requirement and the AIDC data carrier supporting the application. These functions include, but are not limited to, the items described below.

1. **Decoder:** A barcode or RFID reader consists of a scanner, a decoder (either built-in or external), and a connection method to an application. A barcode or RFID reader generally captures and decodes the barcode into numbers, letters and/or character symbols, the data must be processed by a software application to make sense of the data
2. **Parse:** In an AIDC data carrier we would parse the data by analysing the data string and applying the GS1 syntax rules (plain syntax, GS1 Element String, GS1 Digital Link URI or EPC binary). As an example, the data string parsing result could be the list of application identifiers with their values ((01)-GTIN, (10)-Lot/Batch, (17)-expiry date, (21)-serial number...).
 - i. Data string transmitted by the scanner:
jd201095011014200693922995<GS>320200010017210615422123<GS>2112345678
 - ii. 2D symbol with parsed element string data



(01)09501101420069
 (3922)995
 (3202)000100
 (17)210615
 (422)123
 (21)12345678

3. **Validate:** Is the content and data structure correctly formed based on the syntax rules. If the AIDC data carrier and the data encoded is using the correct GS1 syntax and the AIDC application meets the appropriate GS1 standards, then it is considered valid.
4. **Verification:** Does the AIDC data carrier conform to encode/decode algorithms and meet quality standards. For example, in a barcode symbol, the bars, modules and symbols must be correctly formed and meet standards for size, contrast, decodability, defects and other verification parameters.
5. **Augment:** Data and AIDC data carriers can be augmented in two ways in AIDC applications, one: the data may be augmented with business context data; and two: the AIDC data carrier may be augmented to improve decodability through error correction methods such as the Reed-Solomon algorithm.
6. **Equivalent representations:** An identifier may have multiple equivalent representations, optimised for different purposes. These can include element strings encoded in barcodes, compact binary strings encoded in EPC RFID tags or GS1 Digital Link URI syntax for easier linking to information resources on the Web.
7. **Process:** Is the defined steps from encoding an AIDC data carrier to use of the encoded GS1 identification key or AIDC data by an application to achieve the desired business or consumer outcome.
8. **Buffer:** Is a mechanism to temporarily store data while it is being moved from one place to another.

5.2.2 GS1 Barcode-Specific Workflow

GS1 barcodes infrastructure includes:

1. Barcode design software provides for all AIDC data carriers approved for use within a GS1 Application Standard. This software encodes a data string and renders a barcode image with a special start pattern to designate GS1 defined encoding and decoding that conforms to GS1

General Specifications definitions, specifications, and rules. The software may output directly to a printing system or to a file used in the production of packaging artwork.

2. Printing of barcodes may be digital or analogue. Digital printing is characterised by a print mechanism creating the barcode image on demand (e.g., thermal transfer, ink jet, laser printing devices). Analogue printing is characterised by printing a fixed barcode image onto a medium like paper or plastic using a printing press (e.g., flexographic, offset, screen printing processes).
3. Print quality verification takes place at some point after the barcode image is rendered. This may occur inline during the printing process or on a random sample basis. The devices used in this process support the methodology to measure print quality and the ability to report whether the minimum print quality needed for each application is specified in the GS1 General Specifications has been met. Conformance Test Cards are also available to ensure proper calibration of verification systems.
4. Scanning systems can determine whether the barcode carries GS1 identifiers or something else. If GS1, then the scanner system can decode the barcode according to GS1 General Specifications definitions and rules. The system includes software that supports the generic workflow functions described above. There are many types of scanners, but in broad terms, laser scanners support 1D barcodes and imaging scanners support 1D and 2D symbols.

Decoding process for a GS1 barcode

1. Determine symbology via symbology identifier standard or proprietary means. If EAN/UPC, process per GS1 definitions for its use. If ITF-14 (Interleaved Two of Five with a 14-digit numeric string) matches a GTIN look-up and validates on check digit, infer a GTIN is encoded.
2. For all other GS1 barcodes, utilise the symbology specifications for start character patterns to determine if the barcode is a GS1 barcode (encoded per GS1 definitions and rules as GS1 conforms to ISO/IEC 15459 as an Issuing Agency).
3. For GS1 barcodes, parse per GS1 element string definitions (Application Identifier and AI data field) and rules (e.g., sequence, concatenation) to yield an identifier to link to stored information or populate an event or yield business data for use or storage by the application (e.g., expiration date prevents the sale of an expired product).

Application Examples

1. General retail point-of-sale (POS) uses GS1 barcodes to identify a product and to retrieve product description and price information which are used to make check-outs faster and more accurate. GS1 DataBar can also be used at POS to provide business information beyond the GTIN like the weight of a variable measure product or an expiration date for a perishable product.
2. Transport and logistics operators use GS1 barcodes to automate receipt, storage, and movement of products and logistics units.

5.2.3 2D Symbol (GS1 Digital Link URI) Specific Workflow

2D Symbol (GS1 Digital Link URI) infrastructure

2D Symbol (GS1 Digital Link URI) shares much of the infrastructure described in GS1 Barcodes section, although the focus is on the use of 2D symbols with GS1 Digital Link URIs by consumers using apps on smartphones and other mobile devices, as well as B2B uses (e.g., GS1 Scan4Transport). Such apps need to retrieve information and interact with services on the Web over HTTP/HTTPS. For syntaxes other than GS1 Digital Link URI, the GS1 identification keys (simple or compound) and AIDC data will need to be converted into the standardised Web URI format.

Decoding process for a 2D Symbol (GS1 Digital Link URI):

The GS1 Digital Link standard defines a Web-friendly URI syntax for GS1 identifiers, including the ability to support any GS1 identifier at any level of granularity (e.g. GTIN, GTIN+Lot/Batch, GTIN+Serial) and to link or automatically redirect to multiple kinds of information and services on the Web, through the use of dedicated link types and a simple Web request for the GS1 Digital Link URI.

When a GS1 Digital Link URI is encoded within a QR code or Data Matrix symbol, there is no FNC1 or dedicated symbology identifier that indicates that the data content is defined by GS1 standards as discussed in section 5.2.2. Instead, it is necessary to check that the extracted Web URI conforms to the URI Syntax defined for GS1 Digital Link (see <https://www.gs1.org/standards/gs1-digital-link> and the URI Syntax chapter in particular). The GS1 Digital Link URI Syntax standard defines a formal grammar for constructing GS1 Digital Link URIs and also provides regular expression patterns that can be used for checking whether any Web URI is plausibly a GS1 Digital Link URI. One way to test whether a Web URI does or does not point to a GS1 conformant resolver for GS1 Digital Link is to check for the presence of a Resolver Description File in the relevant Well-Known location `/.well-known/gs1resolver` [RFC 8615]. Details of the Resolver Description File are defined in GS1 Digital Link Standard in the Resolution chapter.

1. Application Examples: For extended packaging applications, the GS1 General Specifications now permit the encoding of a GS1 Digital Link URI within a regular ISO/IEC 18004 QR Code symbol or regular ISO/IEC 16022 Data Matrix symbol. Such a 2D symbol can be scanned by a consumer smartphone, either using the native camera or Web browser applications, generic scanning apps or by dedicated apps for specific purposes. Dedicated apps might warn a consumer about allergens in a product or provide a consumer with advice about which product to choose, taking into account their dietary or ethical / sustainability preferences. Other convenient uses of GS1 Digital Link could be to scan a 2D symbol to download the instruction manual or recycling information or a patient safety leaflet for pharmaceutical products etc. Depending on the granularity of identification, QR Code and Data Matrix symbols can be printed dynamically (if the GS1 Digital Link URI is specific to a particular serial number or batch/lot) or can be generated with the general product packaging artwork if it only identifies a product by its GTIN. Additional data such as expiration date, weight can be expressed within the URI query string of a GS1 Digital Link URI.
2. Link Types are not typically included in the URI at the time of printing the QR Code or Data Matrix symbol. Instead, a mobile app or other software may specify a value for link type within the URI query string at the time of making a Web request for the GS1 Digital Link URI. This provides flexibility so that a single 2D symbol can link to multiple kinds of information and services on the Web. A full list of current defined link types can be found in the GS1 Web vocabulary at <https://www.gs1.org/voc/?show=linktypes>. A brand owner or other licensee / issuer of a GS1 identification key can specify multiple referral records per GS1 Digital Link URI, each link type indicating a specific kind of service. For example, `gs1:pip = https://gs1.org/voc/pip` points to a product information page, whereas `gs1:instructions = https://www.gs1.org/voc/instructions` points to an instruction manual. The brand owner or licensee/issuer of the GS1 identification key can also specify a default link, to select which link should be used if the client (e.g. smartphone app) does not express a preference. Often, this might be the link to the product information page, although there are product categories such as pharmaceuticals, where regulations may require this to point only to a factual patient safety information leaflet, whose structure and content is specified by legislation.
3. GS1 Digital Link URIs can be translated to element strings and element strings can also be translated to GS1 Digital Link URIs, provided that they include at least one primary GS1 identification key. GS1 provides open source toolkits to support this via its GS1 GitHub site at <https://github.com/gs1>. This translation capability enables a single barcode (based on GS1 Digital Link URI within a QR Code) to serve supply chain and retail POS use, as well as consumer-facing extended packaging use through mobile apps on consumer smartphones and devices.
4. Even before migration to a single barcode is achieved, translation to the GS1 Digital Link URI format enables existing GS1 barcodes to make use of the resolver infrastructure for GS1 Digital Link to redirect to various kinds of information and services on the Web, both for consumer-facing / B2C use and even for B2B use. There can be multiple resolvers for GS1 Digital Link but the GS1 global root resolver at `id.gs1.org` serves as a 'resolver of last resort' so that even if an existing GS1 barcode does not indicate any Internet domain name or hostname to use within the GS1 Digital Link URI syntax, `id.gs1.org` can be used to construct a canonical GS1 Digital Link URI and the GS1-operated global root resolver will redirect to any information and services specified by the respective licensee of the GS1 identification key. In some cases, this may be via national resolvers operated by individual GS1 Member Organisations on behalf of their members.

5. EPCIS v2.0 supports a constrained subset of GS1 Digital Link URIs as an alternative to the EPC URN syntax. The constrained subset corresponds 1:1 with the existing EPC schemes based on GS1 identifiers but in GS1 Digital Link URIs, the length of the GS1 Company Prefix has no significance. This will make it easier to capture EPCIS event data from GS1 barcodes even in situations where the party scanning the barcode does not know (or cannot easily determine) the correct length of the GS1 Company Prefix component; instead they will simply be able to use the GS1 Digital Link URI format instead of the EPC URN syntax. The result is that traceability event data finally becomes easier to capture consistently and correctly, independent of the type of AIDC data carrier technology encountered.
6. GS1 Scan4Transport makes use of 2D AIDC data carriers in the logistics / postal / parcel delivery sectors. Although some implementations may encode significant address, routing and delivery information within the AIDC data carrier, particularly to ensure data availability in areas of low Internet connectivity, user companies are also exploring the use of GS1 Digital Link URIs within QR Codes to support direct Web access to the most up-to-date information, which can support in-flight changes to destination address, service priority etc., which may supersede such details printed on the package or encoded within the 2D AIDC data carrier.

5.2.4 GS1 EPC/RFID-Specific Workflow

GS1 EPC/RFID infrastructure

An RFID infrastructure consists of one or more RFID **readers** and one or more RFID **tags**.

Readers transmit standardised commands (in order to read from and write) to tags by modulating a radio signal. Readers also provide operating energy to tags by transmitting a continuous-wave (CW) signal. Tags are passive, meaning that they receive all of their operating energy via this signal, without needing to rely on a battery. To respond to a reader's commands (i.e., to provide an EPC or confirm execution of an operation), a tag modulates the reflection coefficient of its antenna, returning ('backscattering') information in a binary signal to the reader.

GS1's **EPC UHF "Gen2" Air Interface** standard specifies physical (i.e., signalling, modulation and other radio parameters) and logical (i.e., tag memory, selection, inventory and access) interfaces. This standard is a close subset of ISO/IEC 18000-63, and serves as the backbone for almost all passive UHF deployments of the past 15 years.

Some deployments also make use of GS1's Low Level Reader Protocol (LLRP), which specifies an interface between RFID readers and clients for full control of air interface protocol operations and commands.

Decoding process for a GS1 EPC/RFID tag

RFID tags encoded with Electronic Product Codes (EPCs) per GS1's *EPC Tag Data Standard (TDS)* are referred to as **EPC/RFID** tags. TDS defines EPC encoding schemes (in binary and URI form) that correspond to serialised GS1 identification keys, as well as detailed encoding/decoding* algorithms to convert EPCs to GS1 element strings (and vice-versa, noting that for older EPC schemes defined before TDS 2.0 and based on GS1 identifiers, knowledge of the GS1 Company Prefix (GCP) length is also required for encoding but not for decoding). TDS also specifies the memory layout of EPC/RFID tags and the procedures for encoding supplemental AIs (such as Lot/Batch and Expiry) into a tag's "User" memory.

Tags in the so-called 'interrogation zone' are captured by a reader in the context of air interface *inventory* operations. Read range is typically up to 10 metres from the reader, but this distance can be substantially reduced or extended depending on the amount of absorbing or shielding material present, intentionally or otherwise.

The air interface *select* operation allows for pre-filtering of desired sub-populations of tags, which can enable an application to focus on tagged objects whose EPCs are part of certain class (e.g., by item reference within a GTIN plus serial number) or from a certain brand owner (i.e., by specific GCP).

Readers will often provide the hexadecimal EPC encoding of captured tags as input to application-level software which might be used to perform additional filtering and, in turn, further decode into EPC Tag URI, EPC Pure Identity URI (e.g., for inclusion in EPCIS event data), GS1 element string or GS1 Digital Link URI format(s), as required by the business process application consuming this data.

TDS is complemented by GS1's *EPC Tag Data Translation (TDT)* standard, which includes machine-readable versions of TDS encoding/decoding rules to support automated translation between these formats.

Application Examples

- 1. Retail inventory management:** The SGTIN of each item-level source-tagged article is captured by RFID readers at a retail outlet's goods receiving and added to that location's inventory database, ideally using EPCIS event data. Readers on the shop floor can be used to alert to low levels of a given product on the shop floor, to trigger re-stocking of shelves. Readers at point of sale simultaneously support automated self-checkout, electronic article surveillance (EAS) to detect the departure of unpaid merchandise and an update of the location's inventory database, in turn serving as a trigger for automatic replenishment. The increase in item-level visibility helps increase product availability and reduce out-of-stock and so-called 'NOSBOS' (*not on shelf but on stock*) situations. Customer satisfaction does not end there, as item-level tagging enables paperless returns and guarantee claims.
- 2. Rail sector - Maintenance, Repair and Overhaul (MRO):** The SGTIN or GIAI of rolling stock parts and components are captured along the entire life cycle, from manufacture to installation, servicing and eventual replacement. This provides the foundation for safe transport of passengers and cargo, as well as unambiguous exchange of visibility data between internal and external stakeholders.
- 3. Rail sector - Rolling stock visibility:** The GIAI of each wagon is captured by wayside reading units installed in regular intervals along stretches of track as well as at junctions and terminals, simultaneously linking the vehicle's GIAI with its travel direction, axle count, speed and length. This provides real-time visibility of all rolling stock within an entire rail network. including a train's departure and arrival movements, as well as its composition. Link to video: [GS1 standards keep rail companies on track](#)
- 4. Asset management of Returnable Transport Items (RTIs):** Returnable containers (e.g., pallets, plastic trays, collapsible crates, dollies) identified by GRAI are captured at each step of their processing at RTI pool warehouses, from arrival to counting and sorting, washing, repair, allocation and despatch to logistics providers. Automated inventory and maintenance procedures eliminate the need for manual intervention and guesswork, and increase transparency for pool operators and their supply chain customers.

5.2.5 Sensor Device-Specific Workflow

Sensor device infrastructure

In terms of the required infrastructure, there is a huge variety in the market of how sensor systems are designed.

First, a sensor device does not just comprise one, but typically several sensors measuring physical properties such as temperature, luminosity, movement, humidity, to mention only a few. Apart from basic devices that simply capture and provide observed physical properties as is, there are also smart sensor devices equipped with a local processing unit which, based on some local software logic, already abstracts, filters and aggregates raw sensor data.

Second, some sensor devices come with a logger feature which has the capability to locally store/cache a certain amount of data before it is transmitted or read out. In this context, there are both active and passive sensor devices, i.e. with or without an own power source enabling data transmission.

Third, there are several technologies to convey data from a sensor device to a base station: there are systems which make use of sensor gateways through leveraging e.g. Bluetooth Low Energy (BLE), RFID or Wi-Fi, whereas others transmit data directly e.g. via cellular or low power wide area networks (LPWAN).

Processing sensor data

Therefore, there is no one-size-fits-all workflow describing how sensor data is processed. Notwithstanding, the following bullet points try to characterise a typical workflow in a

generic manner (note that devices outputting signals in a non-electronic manner, e.g. consumer-facing colour-changing labels, are out of scope):

- Raw sensor data is recorded in binary (usually timestamped) datasets according to a vendor-defined protocol.
- Based on a set of business rules, a local or central capturing application parses, validates and translates these datasets into a higher-level data format which can be better processed by business applications. Thereby, the data may be augmented with business context data.

Note: An appropriate output data format after this step is an EPCIS event providing the What, When, Where, Why and How of a given sensor-based observation. EPCIS and CBV v2.0 specify a flexible framework to accommodate all kinds of sensor data.

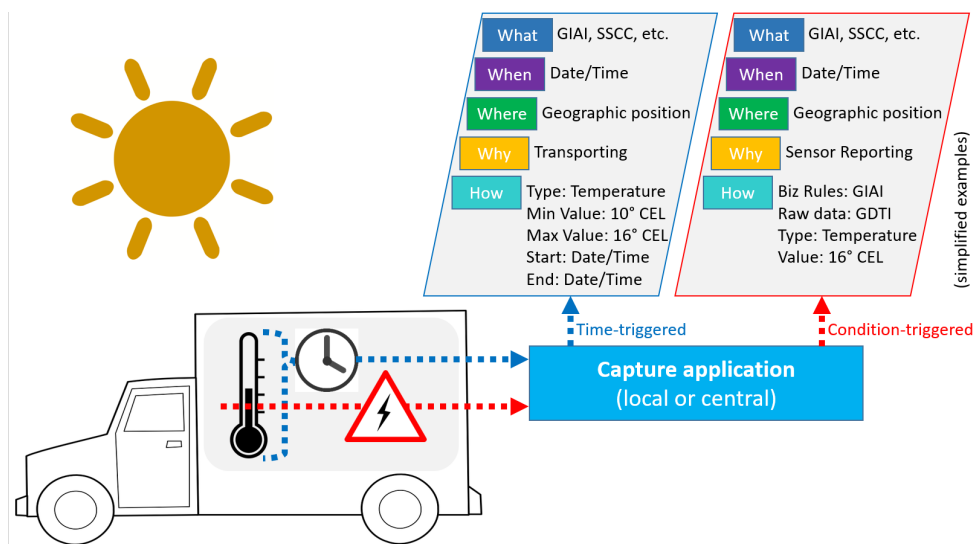
- The datasets are then made accessible to either internal or external business applications, where they may trigger business processes to properly react to the events detected by the initial sensor reading.

Application example

Cold chain compliance comprises controlling the temperature range product need to be in as well as ensuring that a defined threshold is not exceeded. Organisations, as part of supply networks in which cold chains must not be interrupted, have different choices on how to set up an appropriate infrastructure. For instance, logistics units loaded in a truck can be tagged with sensor devices that continuously transmit sensor readings to a fixed gateway which in turn (typically after some local filtering/aggregation) sends the corresponding datasets to a central capture application.

As shown in the [Figure 5-2](#), the latter consumes the datasets and translates them into EPCIS events. This could be for documentation purposes (as shown on the left simplified example) or to trigger alerts for the respective process owners in case a temperature threshold was exceeded (right simplified example). In addition, there are many further business applications (e.g., quality assurance, business intelligence, tracking & tracing) for which sensor-enhanced visibility event data are relevant.

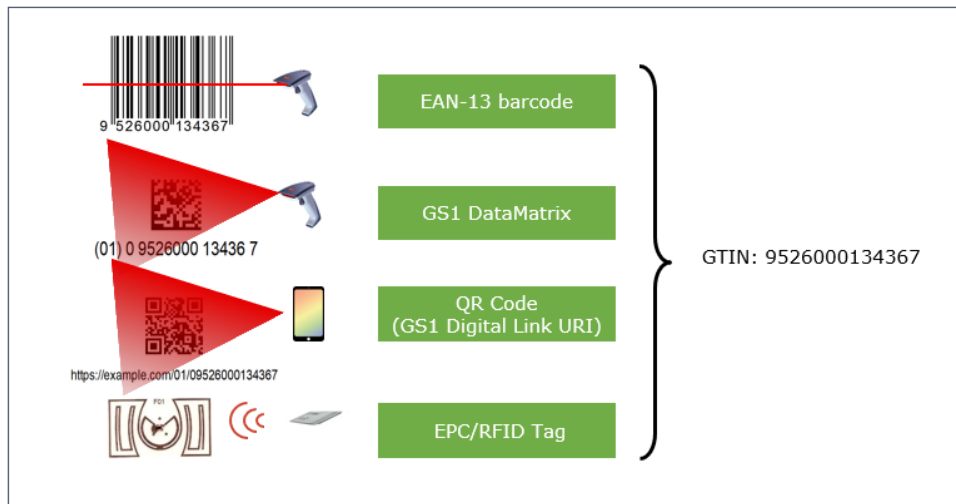
Figure 5-2 Cold chain compliance application example



5.3 AIDC data carrier independence of data

GS1 defines GS1 identification keys and AIDC data in a AIDC data carrier-neutral way so that their semantics are the same regardless of which AIDC data carrier, or electronic messaging, is used.

Figure 5-3 Four AIDC data carriers encoding the same GTIN value 9506000134352



5.4 Types of AIDC data carriers

From a GS1 perspective, we can distinguish three types of AIDC data carriers, (see [Table 5-1](#)). According to the categorisation below, only AIDC data carriers belonging to 'Type A' are considered global AIDC data carrier standards, (e.g., EAN/UPC, GS1 DataBar, GS1 2D, 2D (GS1 Digital Link URI), or UHF EPC/RFID).

Many AIDC data carrier technologies possess the capability to encode GS1 data structures, too. However, GS1 community members either did not see a (business- or technical-driven) reason to justify their introduction into the GS1 system or the technology did not meet GS1's AIDC data carrier adoption policy as defined in Policy B-11 (available on <https://www.gs1.org/standards/development/how-we-develop-standards>). All technologies that fall into this category are termed 'Type B AIDC Data Carriers'.

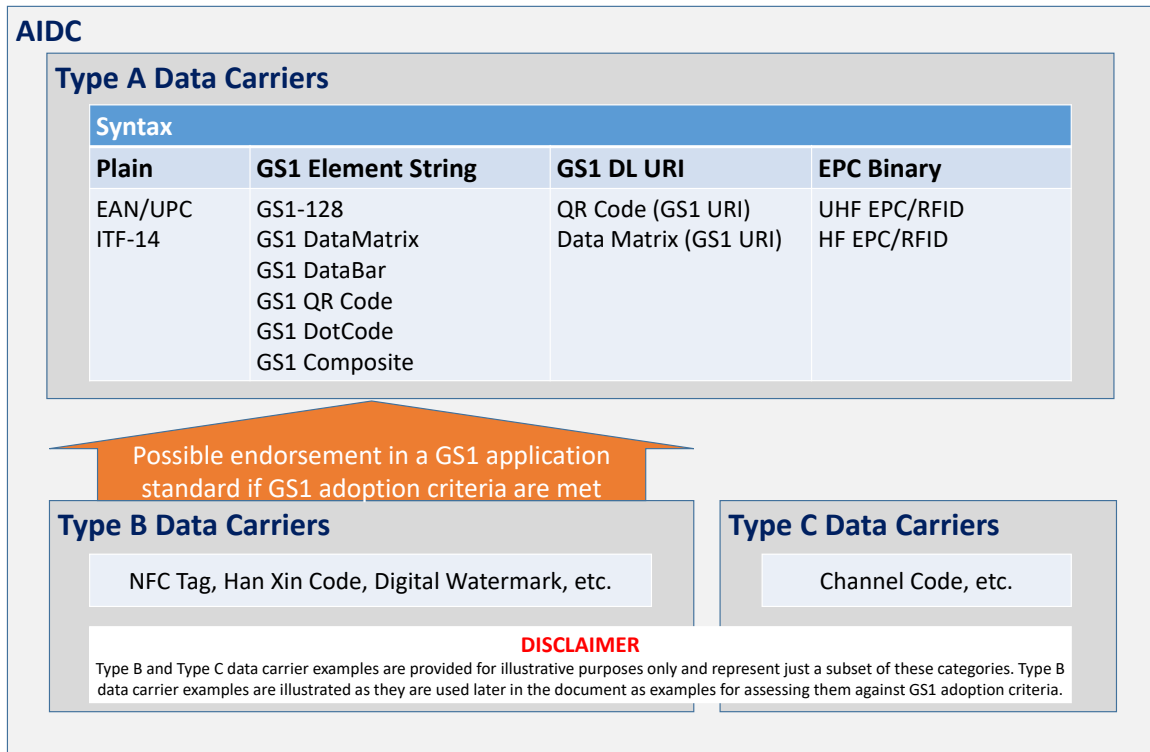
In addition, there are also carrier technologies ('Type C') that cannot encode GS1 data structures. Two examples for this category are the Deutsche Post Identcode and the Channel Code whose specifications, for instance, prohibit the encoding of any GS1 identification key apart from theoretical edge cases. [Table 5-1](#) provides a definition for each of the three AIDC data carrier types.

Table 5-1 AIDC data carrier types

Term	Definition
Type A Data Carrier	Technology (e.g. barcode, tag) attached to or integrated in a physical object for representing data elements in machine-readable format that carries GS1 data structures , which is specified for use by a GS1 application standard and which meets GS1's adoption criteria (as defined per "Policy B-11").
Type B Data Carrier	Technology (e.g. barcode, tag) attached to or integrated in a physical object for representing data elements in machine-readable format which is able to carry GS1 data structures but is not specified in a GS1 application standard .
Type C Data Carrier	Technology attached to or integrated in a physical object for representing data elements in machine-readable format which is not capable of carrying GS1 data structures .

[Figure 5-4](#) comprises an overview of all Type A AIDC data carriers in the GS1 system of standards (thereby distinguishing between the four different syntax forms which are supported so far). In addition, it names a few out of many AIDC data carrier instances that have the capability to encode GS1 data structures, but do not yet fulfil GS1's adoption criteria (Type B). Further, it makes clear that there is no chance for a Type C technology to ever become a Type A data carrier.

Figure 5-4 AIDC data carrier systematisation



The following paragraphs focus on Type A AIDC Data Carriers.

For all Type A GS1 AIDC data carriers there are three levels of abstraction through which the data passes. From highest to lowest, they are:

- **Application data:** These are GS1 data elements defined in a data-carrier neutral way. A business application sees the same data regardless of AIDC data carrier used.
- **Transfer encoding:** This is the representation of data used in the interface between a capturing application and the hardware device that interacts with the AIDC data carrier (barcode scanner or RFID Interrogator).
- **Carrier internal representation:** This is the representation of data in the AIDC data carrier itself. In a barcode, this is the pattern of light and dark bars, squares or dots. In an RFID tag, this is the binary data stored in the digital memory of the RFID chip.

Table 5-2 AIDC data carrier representations and the corresponding GS1 standards

Abstraction level	Data representation		Corresponding GS1 standard	
	Barcode	RFID	Barcode	RFID
Application data	Plain data values EPC URI GS1 Digital Link Standard (URI)		GS1 General Specifications EPC Tag Data Standard GS1 Digital Link Standard	
Transfer encoding	Plain data values GS1 element string (Application Identifiers) GS1 Digital Link URI	EPC Tag URI EPC binary encoding ISO/IEC 15962 binary data	GS1 General Specifications	EPC Tag Data Standard
Carrier internal representation	Barcode symbology	EPC binary encoding ISO/IEC 15962 binary data	GS1 General Specifications	EPC Tag Data Standard

There are three types of data that may be involved in carrier internal representation and in transfer encoding:

- **Application data:** Data that is delivered from the Capture layer to the Share layer. Application data is AIDC data carrier independent.
- **Control data:** Data that is used to control interaction with the AIDC data carrier.
- **Carrier data:** Data that describes the AIDC data carrier itself.

Table 5-3 Means of indicating GS1 data structures in Type A AIDC Data Carriers

AIDC data carrier	Means of recognition
EAN/UPC]E0,]E1,]E2,]E3, and]E4 symbology identifiers, restricted to GS1 per the symbol specification
GS1 DataBar]e0 symbology identifier, restricted to GS1 per the symbol specification
2D Composite Component]e1 symbology identifier, Restricted to GS1 per the symbol specification
ITF-14	None (legacy exception)
GS1-128]C1 symbology identifier, FNC1 start pattern per the symbol specification
GS1 QR Code]Q3 symbology identifier, FNC1 Mode
GS1 DataMatrix]d2 symbology identifier, FNC1 start pattern per the symbol specification
GS1 DotCode]J2 symbology identifier, absence of FNC1 in start pattern per symbol specification
QR Code (GS1 URI)]Q1 symbology identifier, GS1 DL URI Regular Expression
Data Matrix (GS1 URI)]d1 symbology identifier, GS1 DL URI Regular Expression
UHF EPC/RFID	Toggle bit (as defined in the EPC Tag Data Standard) set to zero
HF EPC/RFID	Toggle bit (as defined in the EPC Tag Data Standard) set to zero

6 Share – Business data and communication

This section discusses the architectural foundations underlying GS1 standards for business data sharing.

The GS1 standards for sharing business data enable automated interactions between two or more end users. The end users involved must have a common understanding of the structure and meaning of business data, and this leads to GS1 standards that define the **content** of business data. Moreover, the end users must have an agreed method of communicating data between themselves, and this leads to GS1 standards for **communication** of business data. The open nature of value networks implies that an end user may not always know in advance where to find relevant business data, and this leads to GS1 interface standards for data and service **discovery** across the value network. In an international environment, such standards must balance the need for the seamless flow of data across the world with the need to respect national sovereignty and local regulation. This leads to principles of world-wide **federation** that inform the design of GS1-provided services that aid in discovery.

These four topics are discussed in detail in the remainder of this section.

6.1 Content of standardised business data

The goal of GS1 data standards can be understood as defining relationships between entities as well as relating entities to associated data. GS1 standards for business data pertain to three categories:

- **Master data** that provide descriptive data elements of entities identified by GS1 identification keys, including trade items, parties, and physical locations.
- **Transaction data** that consists of transactions related to business processes across the value network.

- **Visibility data** provide details about the “what, when, where, why” activity in the value network. Visibility data includes event data as well as state data about current location, status etc.

6.1.1 Master data

Master data are descriptive data elements of an entity that are static or nearly so. For a trade item class, for example, master data might include the trade item’s dimensions, descriptive text, nutritional information in the case of a food product, and so on. For a legal entity, master data might include the name of the organisation, its postal address, geographic coordinates, contact information, and so on.

Master data provide the information necessary for applications to understand entities and to process them appropriately in business processes.

Data sharing in the GS1 system is built on an architectural pattern that combines data in recurring business documents with master data:

- Master data associates the GS1 identification key with the data elements that describe the corresponding entity.
- Recurring business documents with transaction data and visibility event data refer to entities by use of GS1 identification keys.
- Applications that process the recurring business documents obtain a complete set of information by combining the GS1 identification keys referenced in business documents with the associated master data. In this way, the repetition of master data elements in each recurring business document is avoided.

There are six methods supported in the GS1 system by which a data recipient may receive master data from a data source:

1. **Synchronisation in advance:** A data recipient obtains master data prior to processing any recurring business documents. This is referred to as “synchronisation” because the process of obtaining master data in this way is repeated periodically in order that the data recipient’s copy of master data is consistent (“synchronised”) with the master copy published by the data source.
2. **Peer-to-peer communication in advance:** A data source of master data can send master data directly to a data recipient in a specialised EDI message, such as Item Data Notification (GS1 XML) and Price Sales Catalogue – PRICAT (GS1 EANCOM).
3. **Query on demand:** A data recipient obtains master data for a given entity by issuing a query to a lookup service, where the query contains the GS1 identification key for the entity whose master data is desired. In this method, it is possible to defer obtaining master data associated with a given GS1 identification key until the data recipient is processing a business document containing that key.
4. **Embedding in a business document:** A business document itself may contain master data in addition to a GS1 identification key. In this way, the consuming application does not need to obtain master data from another source.
5. **Embedding in an AIDC data carrier:** An AIDC data carrier (barcode or RFID tag) affixed to an entity may contain data elements that describe the entity. GS1 standards for capture may be used to extract these data elements and pass them to a business application.
6. **Embedding in a web page:** A set of master data may be published on a web page using the GS1 Web Vocabulary. GS1 Digital Link URIs can be used to point to such data.

The first three methods in this list follow the architectural pattern of pre-aligning master data as described above. Methods 4 and 5 are used when it is not possible or convenient to pre-align master data. Method 6 can be used for pre-alignment and non-pre-alignment situations.

The following subsections cover master data for trade items in detail and for other GS1 identification keys more generally.

6.1.1.1 Master data for trade items

Master data for trade items may apply to one or more trade items. Five different scopes exist for trade item master data, each corresponding to a different level of identification:

Level	Description	Identified by	Attribute example
Model	Data elements that apply to all GTINs that are part of a "Model" or "type" of trade item.	Global Model Number	Material composition of a stent approved as a medical device and registered with a regulator
Trade item	Data elements that apply to all instances of a given GTIN are GTIN-level master data	Global Trade Item Number	Product name and its physical dimensions (for a fixed-measure trade item)
Trade item variant	Data elements that apply to a specific variant of a given GTIN	Global Trade Item Number plus Consumer Product Variant	Image for seasonal/holiday packaging
Batch/lot	Data elements that apply to all instances of a GTIN within a single batch or lot as defined by the manufacturer	Global Trade Item Number plus batch/lot number	Expiration date, identical for all instances within a given batch/lot but variable from one to the next
Instance	Data elements that apply to a single instance of a GTIN identified by GTIN plus serial number	Global Trade Item Number plus serial number	IMEI of a mobile phone

In all of the above examples, the master data does not change over the life of the trade item instances concerned. It is this static nature of such data elements that makes them "master data." The volume and rate of creation of master data is different for different scopes of business application. GTIN-level master data is created infrequently, at the rate of new product introduction, instance-level master data is created every time a new trade item instance is manufactured, and batch/lot-level master data is somewhere in between.

The Global Product Classification (GPC) defines a code that locates a trade item within a taxonomy of all trade items; a trade item's GPC code is therefore a very important master data attribute, both to describe the trade item and to identify what sets of category-specific master data might be available for that trade item.

6.1.1.2 Master data associated with other entities

Besides trade items, the entities for which master data alignment is most important are locations and organisations. The GS1 identification key for locations and organisations is the GLN. Master data related to the GLN include for example its function, postal address, geo-coordinates, opening hours, etc. In case the GLN is used to identify an organisation, the master data may include other data elements such as a company registration number, associated bank account, etc.

Master data may exist for any of the types of entities that can be identified by GS1 identification keys. In practice, the communication of master data for entities other than those identified by GTIN or GLN is achieved during the sharing of business transactions or event data related to these entities. Examples of master data about a logistics unit identified by an SSCC include content description, deliver-by date, routing code, and dangerous goods indicator.

6.1.2 Transaction data

Transaction data are business information required to support a collaborative business process shared bilaterally between organisations. Often these are functionally the same as their namesake paper documents, such as purchase order and invoice. Transaction data is consumed by software

applications, not directly by humans. This means that the GS1 design principles include rules such as only exchanging coded rather than clear text information and that master data should be aligned before exchanging the transactional data.

GS1 standards for transaction data, collectively named GS1 EDI, are provided to automate business transactions commonly occurring across value networks. This includes business processes beginning with a buyer ordering goods from a supplier and progressing to the final receipt of cash by the supplier in exchange for those goods. GS1 standards for transaction data also support business processes such as demand forecasting, transport, traceability data, clinical trials, etc.

Transaction Data are always shared within the framework of a business agreement (contract) between two parties. Each document confirms the commitment to execute the agreement; for example, sending an electronic purchase order message implies that the sender wants to receive the ordered goods according to the conditions agreed in the contract, and will pay for them.

The GS1 standards for transaction data include:

- GS1 EANCOM
- GS1 XML
- GS1 UN/CEFACT XML

6.1.2.1 EDI standards evolution

EDI standards evolve to support the emerging business requirements. There could be different technical solutions depending on the requirement. The range could be a simple addition of a new value in a code list to the creation of a new message or a set of messages. To drive consistency, identification of the best approach is a critical part of the standard evolution, keeping into account two main objectives:

1. Reduce the impact in terms of complexity and affected community outside the one requiring the change.
2. Keep the standards as much cross sectorial as possible.

To support these goals, a GSMP Procedure defines a workflow including the most relevant points to assess. This GSMP Procedure is not applicable when the business requirement is strongly related to the adoption of new technologies, not yet supported. In that case the extension of existing standards is not possible.

6.1.3 Visibility data

Visibility data consists of event data and state data. State data provides a current or historic snapshot of the location or condition of an object. Event data typically records changes in state, while the current state information may need to consider the cumulative effect of multiple events that have occurred since a previous known state.

Event data are records of the completion of business process steps in which physical or digital entities are handled. Where transaction data confirm legal or financial interactions between trading partners, event data confirm the carrying out of a physical process or a comparable digital process. Examples of processes that may be the subject of event data include affixing of identification to a newly manufactured object (“commissioning”), shipping, receiving, movement from one location to another, picking, packing, transfer at point-of-sale, and destroying.

Each event can have up to five data dimensions:

- **What:** Identification of the physical or digital object(s) involved in the event, expressed using a GS1 identification key (e.g., GTIN with a serial number)
- **When:** The date and time when the event took place
- **Where:** The physical location involved in the event, which may include:
 - The physical location where the event took place
 - The physical location where the objects are expected to be following the event

- **Why:** Details about the business process context in which the observation took place, which may include:
 - An identification of the business process taking place at the time of the event
 - The business state of the objects following the event
 - Links to relevant Transaction Data (especially in those cases where a visibility event and a business transaction occur simultaneously)
- **How:** Conditional information about an object or a physical location, as captured by sensors (ranging from simple or multi-dimensional physical observations to outputs of smart sensor devices, incl. concentration of chemical substances and microorganisms)

The GS1 Electronic Product Code Information Services (EPCIS) standard defines a standardised data model for visibility data, together with standardised interfaces for its capture and retrieval/query. While focused primarily on event data, the EPCIS data model also includes some fields with prospective semantics, such as bizLocation (business location), disposition, and persistent disposition, and that these provide a convenient mechanism to transmit some state data that can be computed locally by the organisation that captures the event, using some internal logic and consideration of previous event data known to that organisation. Sensor data, while recorded as an event, is in fact a snapshot of the state of one or more objects or their environment at a point in time.

State data provides a current or historic snapshot of the location or condition of an object. Event data typically record changes in state, while the current state information may need to consider the cumulative effect of multiple events that have occurred since a previous known state.

Visibility state data indicate the current location, state, or status of an object. This could include its disposition, such as whether or not it has been recalled or reported stolen. State data is typically derived from event data and transaction data, considering the cumulative effect of the event data and transaction data gathered to date and may require cross-checks of master data, such as whether the expiration date on the product packaging agrees with the expiration date for that product instance, as recorded by the respective manufacturer or brand owner. The processing of event data into state data may involve a set of logical rules that might be expressed as 'finite state machines' or flowcharts that explain a sequence of permitted / non-permitted changes in state.

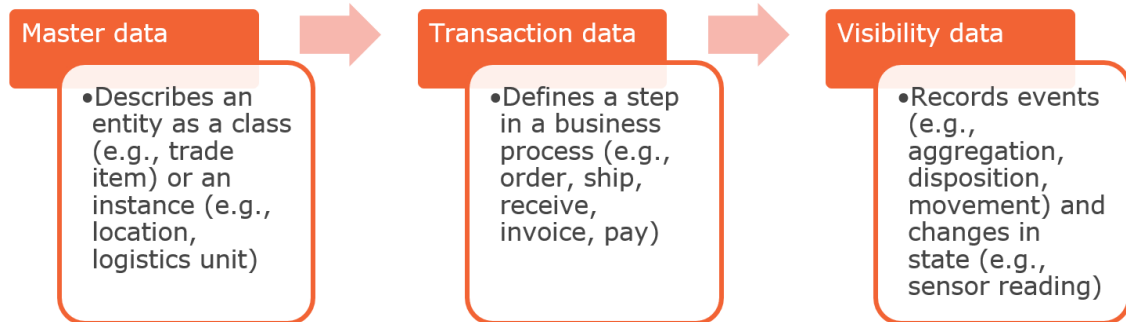
An example of state data is the data retrieved via the GS1 Lightweight Verification Messaging standard, which provides a simple and lightweight messaging framework for value network participants to ask verification questions to each other, such as whether an individual product instance was commissioned and whether it is still considered suitable for onward distribution or dispensing. The standard defines how actionable information can be shared between parties. Messaging is based on various authentication checks on the product identifier and associated data. Whereas EPCIS could be used to retrieve event data about the individual product instance, multiple events may need to be retrieved and analysed in order to provide an actionable answer about whether that product instance is suitable for onward distribution or dispensing.

6.1.4 Data flow

Examples of three business processes that generate different kinds of data:

- In some cases, a visibility event coincides with a business transaction, so that there may be a piece of transaction data and a piece of event data describing different aspects of the same occurrence. For example, when products are shipped from a loading dock, there may be a Despatch Advice confirming the sender's intent to deliver specific products to the receiver and one or several "shipping" EPCIS events confirming the observation of products leaving the loading dock.
- A visibility event may occur with no corresponding business transaction. For example, when a trade item moves from the "back room" storage of a retail store to the sales area where a consumer can purchase it. This is a highly relevant event for purposes of assessing availability of product to consumers (and changes its state), but it has no associated business transaction.
- A business transaction may take place with no corresponding visibility event. For example, when a buyer sends an "order" message to a supplier, there is a legal interaction, but nothing occurring in the physical world where the ordered products reside.

Figure 6-1 Relationship between different types of data



6.2 Communication of business data

GS1 standards offer several methods for communication of Business Data between end users. In summary, the methods are:

- **“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, 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 publicly accessible place such as a World Wide Web page, where it may be retrieved by any interested party.
- **“Pull” or “query” methods**, where one party makes a request for specific data to another party, who in turn responds with the desired data.

In principle, any of the above communication methods could be used for any of the categories of business data that are governed by GS1 business data standards. In practice, the type of data dictates the most appropriate communication methods and GS1 standards support the combinations that end users have found to be most useful. They are summarised in the table below:

Table 6-1 Summary of the most useful communication methods per data type

Data Type	Example data	Data standard	Available communication methods			
			Bilateral “Push”	Publish/Subscribe	Broadcast	“Pull” (“Query”)
Master Data	Trade item / catalogue item Batch/lot master data	GDSN (supported by GS1 XML CIN & EANCOM PRICAT as noted below)	✓	✓		
	Instance-level master data (ILMD)	EPCIS				✓ (master data query, ILMD)
	Location / party info	GS1 Web Vocabulary			✓ (via web pages)	
Transaction Data	Order Delivery Pay	GS1 EDI XML GS1 EANCOM	✓			
Visibility Event Data	Observation Aggregation Transformation	EPCIS	✓ (via AS2)	✓ (standing queries)		✓

6.3 Data and service discovery

GS1 standards for business data and communication provide the means for two end users to share business data reliably, once they have identified each other. GS1 standards for data and service discovery exist to help end users identify each other.

In general, there are four ways that one end user might identify sources of data owned or maintained by other end users:

- **Pre-arrangement:** In many cases, one end user identifies another by means of some pre-arrangement that takes place outside the scope of any GS1 standard. For example, bilateral sharing of business transaction data via GS1 EDI typically takes place between end users who have identified each other in advance and agreed to trade with each other. Pre-arrangement requires no GS1 standards. In principle, it is possible to share data across an entire value network by exploiting pre-arrangement in a "1 up, 1 down" pattern. In this pattern, it is presumed that each party in a value network has pre-arranged data pathways established between its immediate predecessor ("1 up") and immediate successor ("1 down") with respect to the flow of goods. Such pathways therefore form a chain along which data can be shared from any point in the chain to any other. However, the ability to do so is limited by the willingness of all parties along the chain to cooperate, and whether they are all operational at the time data is to be shared, and whether they are willing to propagate the data with the flow of goods or otherwise identify the next adjacent trading partner in response to a query.
- **Originating Party Service Lookup:** In some cases, an end user may wish to share data with the party that originates a given entity, such as the brand owner of a trade item. Originating Party Service Lookup refers to methods by which any value network party can find and initiate data sharing with the originating party.
- **Identifier resolution:** The concept of Identifier resolution is the ability to connect or redirect a GS1 identification key to one or more Web resources that provide information and/or services related to the entity identified by the GS1 identification key.
- **Event Data Discovery:** In some cases, an end user may wish to advertise the availability data to all parties that have interacted with or otherwise have an interest in a given entity throughout its lifetime in the value network. For example, in "tracking" goods through the value network it is useful to obtain observations made by all parties that handled the goods to form a complete picture of what happened. Event Data Discovery refers to finding the complete set of value network parties that have relevant data, though that introduces related problems of trust and access control.

Originating Party Service Lookup, Identifier Resolution and Event Data Discovery require additional services beyond the bilateral relationships between trading partners, and those services may be supported by GS1 standards. The following sections explain this in more detail.

6.3.1 Originating Party Service Lookup

The GS1 Digital Link standard specifies not only a Web URI syntax for GS1 identifiers but also a resolver / resolution capability for linking a GS1 Digital Link URI to one or more sources of relevant information and services. Resolvers for GS1 Digital Link typically redirect to one of those services, depending on the value of the link type specified by the client or the default link specified within the resolver records. Any party may operate a resolver for GS1 Digital Link and one resolver may redirect to another

GS1 operates a global root resolver for GS1 Digital Link at hostname `id.gs1.org`. This resolver has a special policy that only permits the respective licensee of the GS1 identifier to configure redirection records for that identifier. In some cases, the GS1 global root resolver redirects requests for a particular GS1 prefix to the corresponding national GS1 member organisation, if they also operate a resolver for GS1 Digital Link.

The GS1 global root resolver also acts as a 'resolver of last resort' to support resolution of GS1 Digital Link URIs in canonical or reference format. This is useful in situations where the AIDC data carrier encodes element strings and the GS1 Digital Link URI is obtained by translation, rather than being read directly from the AIDC data carrier.

Before GS1 Digital Link resolver infrastructure was standardised and operational, GS1 previously standardised and operated the Object Name Service, which had more limited capabilities and did not handle redirection natively via HTTP(S) redirection.

GS1 no longer operates an Object Name Service globally, and although its standard has not yet been deprecated or withdrawn, it is no longer maintained and the infrastructure for ONS is no longer supported by GS1 GO.

6.3.2 Identifier Resolution

A Resolver for GS1 Digital Link URIs connects a GS1-identified item to one or more online resources that are directly related to it. The item may be identified at any level of granularity, and the resources may be either human or machine readable. Examples include product information pages, instruction manuals, patient leaflets, clinical data, product data, service APIs, marketing experiences and more. By adhering to a common protocol based on existing GS1 identifiers and existing Web technologies, each conformant GS1 resolver is part of a coherent yet distributed network of information resources.

6.3.3 Event Data Discovery

Event Data Discovery refers to the challenge of finding all relevant source of visibility event data (traceability data) for an individual product instance / shipment at each stage of its journey through a supply chain network or value network.

Because of commercial sensitivities, companies are reluctant to share traceability data with parties beyond their immediate 1-up/1-down trading partners except on a need-to-know / right-to-know basis. As a list of links or proof of connectedness can be commercially sensitive, we need mechanisms that enable it to be prepared, shared and used/navigated in a way that does not enable harvesting of commercially sensitive business intelligence.

A viable prototype algorithm is now in development, which will enable a machine-interpretable cryptographic 'proof of connectedness' to be used to enable data sharing beyond 1-up / 1-down immediate trading partners, allowing each querying party to prove their 'connectedness' for any product instance or shipment mentioned in their query.

6.4 Worldwide federation

A fundamental architecture principle of the GS1 system is that each end user retains control over the data it originates. However, certain types of data are logically aggregated across many different end users. An example is master data in the Global Data Synchronisation Network, where each end user can synchronise master data for trade items identified by their Global Trade Identification Number (GTIN), regardless of the originator.

The most straightforward implementation of a global information resource of this kind is a single database maintained by some central authority. However, a single, centralised database has several drawbacks:

- **Scalability:** A single database must be large enough to accommodate the aggregate volume of data and queries across the world.
- **Local Preferences:** In different countries there may be different regulatory requirements as well as cultural preferences for critical services of this kind.
- **National Sovereignty:** To the extent that each nation views services of this kind as an essential part of its business infrastructure, it may be uncomfortable with a centralised service hosted by another nation.

In contrast, a federated approach has the following properties:

- Data distributed among multiple repositories, using the GS1 identification key as the basis for distribution.

In GDSN, this is realised through the existence of multiple certified GDSN Data Pools, each of which is the "home" repository for the master data associated with a subset of GS1 identification keys.

GS1 Resolvers can be set up by any party and are thus part of a federation, especially if they redirect to each other as appropriate to answer a given query.

- Data may be replicated among repositories so that the failure of one repository does not affect users of others.

In GDSN, this is realised through synchronisation of data pools so that all data pools receive copies of the master data for all GS1 identification keys, regardless of where the data originated.

In the GS1 Registry Platform, this is realised through multiple redundant servers.

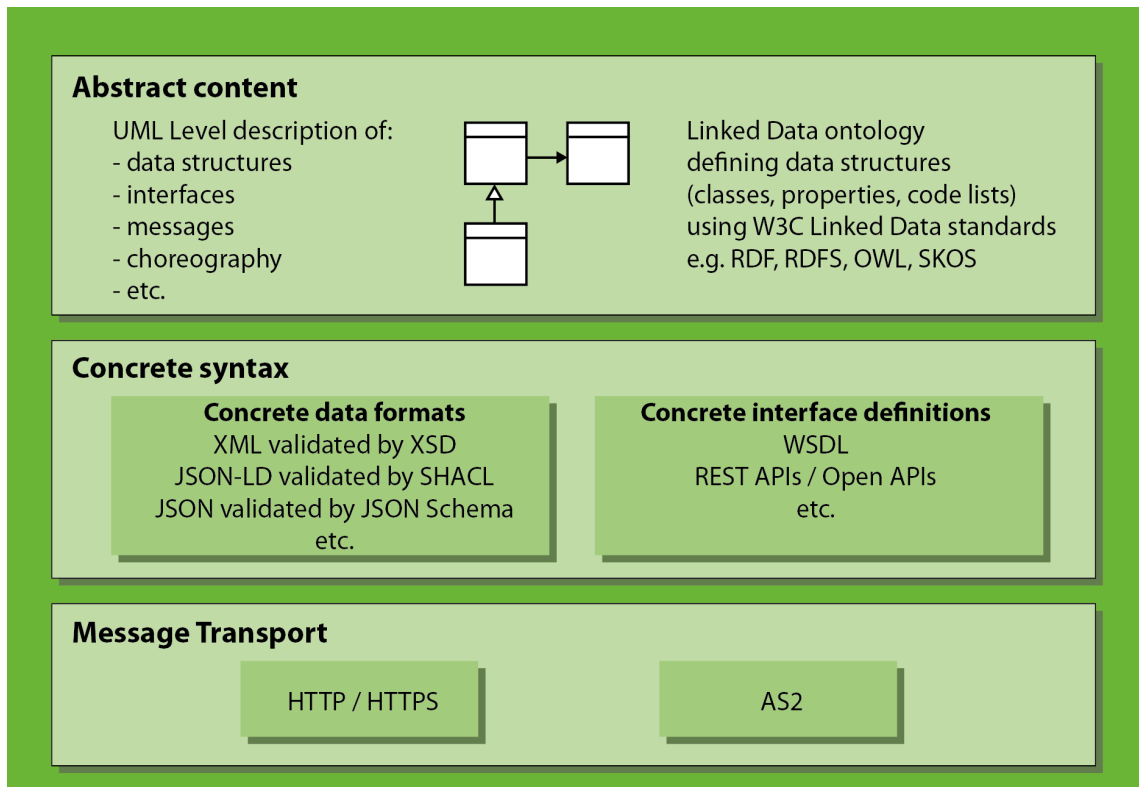
6.5 Layering of interface standards – Content vs. Syntax vs. Transport

GS1 standards that define interfaces facilitate interoperability between different system components deployed by end users. They are typically specified in three layers. All standards in the Share layer, as well as some infrastructure standards in the Capture layer, are designed in this way.

- **Abstract content:** This is the primary layer of an interface specification. In this layer, the roles that interact via the interface are defined, along with their specific interactions. Abstract content is often specified in GS1 standards using the Unified Modelling Language (UML). There is increasing interest in defining our semantic data models in a way that is independent of concrete syntax. In addition to the visual approach of UML, W3C Linked Data standards such as RDF, RDFS, OWL and SKOS are also relevant for such semantic modelling. The [Semantic Data Modelling Technical Bulletin](#) provides a primer on these and how they relate to UML class diagrams.
- **Concrete syntax:** In this layer, the concrete syntax for the representation of data defined in the abstract content layer is specified. Many standards provide a single concrete syntax definition, but some standards may provide two or more alternative concrete syntaxes for the same abstract syntax. An example is the coexistence of GS1 XML and GS1 EANCOM syntax for GS1 EDI or the coexistence of JSON/JSON-LD and XML data bindings in the forthcoming new version of EPCIS (v2.0).
- **Message transport:** In this layer, the means for delivering a message having a concrete syntax from one side of the interface to another is specified. Message transport is the area where there is the most variety in the technical choices that can be negotiated between the parties. The layered structure ensures, however, that regardless of the choice of message transport the content of the messages may have the same syntax, and in all cases have the same meaning.

These layers are illustrated in [Figure 6-2](#) (in this figure, the specific technologies mentioned are illustrative only; a given standard may specify a different set of options):

Figure 6-2 Typical GS1 interface standard



7 GS1 Data Services

“GS1 Data Services” is an umbrella term for services that are defined by the GS1 federation for the ultimate benefit of the users of the GS1 system. Most of the services are provided by GS1 Global Office (GO), but in some cases, GS1 Member Organisations (MOs) are free to provide their own versions of the services as long as they are certified as being equivalent to those provided by GO. Furthermore, MOs are free to enhance the services provided by GO by supplementing them with additional features, as long as the core capabilities are still available to their users. Each GS1 Data Service is available globally and with consistent functionality (as viewed by the intended users of the service) around the world.

There exists a subset of GS1 Data Services that have, as their direct customers, only GS1 MOs. Some of these are mandatory to be implemented by all GS1 MOs. These are referred to as Core Data Services, as shown in [Figure 7-1](#). Additionally, there are:

- SaaS Component Services that are available for optional use by GS1 MOs so that they may implement their own versions of some services.
- Value-Added Services that are not necessarily offered globally and are not coordinated by GS1 globally. As such, value-added services are out of scope for this architecture document.

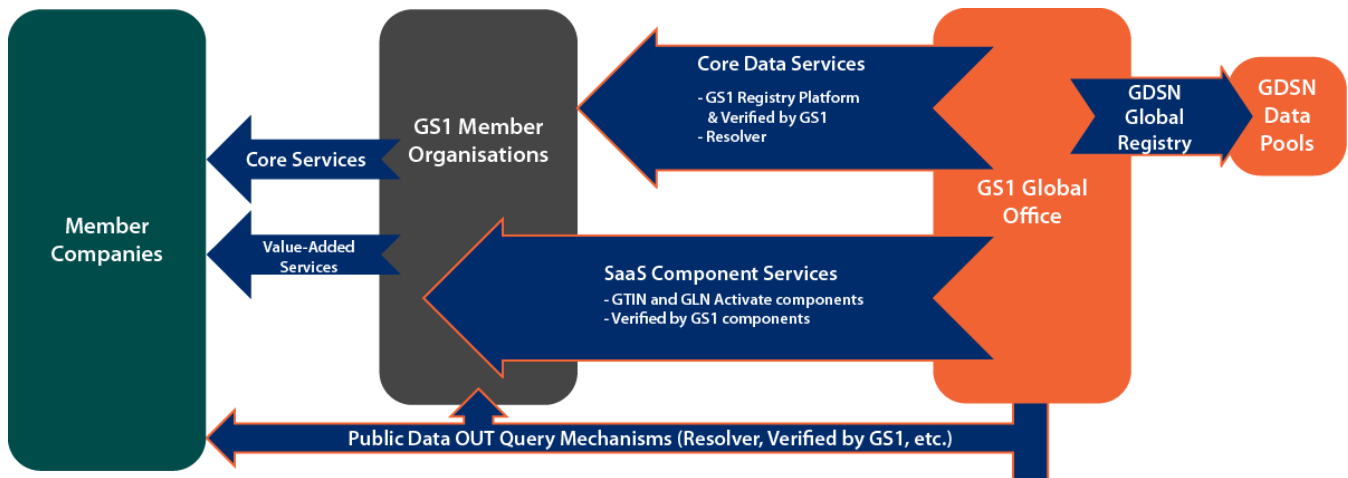
GS1 also offers a number of public data access mechanisms, including the GS1 Resolver service, and the Verified by GS1 public query service.

GS1 maintains and provides access to Data Services Resources that include the EPCIS Libraries and various software development kits (SDKs).

Lastly, GS1 maintains the GS1 Global Registry™, which is a single-function registry that is used solely within and across the Global Data Synchronisation Network (GDSN) Data Pools. It is considered a Core Data Service for GDSN.

These GS1 Data Services are illustrated in [Figure 7-1](#), which is intended to convey only the provision of a service (and does not represent the data flows back and forth for any particular service).

Figure 7-1 GS1 Data Services breakdown



GS1 Global Office builds services on a series of foundational principles that ensure fitness for use by the GS1 Federation to serve industry:

- 1. Be user-centric:** GS1 Data Services are designed to support business processes and use cases, focused on trading partner needs and providers of business value.
- 2. GS1 identification keys and standards as the foundation:** GS1 Data Services are based on the foundation of the GS1 identification keys and associated basic master data. The formats of data stored in and shared by the services are compliant with the GS1 standards for data exchange and validation.
- 3. Security:** GS1 Data Services are provided with appropriate physical, logical and commercial security (access control, authentication, non-repudiation and so on).
- 4. Data quality and integrity:** Data quality is core to the design of all GS1 Data Services and supporting programs.
- 5. Regulatory compliance:** The aim is to provide a framework that GS1 Member Organisations can draw on to help with local and regional regulatory compliance.
- 6. Service availability:** GS1 Data Services should be available globally, at all times (24x7x365), and should be accessible and supportable to meet the needs of the industries that GS1 serves.
- 7. Extensible and backward-compatible system:** Extensibility and agility are necessary for all GS1 Data Services to adapt to new technologies, to enable more efficient business processes and to expand the user community.

7.1 Services offered by GS1 Global Office to GS1 Member Organisations

7.1.1 Core Data Services

Core Data Services are the GO-developed, mandatory services that are accessible by GS1 MOs and that serve as elements of an IT infrastructure to partially enable MO provision of Core Services to their member companies.

7.1.1.1 GS1 Registry Platform and Verified by GS1

In 2019, GS1 agreed to develop a global registry platform to store GS1 Company Prefix and single-issue GS1 identification key licences (Licence Registry) and only a minimal, thin set of basic master data elements related to GS1 identification keys. These scalable, global, thin GS1 identification key registries are accessed by MOs only through a standard framework of APIs that enable GS1 MOs to get data IN and OUT. In June 2023, this work was completed as planned, resulting in a Licence Registry, a GTIN Registry, a GLN Registry and a Links Registry. Together, these services make it

possible for MOs to offer the Verified by GS1 service. Additional GS1 identification key registries may be added in accordance with industry priority.

The GS1 Registry Platform also includes a Data Analytics environment for GS1 MOs that enables dashboarding and reporting on usage of the platform and about data quality and completeness.

7.1.1.2 Resolver

The GS1 Global Office (GO) Resolver service (<https://www.gs1.org/standards/gs1-resolver-service>), while technically integrated into the GS1 Registry Platform infrastructure, is a standalone service that allows MOs to offer their members the ability to link their identifiers at any level of granularity, to one or more sources of information, as defined in the GS1-Conformant Resolver Standard.

Moreover, the GS1 GO Resolver can enable the redirection of GS1 Digital Link requests to GS1 MO-operated Resolvers, based on their respective GS1 prefixes. In such a case, all incoming requests to id.gs1.org are immediately forwarded to the resolver of the respective GS1 MO which granted the underlying licence of the respective GS1 Identification Key. The GS1 GO Resolver service significantly increases the value of the GS1 system of identifiers. It means that GTINs (+CPV, batch/lot, and/or serial if applicable), GLNs, SSCCs, GRAIs and more, can act as gateways to multiple sources of information for business partners and consumers. The possibilities are endless: linking a food product to traceability and allergen information, linking an asset to its service history, linking a pharmaceutical to information for patients on the one hand and for clinicians on the other, and much more are possible. With the GS1 GO Resolver service, each barcode and/or EPC/RFID tag can perform multiple functions, eliminating the need to add new codes to an item every time there is a new use case.



Note: As defined by the GS1-Conformant Resolver Standard, the dedicated link type <https://ref.gs1.org/voc/handledBy> is used to configure redirections from one resolver to another, which enables incoming requests to be forwarded to and handled by the required resolver.

7.1.2 SaaS Component Services

GS1 Global Office has developed and maintains global service components that enables GS1 MOs to create keys and register them into the GS1 Registry Platform with the required attributes (GTIN and GLN Activate components). These components enable simple integration of the necessary APIs into their existing systems.

Additionally, Global Verified by GS1 component is a web-based application/tool that provides MOs with a user interface that enables them to offer Verified by GS1 to their member companies.

7.2 Services offered by GS1 Global Office to Public

7.2.1 Verified by GS1 on [gs1.org](https://www.gs1.org)

GS1 Global Office offers public access to Verified by GS1 at <https://www.gs1.org/verified-by-gs1>. Users can query:

- GTIN and GLNs to receive licence and key information
- All other GS1 keys and company name to receive licence information

The service is limited to 30 queries per day per IP address to avoid web-scraping of the GRP data.

7.2.2 GS1 Resolver Query Service

GS1 provides an unrestricted public query service for the GS1 Resolver. Users may query the service for any links provided for a GS1 Digital Link URI.

7.3 Standards Support Resources offered by GS1 Global Office to Public

GS1 offers a portfolio of support resources to make adoption of GS1 standards easier.

7.3.1 Global Product Classification (GPC) Browser

The Global Product Classification (GPC) is a standardised classification system (<https://www.gs1.org/services/gpc-browser>) that gives buyers and sellers a common language for grouping products in the same way, everywhere in the world. The official (normative) GPC schema and corresponding GPC Browser is published in Oxford English, and both the schema and the Browser are translated to other languages. The GPC Browser allows an end user to browse all components (Segment, Family, Class, Brick and Attribute) of the latest GPC schema and that supported by GDSN (which may be older).

7.3.2 GS1 Navigator

The GS1 Navigator (<https://navigator.gs1.org>) enables users to explore GS1 data standards on the web, enabling search across the GS1 Global Data Model (GDM), GS1 Global Data Synchronisation Network (GDSN), EDI, Global Product Classification (GPC) and GS1 Web Vocabulary specifically or across all standards.

7.3.3 Check Digit and Check Character Pair Calculator

The Check Digit Calculator (<https://www.gs1.org/services/check-digit-calculator>) is available to the public as most GS1 identification keys need a check digit. After entering the GS1 identification keys' numeric value, a check digit is automatically and accurately calculated to ensure the integrity of the GS1 identification key. A Check Character Pair Calculator (<https://www.gs1.org/services/check-character-calculator>) is also available to generate or validate a Global Model Number (GMN) or Highly Individualised Device Registration Identifier (HIDRI), based on the GS1 Company Prefix and an internal number or model reference.

7.3.4 GS1 GitHub Site

GS1 maintains a GitHub site (<https://github.com/gs1>) with source code examples for solution providers and other third-party developers to create products based on the GS1 system of standards. This code library is available for anyone to create proofs of concept or to integrate into their solutions based on the standards. Public repositories at this time include code for the GS1 Digital Link standard, EPCIS, Tag Data Translations (TDT), the GS1 Barcode Syntax Dictionary and Tests, and the GS1 Barcode Syntax Engine.

7.3.5 Tools for EPC and EPCIS

The set of EPC and EPCIS tools allow third parties to make use of and build on the GS1 EPC family of standards.

7.3.5.1 EPC Encoder/Decoder

<https://www.gs1.org/services/epc-encoderdecoder>

This web interface translates between different forms of the Electronic Product Code (EPC), in compliance with [GS1's EPC Tag Data Standard \(TDS\) 1.13](#).

Note that this is a **legacy tool** which is no longer maintained, and which will be **superseded by the TDS 2.x Encoder/Decoder**.

7.3.5.2 TDS 2.x Encoder/Decoder

Coming in late 2024 to <https://ref.gs1.org/tools/> and <https://github.com/gs1>

This tool consists of a web interface demo based on an open-source JavaScript encoder/decoder library, utilising TDT 2.x translation files.

This demo will facilitate translation between GS1 formats (e.g., GS1 Element String and GS1 Digital Link URI) and all new (TDS 2.x) and legacy (TDS 1.x) EPC schemes, with auto-detection of input/output format. It will also feature determination of optimal encoding method for variable-length alphanumeric fields (e.g., for Serial Number, Lot/Batch number, etc.), as well as encoding/decoding of optional "+AIDC data" encoded in EPC Memory after the new TDS 2.x EPC schemes.

7.3.5.3 EPCIS Workbench

<https://epcisworkbench.gs1.org/>

This is a free, web-based tool for working with the GS1 EPCIS standard.

Note that this is a **legacy tool** which is no longer maintained, and which has **been superseded by the EPCIS Sandbox**.

7.3.5.4 EPCIS Sandbox

<https://epcis-sandbox.gs1.org/>

This is a free, web-based tool intended to raise EPCIS 2.0 awareness and promote best practice.

Its evolving feature set currently incorporates an Event Data Generator and Viewer, including validation of uploaded XML or JSON-LD EPCIS files. The tool's Format Converter allows for translation between EPCIS and CBV versions (1.2 and 2.x), EPCIS Syntax (XML and JSON-LD), GS1 Keys (EPC URN and GS1 Digital Link URI) and EPCUS Event vocabulary (EPC URN and WebURI).

Future enhancements will include the integration of EPCIS, CBV and GS1 Web Vocabulary Ontologies in the Event Data Creator, as well as Capture and Query using the EPCIS 2.x REST API. A hosted EPCIS Repository will serve as a EPCIS 2.x-compliant successor to the legacy FREEPCIS.

7.3.5.5 EPC Translator Library

The EPC Translator Library (<https://www.gs1.org/sites/default/files/2023-10/epc-translator-brochure-20231010.pdf>) is commercial-grade licensed software designed to handle all the RFID and barcode data translation needs. It is designed for rapid integration with software development. All EPC schemes, including those defined in TDS 2.x, and their respective binary formats are supported.

7.3.5.6 FREEPCIS

<https://freepcis.gs1.org>

This is a free, limited capacity EPCIS repository for development and testing. It allows third party providers to test their systems with respect to the EPCIS 1.x Capture and Query interfaces.

Note that this is a **legacy tool** which is no longer maintained, and which has been **superseded by the EPCIS Sandbox**.

7.3.5.7 RFIDcoder

RFID encoding and decoding API services (<https://rfidcoder.gs1.org>) provide a REST API for encoding and decoding UHF Gen2 RFID tags according to the GS1 EPC Tag Data Standard up to version 1.11. While still available, this tool is no longer maintained.

7.3.6 GS1 Web Vocabulary

The GS1 Web Vocabulary (<https://www.gs1.org/voc/>) publishes terms defined in various GS1 standards and data systems, for general use following Linked Data principles. It is designed as an extension to schema.org, to enable products, organisations and locations to be described with additional details, and where relevant, mappings and relationships arising from schema.org vocabulary are made explicit. The GS1 Web Vocabulary is intended to provide easy on-demand access to structured data via simple Web requests.

7.3.7 GS1 Application Identifier Browser

This tool (<https://ref.gs1.org/ai/>) provides an easy way to view, search and share details about individual GS1 Application Identifiers through web-browsers or on a mobile device. The dataset for the tool is also provided in JSON-LD.

7.3.8 GS1 Barcode Syntax Resource (BSR)

The GS1 Barcode Syntax Resource (<https://www.gs1.org/standards/gs1-barcodes/gs1-barcode-syntax-resource>) is a software library that helps solution providers implement and stay updated with GS1 standards easily and consistently. Developed and maintained in GitHub under two public repositories as noted above in Section 7.3.4, the BSR is based on the core conformance requirements for GS1 barcode syntaxes and GS1 Application Identifiers, as defined by the GS1 General Specifications and GS1 Digital Link standard: URI syntax. Consisting of the following three components, the BSR can be integrated directly to an application's code base or simply used as an implementation reference, as required by the solution:

GS1 Barcode Syntax Dictionary

A simple text file that lists all currently assigned GS1 Application Identifiers (AI) and the components required to form a valid GS1 barcode syntax.

GS1 Barcode Syntax Tests

A set of source code files, known as reference linters, that provides instructions to perform a series of analytical actions to check if data, whether input by a keyboard or barcode scanner, is valid against GS1 conformance specifications and rules for the GS1 barcode syntax.

GS1 Barcode Syntax Engine

An example of the harmonised framework required to implement the GS1 Barcode Syntax Dictionary and GS1 Barcode Syntax Tests, to facilitate the detection of common data errors and the consistent interpretation and conversion of GS1 syntaxes. Includes demonstration applications for various operating systems and environments, to showcase the functionality of the BSR.

7.3.9 GS1 TraceWay

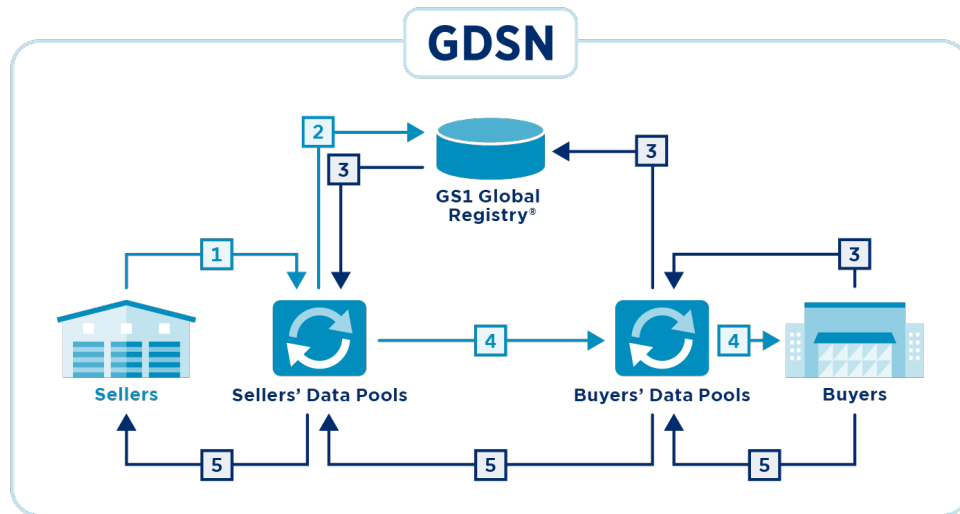
GS1 TraceWay (<https://www.gs1.org/standards/traceability/traceway>) is an online methodology to implement interoperable traceability systems across supply chains. It provides essential information and questions to be addressed during the diagnosis, design and deployment phases. Within the tool, you can explore key steps in each phase, their respective outputs, applicable GS1 standards, actions to be performed, benefits, tips and resources. Its added value extends beyond the use of GS1 systems, encompassing common business and regulatory traceability requirements.

7.4 Services offered for the GDSN

The GS1 Global Data Synchronisation Network (GDSN) is a network of interoperable data pools enabling the collaboration of users to securely synchronise master data based on GS1 standards. GDSN supports accurate, trade item updates among subscribed trading partners. This network relies on a central registry called the GS1 Global Registry™, which is developed and maintained by GS1 Global Office.

For more information visit <https://www.gs1.org/services/gdsn>.

Figure 7-2 How GDSN works



- 1. Loading of company data
- 2. Registering of company data
- 3. Subscription to seller's data pool
- 4. Publishing of company data
- 5. Confirmation receipt of company data

8 Glossary

The glossary lists the terms and definitions that are applied in this document. These definitions may not align across various GS1 standards however the Architecture Group will work to promote harmonisation wherever possible. Please refer to the www.gs1.org/glossary for the online version.

Term	Definition
abstract content (standards layer)	The layer of an Interface Standard that specifies the interactions that occur over the interface, including the abstract structure, meaning, and interaction patterns, but not including concrete syntax or transport.
AIDC	See <i>Automatic Identification and Data Capture</i>
AIDC carrier data	Data contained in a barcode or tag that describes the data carrier itself, as opposed to the entity to which the data carrier is affixed (e.g., symbology start pattern).
AIDC control data	Data contained in a barcode or tag that is used to by the Data Capture Application to control the interaction with the data carrier (e.g., filter bits in EPC RFID tags).
AIDC data	Data associated with AIDC data carriers that provide business information about an entity such as a use by date or its weight.
AIDC data carrier	Generic term for a barcode or RFID Tag; a means of physically affixing machine-readable data to a physical entity.
ALE	See <i>Application Level Events</i>
application area	A use case where some component of the GS1 system is used (e.g., for traceability, patient safety, last mile, eProcurement, consumer engagement).
Application Level Events (ALE)	A GS1 standard interface between a Data Capture Application and one or more Radio-Frequency Identification (RFID) Interrogators (readers).
attribute	See data element.
attribution	The act of associating a specific data element with a specific entity.
automatic identification and data capture (AIDC)	A technology used to automatically capture data. AIDC technologies include barcodes, smart cards, biometrics and RFID.

Term	Definition
<i>Capture</i>	A category of GS1 standards, encompassing the standards that are used to capture data elements that are carried directly on physical entities, bridging the world of physical things and the world of electronic information.
carrier internal representation	The representation of data as it exists within an AIDC Data Carrier. In a barcode, this is the pattern of light and dark bars or squares. In a Radio-Frequency Identification (RFID) tag, this is the binary data stored in the digital memory of the RFID chip.
closed value network	A value network consisting of a fixed universe of trading partners, all of whom are known in advance.
commissioning	The act of associating a specific identifier value with a specific entity.
compound key	Two or more data elements which together serve as a key, where no subset of those data elements taken by themselves would do so (also see simple key).
concrete syntax (standards layer)	The layer of an Interface Standard which specifies a specific syntax that realises the abstract data structures defined in the Abstract Content layer.
conformant	The state in which a system meets a specified standard.
data capture application	Software responsible for interacting directly with AIDC Data Carriers, and coordinating this interaction with the enclosing business process.
data carrier	See <i>AIDC Data Carrier</i>
data discovery	A future GS1 standardisation effort intended to provide a means for a value network party to locate all sources of data within the value network that meet specified criteria.
data element	One piece of information (descriptive data element) or one identification component (identification data element) associated with a specific thing, transaction, or event. A data element may be recognised if one can construct a sentence of the following form: "The [data element name] of [entity] is [data element value]."
data element definition	Description of the meaning and purpose (semantics) for the data element.
data element encoding	A data element value may be encoded in a particular format depending on where it is stored or expressed (e.g., as a binary string in an RFID tag, in a particular format e.g. 6-digit YYMMDD in a barcode, as an xsd:date format within an XML / JSON message or data structure, all of these having potentially the same meaning but different encodings for different purposes)
data element field	The data location (e.g. within a document or message or dataset) where a data element value is encoded, stored, queried, or transmitted.
data element field name	The name of a property/attribute within a data structure or message or event (e.g., 'eventTime' within an EPCIS event, gs1:expirationDate within the GS1 Web vocabulary)
data element qualifier	Characters, within AIDC, that designate the meaning of the data element (e.g., Application Identifier, data title).
data element syntax	Description of the character set of, format, and length.
data element value	The actual characters used to create a data element (e.g., ABC123, 220708, 117 Hopkins Street).
data standard	A type of GS1 standard that defines the syntax and semantics of data.
DCI	See <i>RFID Discovery, Configuration, and Initialisation Interface</i>
dynamic data	A data element whose value changes frequently over the life of the entity (e.g., the price of a product).

Term	Definition
Electronic Product Code Uniform Resource Identifier (EPC URI)	A uniform syntax for tier 1, tier 2, and tier 3 keys that identify specific physical or digital objects, based on Internet Uniform Resource Identifier (URI) syntax.
end user	An organisation that employs the GS1 system as a part of its business operations.
entity	Within data modelling or identification, something that can be identified or described with data (e.g., trade item, assets, business process, patient record, location, organisation).
EPC URI	See <i>Electronic Product Code Uniform Resource Identifier</i>
event data	A record of a change in the state of an object.
Global Data Dictionary (GDD)	A compendium of the data elements defined across all GS1 standards. The GDD is not itself a GS1 standard, but rather is a tool which helps to ensure consistency across all GS1 standards. The GDD has been discontinued and replaced with the GS1 Navigator.
Global Standards Management Process (GSMP)	The GS1 community based, global consensus process for creating GS1 standards, GS1 guidelines and collateral that are based on business needs and user-input.
GS1 application standard	A type of GS1 standard that specifies the scope as well as a set of technical standards and establishes rules for their use in a particular application area, potentially including choreography of data exchanges.
GS1 data service	GS1 standards-based application offered to Industry to address a specific business need.
GS1 element string	A syntax for representing one or more data elements, including GS1 identification keys and AIDC data, that is used in barcodes.
GS1 guideline	Best practice document which provides information considered useful in implementing one or more GS1 standards, developed with a balance of stakeholders represented via transparent due process (Global Standards Management Process) and which never introduces, modifies or removes normative content beyond the standard(s) to which it refers.
GS1 identification key	A unique identifier for a class of entities (e.g. a trade item) or an instance of an entity (e.g. a logistic unit) as defined by GS1 standards.
GS1 identification key tiers	A categorisation of identification keys, used as primary identifiers, drawn from a GS1 perspective, that clarifies the relationship between various identification keys, defined by GS1 and others, and the GS1 system.
GS1 identification key types	Various areas of entity identification for which GS1 has defined GS1 identification keys and established rules for their allocation (e.g., trade items, logistic units, locations, parties, assets, documents, service relations).
GS1 Navigator	A repository of data elements defined across GS1 data standards including GS1 Global Data Model (GDM), GS1 Global Data Synchronisation Network (GDSN), EDI, Global Product Classification (GPC) and GS1 Web Vocabulary. The GS1 Navigator is not a GS1 standard, but rather a tool which enables users to search for data elements within a specific GS1 data standard, or across all standards.
GS1 solution	GS1 offering to Industry that combines GS1 standards, services, guidelines, and/or other activities to address a specific business need.
GS1 standard	One or more documents that (a) provide normative specifications and rules developed with a balance of stakeholders represented via transparent due process (Global Standards Management Process) and (b) establish conformance requirements for the structure, meaning, and mechanism of data exchange between parties to facilitate efficiency and interoperability in open value networks.

Term	Definition
GS1 standards artefact	Something that is primarily a machine-readable document or data resource (e.g., executable code, or an ontology file in JSON-LD) but is the source of a normative agreement subject to conformance.
GS1 standards-based artefact	Something that is primarily a machine-readable document or data resource (e.g., check digit calculator), is not the source of a normative agreement subject to conformance but claims to be in conformance with GS1 standards.
GS1 syntax	A data structure used within the GS1 system of standards for representing data elements. GS1 syntaxes include plain syntax, GS1 element string, GS1 Digital Link URI, and Electronic Product Code (EPC) URI.
GS1 system	The sum of all the artefacts created by the GS1 community through GS1's community development processes, including GS1 standards, GS1 guidelines, GS1 solutions, and GS1 data services.
GS1 technical standard	A type of GS1 standard which defines a normative set of behaviours of system components such as the definition of data models, rules and interfaces.
GS1 tier 1 key	A key defined, administered, and managed entirely by GS1.
GS1 tier 2 key	A key whose structure is defined by GS1 as a GS1 tier 1 key, but that is otherwise defined, administered, and managed by an external organisation.
GS1 tier 3 key	A key defined, administered, and managed entirely by an organisation external to GS1, but which is explicitly supported in some parts of the GS1 system.
GS1 tier 4 key	A key defined, administered, and managed entirely by an organisation external to GS1, and which is not explicitly supported in any part of the GS1 system.
GS1 Web Vocabulary	A list of concepts, classes (types of thing) and properties or predicates (relationships, attributes), together with their definitions.
GSMP	See <i>Global Standards Management Process</i>
identification key	One or more data elements for an entity that serve to uniquely identify that entity. An information system uses an identification key as a proxy for the entity itself.
identification key - class level	An identifier of entities which share common characteristics (e.g., all cans of tomato basil soup, 0.5L, no salt added).
identification key - instance level	An identifier on an individual entity (e.g., one can of tomato soup).
<i>Identify</i>	A category of GS1 standard, encompassing the standards that define unique identification codes which may be used by an information system to refer unambiguously to an entity.
interface standard	A type of GS1 standard that defines an interaction between system components, often by defining the syntax and semantics of messages that are exchanged between system components.
key	One or more data elements associated with an entity that serves to uniquely identify that entity, within some specified application.
Low-Level Reader Protocol (LLRP)	A GS1 standard interface to a single Radio-Frequency Identification (RFID) device.
master data	Data elements associated with an entity that are static (unchanging through the life of the entity) or nearly so.
Message Transport (standards layer)	The layer of an Interface Standard that specifies the means for delivering a message from one side of the interface to the other.
Object Name Service (ONS)	A GS1 standard for a service that provides a lightweight facility to identify services associated with a GS1 identification key that are registered by the party that originated the key.

Term	Definition
OID/value pair	The combination of an Object Identifier as specified in ISO/IEC 9834 with the value of the OID for a specific object.
open value network	A value network where the complete set of trading partners is not known in advance, changes over time and where, to a certain degree, trading partners are interchangeable.
plain syntax	GS1 data structure containing GS1 identification key with no additional characters or syntactic features
Profile	A type of standard whose normative content consists exclusively of references to other standards along with normative constraints upon their use.
Reader management (RM)	A GS1 standard interface through which a monitoring application may obtain information about the health and status of a Radio-Frequency Identification (RFID) Interrogator (reader).
regular expression	A sequence of characters that specifies a search pattern that are usually used by string-searching algorithms for search / find-and-replace operations on strings or for validation of string input.
RFID Discovery, Configuration, and Initialisation Interface	A GS1 standard interface through which a Radio-Frequency Identification (RFID) Interrogator (reader) may automatically make itself known to a network, obtain configuration information, and initialise itself so that it communicates with filtering and collection or application software.
<i>Share</i>	A category of GS1 standards, encompassing the standards that facilitate the sharing of data between business applications and trading partners.
simple key	A single data element that serves as a key (also see compound key).
solution provider	An organisation that implements for end users systems that are based upon or implement the GS1 system.
state data	Data that provides a current or historic snapshot of the location or condition of an object.
static data	A data element whose value does not change over the life of the entity (e.g., the load capacity of a specific forklift).
symbology identifier	A 3-character piece of Control Information used in barcode interface standards to identify which type of barcode symbol is read.
transaction data	Business documents that are shared bilaterally between trading partners, each document serving to automate a step in a business process involving a business transaction between parties.
transfer encoding	The representation of data used in the interface between a Data Capture Application and the hardware device that interacts with the AIDC Data Carrier (barcode scanner or Radio-Frequency Identification (RFID) Interrogator).
unique GS1 identification	A given GS1 identification key type value corresponds to one and only one entity within all specified application areas for its lifecycle; two different entities within all specified application areas must have different values for each GS1 identification key type for its lifecycle. This applies to class and instance level identification.
value network	A set of parties who are involved in business relationships with one another.
visibility data	Data consisting of event data and state data.

9 References

The various links and references contained in Annex A (Summary of GS1 standards: Identify, Capture & Share) and B (Summary of GS1 application standards & solutions) of the previous version of this *GS1 System Architecture* can be found at:

- <https://www.gs1.org/standards/log>
- <https://www.gs1.org/standards/how-gs1-standards-work>