GS1 System Architecture Document

How GS1 standards fit together

Release 5.0, Approved, Apr 2016

Document Summary

Document Item	Current Value
Document Name	GS1 System Architecture Document
Document Date	Apr 2016
Document Version	5.0
Document Issue	
Document Status	Approved
Document Description	How GS1 standards fit together

Contributors

Name	Organisation
Henri Barthel, GS1 AG co-Chair	GS1 GO
John Duker, GS1 AG co-Chair (past)	Procter & Gamble
Vera Feuerstein, GS1 AG co-Chair	Nestle
Sue Schmid, GS1 AG co-Chair	GS1 Australia
Ken Traub, Editor	Ken Traub Consulting LLC
Robert Abate	Walmart
Xavier Barras	GS1 France
David Buckley	GS1 GO
Kevin Dean	GS1 Canada
Andreas Füßler	GS1 Germany
Pierre Georget	GS1 France
Hein Gorter de Vries	GS1 Nederland
Mark Harrison	Auto-ID Labs, Cambridge
Fred Kempkes	Unilever
Jens Kungl	Metro Group
Sean Lockhead	GS1 GO
Roberto Matsubayashi	GS1 Brasil
Paul Michicich	Kraft Foods, Inc.
Staffan Olsson	GS1 Sweden
Andrew Osborne	GS1 UK
Kunle Oye-Igbemo	GS1 Nigeria
Josef Preishuber-Pflügl	CISC Semiconductor
Pere Rosell	GS1 Spain
Eugen Sehorz	GS1 Austria
KK Suen	GS1 Hong Kong
John Terwilliger	Abbott Laboratories
Junyu Wang	Auto-ID Labs, Fudan

Name	Organisation
Tony Zhang	FSE

Log of Changes

Release	Date of Change	Changed By	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

Disclaimer

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

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

THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGMENT, FITNESS FOR PARTICULAR PURPOSE, OR ANY WARRANTY OTHER WISE ARISING OUT OF THIS SPECIFICATION. GS1 disclaims all liability for any damages arising from use or misuse of this Standard, whether special, indirect, consequential, or compensatory damages, and including liability for infringement of any intellectual property rights, relating to use of information in or reliance upon this document.

GS1 retains the right to make changes to this document at any time, without notice. GS1 makes no warranty for the use of this document and assumes no responsibility for any errors which may appear in the document, nor does it make a commitment to update the information contained herein.

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

Table of Contents

1 Introduction

This document defines and describes the *GS1 System Architecture*. GS1 is an international not-for-profit association with Member Organisations in over 100 countries. GS1 is dedicated to the design and implementation of global standards and solutions to improve the efficiency and visibility of supply and demand chains globally and across sectors. The "GS1 System" is the collection of standards, guidelines, solutions, and services created by the GS1 community through GS1's community development processes, and is the most widely used supply chain standards system in the world.

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. For the purpose of this document, an end user is any organisation that employs the GS1 system as a part of its business operations. A solution provider is an organisation that implements for end users systems that are based upon or implement the GS1 system. GS1 standards are available for use by any party.

This document has several aims:

- To enumerate, at a high level, each of the hardware, software, and data standards that are part of the GS1 system and to show how they are related. These standards are implemented by hardware and software systems, including components deployed by individual end users as well as GS1 services deployed by GS1, its delegates, and others.
- To explain the underlying technical foundations that have guided the design of individual standards and service components within the GS1 system. These underlying foundations provide unity across all elements of the GS1 system and provide guidance for the development of future standards and new services.
- To provide architectural guidance to end users and solution providers seeking to implement GS1 standards and to use GS1 services, and to set expectations as to how these elements will function.
- To define the top-level architecture of GS1 services, which provide common services to all end users, through interfaces defined as part of the GS1 system.

This document exists only to describe the overall architecture, showing how the different components fit together to form a cohesive whole. Other documents to provide the technical detail required to implement any part of the GS1 system. Specifically:

- Individual hardware, software, and data interfaces, as well as their use in open supply chain application contexts, are defined normatively by GS1 standards, or by standards produced by other standards bodies and referenced by GS1 standards. GS1 standards are developed by the GS1 Community through the Global Standards Management Process (GSMP). GS1 standards are normative and implementations of some GS1 standards are subject to conformance and certification requirements.

  An example of an interface (a hardware interface, in this case) is the UHF Class 1 Gen 2 Tag Air Interface, which specifies a radio-frequency communications protocol by which a Radio Frequency Identification (RFID) tag and an RFID reader device may interact. This interface is defined normatively by the UHF Class 1 Gen 2 Tag Air Interface Standard.
- The design of hardware and software components that implement GS1 standards are proprietary to the solution providers and end users that create such components. While GS1 standards provide normative guidance as to the behaviour of interfaces between components, implementers are free to innovate in the design of components so long as they correctly implement the interface standards.

  An example of a component is an RFID tag that is the product of a specific tag manufacturer. This tag may comply with the UHF Class 1 Gen 2 Tag Air Interface Standard; even if it does, the specific implementation embodied in the design of the chip and its supporting software is not part of the *GS1 System Architecture*.
- A special case of components that implement GS1 standards are shared network services that are operated and deployed by GS1 itself, by other organisations to which GS1 delegates responsibility, or by other third parties. These components are referred to as GS1 Network-based Services, and provide services to all end users.

An example of a GS1 Network Service is the GS1 Global Registry, which provides a registry through which a GS1 identification key may be associated with one or more Global Data Synchronisation Network Data Pools. The Global Registry is logically operated by GS1; from a deployment perspective this responsibility is delegated to a service provider contractor of GS1 that operates the servers and database that comprise the Global Registry.

At any moment in time, there are many parts of the GS1 system that are well established and for which GS1 standards already exist. There are other parts of the GS1 system that are undergoing evolution and enhancement, to meet needs that are determined based on the analysis of known use cases. In these cases, the architectural approach may not yet been finalised, though architectural analysis may be underway within the GS1 Architecture Group. Developing standards or designing additional network services depends on the definition of a broader collection of use cases and their abstraction into general requirements. This document clearly identifies which parts of the GS1 system are well-established architecturally and which parts are the subject of future work. This document will be the basis for working through and ultimately documenting the architectural decisions around the latter parts as work continues.

This document is a companion document to the *GS1 System Landscape* document. The *GS1 System Landscape* provides a structured, complete catalogue of all GS1 standards, including a synopsis of each. The present document complements the *GS1 System Landscape* by providing an architectural view of how the components of the GS1 system fit together and the foundations that underlie the entire system. The emphasis in the present document is on elucidating these relationships, not necessarily describing each and every component. Throughout this document, the reader is referred to relevant sections of the *GS1 System Landscape* by means of the "landscape" icon as illustrated to the left of this paragraph; through these references, together with the standards themselves, the interested reader may find more detail.

2 Overview of GS1 System Architecture

The GS1 system provides the foundation for enhancing open supply chains through the use of digital information. The open nature of supply chains shapes the general orientation of GS1 standards, placing a particular emphasis on achieving interoperability through broadly accepted interface definitions. The business needs of supply chain participants determine the types of interface definitions that require standardisation, and in particular lead to a portfolio of standards that are concerned with *identification* of real-world entities (whether physical, digital, or conceptual), *capture* of identification and other data from physical objects, and *sharing* of information concerning real-world entities among the participants in the supply chain.

2.1 The role of standards

The GS1 system is primarily concerned with raising the efficiency of business processes and providing cost savings through automation based on globally unique identification and digital information. The role of GS1 standards in this area is to further the following objectives:

- *To facilitate interoperability in open supply chains*

  For supply chain trading partners to exchange information, they must have prior agreement as to the structure and meaning of data to be exchanged and the mechanisms by which exchange will be carried out. GS1 standards include data standards and information exchange standards that form the basis of cross-enterprise exchange. Likewise, for trading partners to move physical objects amongst themselves, they must have prior agreement as to how physical objects will carry identification that is mutually understandable and physically affixed using data carriers that are interoperable. GS1 standards include standards for physical data carriers (i.e., barcodes and RFID tags) and data standards governing the encoding of data on those carriers.

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

  GS1 standards define interfaces between system components that facilitate interoperability between components produced by different vendors or by different organisations' in-house development teams. This in turn provides choice to end users, both in implementing systems that will exchange information between trading partners and in those that are used entirely internally. Moreover, the existence of standards helps to avoid fragmentation in the market for system components, which leads to economies of scale that ultimate reduce costs for end users.

- *To encourage innovation*

  GS1 standards define interfaces, not implementations. Implementers are encouraged to be innovatative in the products and systems they create, while interface standards ensure interoperability between competing systems. By building upon a standard foundation, implementers can have greater confidence in the eventual adoption of their products and systems, and therefore the confidence to invest in innovation.

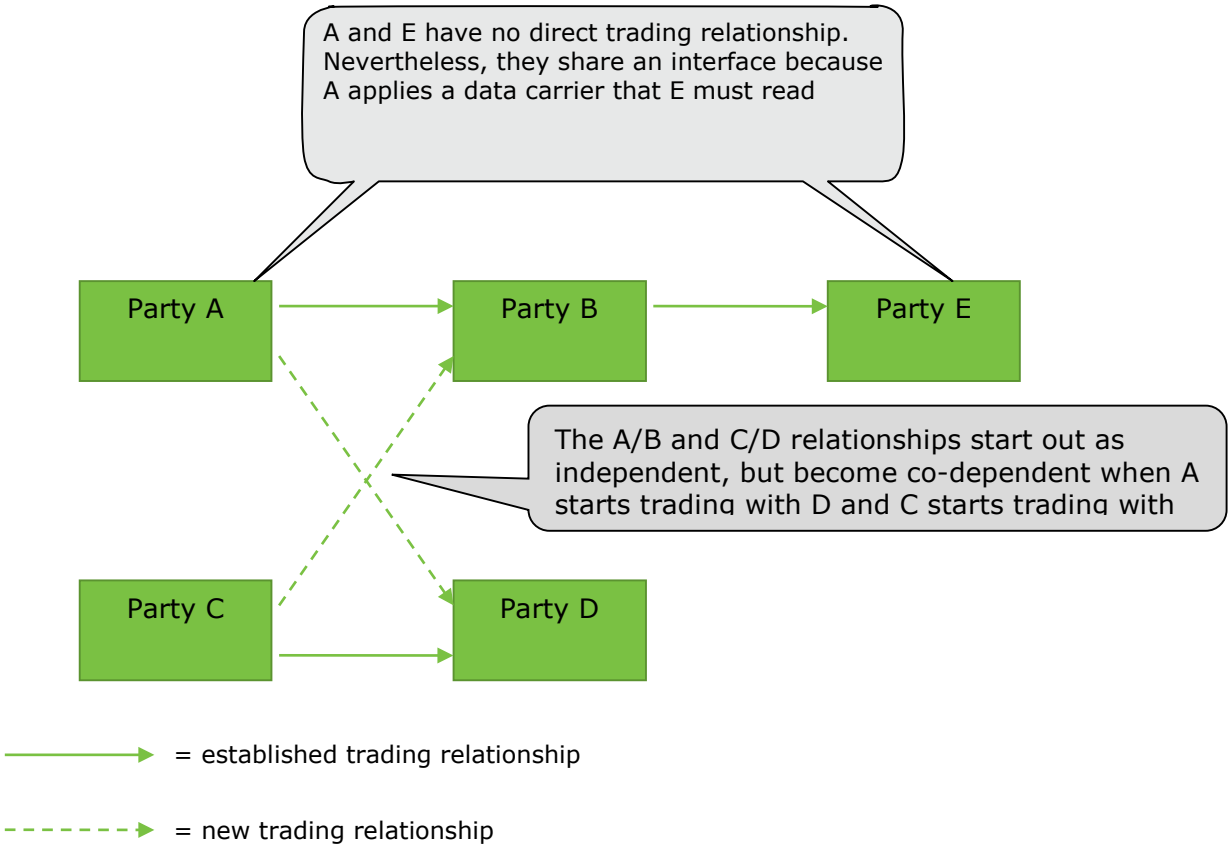
GS1's structure and processes enable it to engage a community of users that have an implicit consensus to use standards (at least some part of the GS1 system according to their needs) and to use them according to the published specifications. This consensus is partly achieved because all users have the opportunity to participate in the development and ongoing maintenance of the standards and mainly because there is a strong commercial incentive to be part of the standards community. Achieving the three objectives listed above depends on adoption by a substantial community of users and as the community grows the benefits to each user multiplies. GS1's community of end users is at least as important as the standards themselves.

2.2 Open supply chains

A *supply chain* is a set of companies and other organisations involved in trading and other business relationships with one another. In many cases, supply chains are concerned with the trade of physical objects such as tangible products, parts, raw materials, and the like. Supply chains may also involve trade of digital objects such as music downloads, video-on-demand, telephony services, virtual world products, and so on.

An *open* supply chain is one in which the complete set of trading partners is not known in advance and which changes continually.[1] This has great significance for the architecture of information systems. The building blocks of an information systems architecture are the interfaces between different system components, and in a supply chain context the most important interfaces are those that exist between different companies in the supply chain. For example, in an interface for communicating digital purchase order information, one company (the buyer) is the sender of data, and another company (the seller) is the receiver. In a closed supply chain, a fixed universe of trading partners is known in advance, and so interfaces can be negotiated in a controlled, coordinated way, and change management is simplified because all parties can agree to make changes simultaneously. In an open supply chain, by contrast, the parties on either side of an interface may not even know about each other.

[1] The word "open" in "open supply chain" has a particular meaning as defined in this section. The use of the word "open" in this context should not be confused with other meanings that are also important to the GS1 System Architecture. In particular, "open standard" refers to a standard that may be freely adopted by any end user, and the word "open" is also used in security discussions to refer to a lack of or lenient access control. These are different meanings of the word "open."



The open nature of supply chain interfaces manifests itself two ways, as illustrated in the above figure. 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 is sold to retailers through distributors, and this barcode is read by all retailers who receive the product. The barcode is an interface between the manufacturer and the retailers, but the manufacturer's only business relationship is with distributors.

Secondly, as trading relationships come and go, a company may find that it needs to extend an existing interface to encompass 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. Some time 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. Company A would like to use the identical interfaces and supporting information systems to trade with C as it does to trade with B, and likewise for C as it trades with B and D.

Both of these manifestations of open supply chains have a profound influence on the design of information interfaces. They require that interface definitions be negotiated and implemented *outside* the context of any particular trading relationship, and be adhered to by all parties so that interoperability will be achieved despite the fact that the companies on each side of the interface are not able to negotiate in advance. It leads to the definition of broadly accepted industry standards, in which the emphasis is placed on interoperability, maximum applicability to a broad range of business contexts, and minimisation of choices that require pre-coordination between interfacing parties. These are precisely the principles that underlie GS1 standards.

2.3 GS1 standards: Identify, Capture, Share

GS1 standards support the information needs of end users interacting with each other in supply chains, specifically the information required to support the business processes through which supply chain participants interact. The subjects of such information are the real-world entities that are part of those business processes. Real-world entities include things traded between companies, such as products, parts, raw materials, packaging, and so on. Other real-world entities of relevance to

trading partners include the equipment and material needed to carry out the business processes surrounding trade such as containers, transport, machinery; entities corresponding to physical locations in which the business processes are carried out; legal entities such as companies, divisions; service relationships; business transactions and documents; and others. Real-world entities may exist in the tangible 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 real-world entities in supply chain business processes:

- Standards which provide the means to **Identify** real-world entities so that they may be the subject of electronic information that is stored and/or communicated by end users. GS1 identification standards include standards that define unique identification codes (called GS1 identification keys) which may be used by an information system to refer unambiguously to a real-world entity such as a trade item, logistics unit, physical location, document, service relationship, or other entity.
- Standards which provide the means to automatically **Capture** data that is carried directly on physical objects, bridging 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 which allow GS1 identification keys and supplementary data[2] to be affixed directly to a physical object, and standards that specify consistent interfaces to readers, printers, and other hardware and software components that connect the data carriers to 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 data capture because not all "identification" is automated and not all "AIDC" is identification.
- Standards which provide the means to **Share** information, both between trading partners and internally, providing the foundation for electronic business transactions, electronic visibility of the physical and digital world, and other information applications. GS1 standards for information sharing include data standards for master data, business transaction data, and physical event data, as well as communication standards for sharing this data between applications and trading partners. Other information sharing standards include discovery standards that help locate where relevant data resides across a supply chain and trust standards that help establish the conditions for sharing data with adequate security.

While GS1 standards may be used in any combination in a given business application, the "Identify, Capture, Share" paradigm is pervasive in situations where GS1 standards apply, and most such business applications employ GS1 standards from all three groups.

For example, consider the business processes that support the retail sale of consumer goods. GS1 standards are commonly used as follows:

- **Identify**: Each class of trade item (informally, each distinct product) is assigned a Global Trade Item Number (GTIN) following GS1 identification standards (specifically, the GTIN section of the *GS1 General Specifications*, and the GTIN Allocation Rules). By adhering to GS1 standards, all products receive a globally unique GTIN, so that any retailer 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 (in contrast to a system where each brand owner devised its own identification system), and each product brand owner need only assign a single identifier to its trade item (in contrast to a system where each retailer devised its own identification system).

- **Capture**: Each trade item carries its GTIN identifier directly on the product package using a barcode that adheres to GS1 barcode standards, possibly also using GS1-compliant radio-frequency identification (RFID) tags. Data capture infrastructure conforming to GS1 standards is

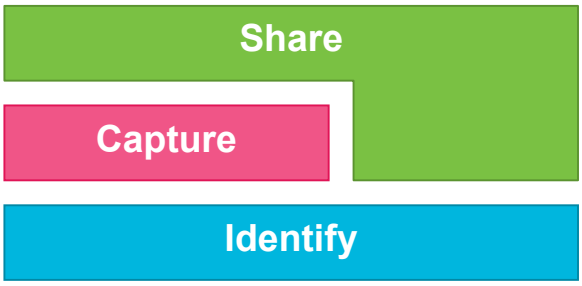
[2] In a strictly layered approach, GS1 Capture standards would deal exclusively with affixing GS1 identification keys to real-world entities, and all supplementary data would be exchanged using GS1 data sharing standards (especially those that define master data). This general approach is outlined in section 7. However, there are certain situations in which supplementary data must be physically affixed to a physical item itself, so that this data is available even if information networks are not. For this reason, certain supplementary data are "borrowed" into the Capture layer so that they may be affixed to physical objects and read using GS1 Capture standards.

used to automatically and reliably record trade items as they move through the supply chain, from shipping to receipt to point-of-sale.

Landscape §3, §6, §6, §8

- **Share**: The retailer obtains from brand owners product master data conforming to GS1 master data standards; such data is used in many ways, for example to display a concise description of the product when it is scanned at the point-of-sale terminal. GS1 Electronic Data Interchange (EDI) standards may be used by the retailer to reorder product from the manufacturer when supplies run low. GS1 visibility event data standards may be used to provide detailed information about events such as what products entered and exited each store, both for use by the retailer and by its suppliers (when such sharing is authorised by the retailer). Master data, electronic transaction data, and visibility event data are all governed by GS1 data standards, and use the GTIN or another GS1 identification standard to refer precisely to the appropriate trade items or other real-world entities.

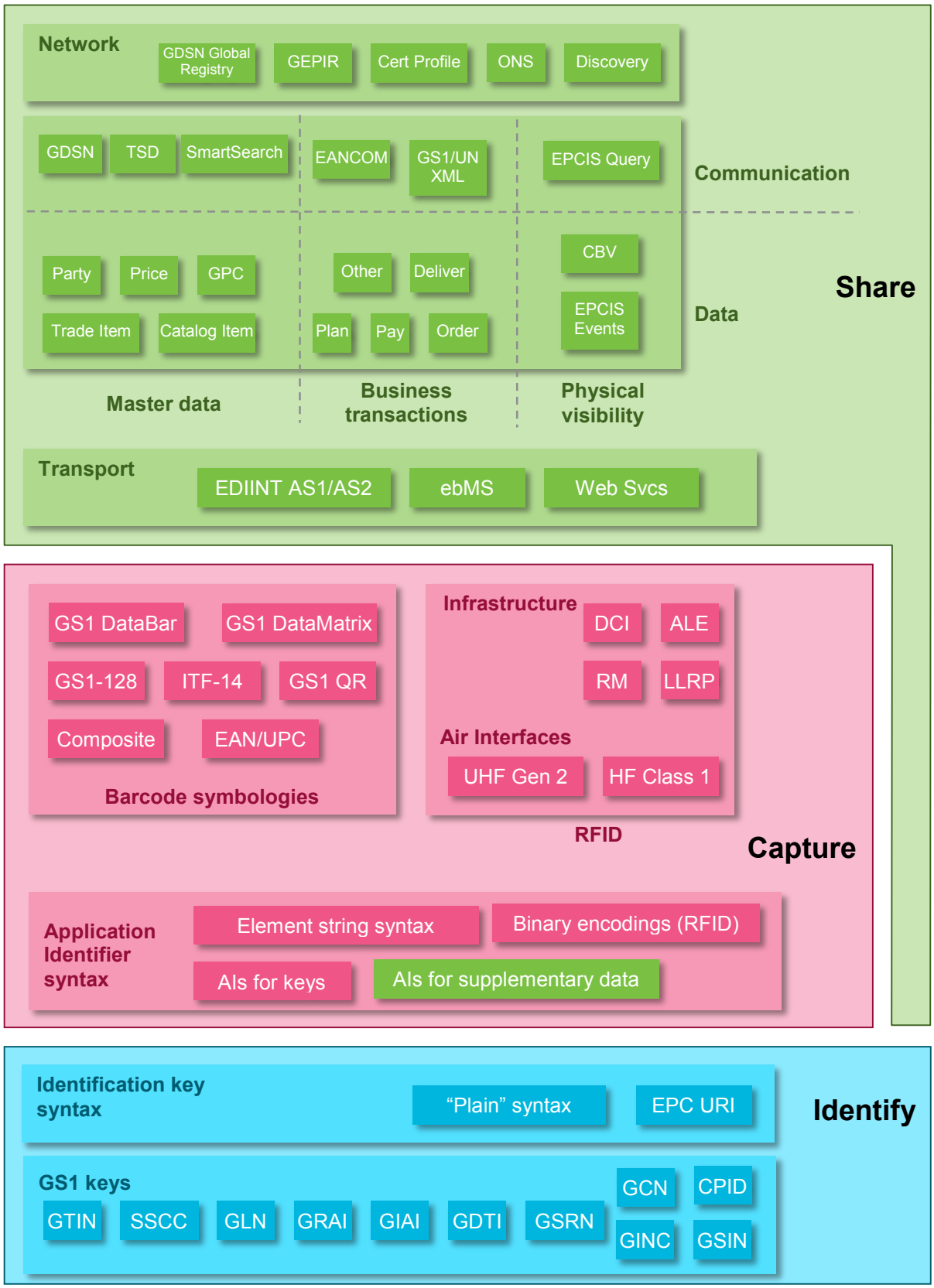
The relationship between GS1 standards for identification, capture, and sharing is depicted below.



The key relationships are as follows:

- Both capture standards and sharing standards make use of unique identifiers for real-world entities, using GS1 identification standards. There is therefore a dependence between the capture and sharing standards and the identification standards. (Some capture and sharing standards may also be used with non-GS1 identification; see Section 4.3. In such cases, the relationship of capture and sharing standards to identification still holds true, even though identification is provided by something other than GS1 standards.)
- Where a real-world entity exists in the physical world, physical data carriers (barcodes and/or RFID tags) are used to bridge the world of the physical and the world of information (where the sharing standards exist). In such situations, GS1 capture standards come into play, and logically sit between the identification standards and the sharing standards.
- However, there are other situations in which identification is used directly by sharing standards without any physical data capture. For example, master data describing a trade item may be shared between trading partners in advance of any instances of that trade item actually being manufactured. In another example, a music download is an example of something that is bought and sold as any other trade item, but the entire transaction including the delivery of the product is entirely electronic and therefore never involves the use of capture standards (which by definition always involve a physical data carrier such as a barcode or RFID tag). For this reason, GS1 sharing standards have a dependence on identification standards both directly, and indirectly through the capture standards.

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



2.4 GS1 services: Assign, Register, Discover

GS1 services are facilities that are offered or coordinated by GS1 that provide benefit or assistance to other parties. Each GS1 service is available globally, with consistent functionality as viewed by end users around the world. The responsibility for provisioning of the service and support of users is divided between the GS1 Global Office, GS1 Member Organisations, and 3rd party service providers. The details of this division of responsibility vary from service to service and are discussed below.

Both GS1 Member Organisations (MOs) and 3rd party service providers may also provide their own services to GS1 end users, which are not "GS1 services" as defined here. Such MO and 3rd party services are not necessarily offered globally and are not coordinated across GS1 as a whole. They are out of scope of this architecture document. However, local services of this kind are sometimes a proving ground for new ideas that eventually become GS1 services.

2.4.1 Functional scope of GS1 services

Some GS1 services are training programs and other types of customer support activities. Other GS1 services have a more direct connection to the *GS1 System Architecture*, the GS1 standards, and the information systems that end users construct using GS1 standards. These GS1 services provide a backbone that provides identification to end users, links end users together, and enables end users and service providers to build all kinds of value-added services based on GS1 identification standards.

The facilities provided by the latter type of GS1 services may be grouped into three categories, as follows:

- **Assign**: GS1 services provide the backbone for assignment of GS1 identification keys according to GS1 standards for identification.
- **Register**: GS1 services provide for the registration of identification keys and associated data. Through the process of registration, the existence of a given identification key and the data associated with it can be published and made available to other organisations.
- **Discover**: GS1 services provide for one party to discover the existence of identification keys registered by others as well as the data and services associated with those keys.

GS1 services for assignment, registration, and discovery together provide a backbone that allows all the users of the GS1 system and their data to be interconnected. They support an open supply chain environment in which the population of supply chain participants is constantly changing.

A given GS1 service may perform functions that span more than one of the above categories. The following table summarises existing GS1 services and the categories of operations they provide for different types of identification:

Type of identification	——————— Services ———————		
	Assign	Register	Discover
GS1 Company Prefix	Provided by each GS1 Member Organisation	Provided by each GS1 Member Organisation	GEPIR
GS1 identification key	Individual assignment provided by each GS1 Member Organisation (Many are self-assigned by the end user using a GS1 Company Prefix, subject to terms of use established when the GS1 Company Prefix was assigned)	GEPIR (for GTINs and GLNs that an end user chooses to register) GDSN for GTINs and GLNs(*), with associated master data ONS	GEPIR (for GTINs and GLNs that are registered) GDSN for GTINs and GLNs(*), with associated master data ONS
Serialised GS1 identification key (e.g., SGTIN)	(Self-assigned by the end user)	Data Discovery (future development)	Data Discovery (future development)

(*) Support in GDSN for registration and discovery of information pertaining to GLNs is not nearly as well developed as it is for GTINs. There are activities currently underway within GS1 to provide

enhanced services for registration and discovery of GLNs, and these services may or may not use GDSN.

The role of GS1 services is limited to the three areas of assign, register, and discover. There may be many other types of useful services provided to end users based on GS1 standards, but these are provided by parties other than GS1. The role of GS1 services is to provide the minimal backbone to make it possible for other parties to implement such services and for end users to discover such services and use them. For example, ONS allows a service provider to register an association between a GTIN or other class-level GS1 identification key and any Internet-based network service. Such services are then discoverable using ONS as a lookup mechanism.

2.4.2 Division of responsibilities

The responsibility for provisioning of the service and support of users is divided between the GS1 Global Office, GS1 Member Organisations, and 3rd party service providers. The goal of this division is to promote a federated approach to services where consistent functionality is available to end users on a global basis, but where GS1 Member Organisations and 3rd party service providers can cater to local markets, customs, and business models.

The division of responsibilities is summarised below:

Responsibility	How provided
Interface definition of GS1 service	A consistent interface specification of the GS1 service is employed globally. The scope of this interface specification includes: ▪ The interaction between the GS1 service and an end user client. The interface specification defines the minimum required functionality between the service provider and an end user; for some GS1 services it is possible for the service provider to provide value-added enhancements in addition. ▪ If the service requires coordination among the federated service providers, the interaction between providers is also governed by the interface specification. In some cases, this interface specification is a GS1 standard. In other cases, the specification is a document agreed by GS1 but not formally ratified as a standard. A GS1 standard is always used if 3rd party service providers offer the service directly to end users (as opposed to a 3rd party acting as a subcontractor to a GS1 Member Organisation in an outsourcing relationship).
Deployment and operation of systems and processes that provide the service	Depending on the service, systems are provided by GS1 Member Organisations (MOs) or 3rd party service providers, or both. Where a GS1 MO does not choose to provide the service directly to its end users, the GS1 Global Office may provide the service for that geography. Some services involve a technical component deployed by the GS1 Global Office that coordinates the systems provided by GS1 MOs and/or 3rd party service providers. Example: The GEPIR service is provided by systems deployed by GS1 MOs, with the GS1 GO providing a central point of coordination to federate the local systems. The GS1 GO also provides the MO-level service for MOs that cannot or do not wish to deploy their own system. Example: The GDSN service is provided by GDSN certified data pools, which in many cases are run by 3rd party service providers and in some cases by GS1 MOs. The GS1 GO operates the GS1 Global Registry, which facilitates the flow of data between data pools.
Customer Relationship and Pricing	The relationship to individual end users and pricing of services to end users are governed by the GS1 MOs and/or 3rd party service providers that provide the service, or the GS1 GO in those cases where an MO chooses not to provide the service itself.

Within the above framework, the architecture of each GS1 service varies according to the business requirements for that service.

3 General considerations

The term "GS1 system" refers broadly to all of the artefacts created by the GS1 community, including GS1 standards, GS1 guidelines, GS1 solutions, and GS1 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, solutions, services

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

- **GS1 standards**: A GS1 standard is a specification that defines the behaviour of one or more system components so that certain goals are achieved. Typically these goals are interoperability of system components, whether different components deployed by the same supply chain party or components deployed by different supply chain parties. Standards contain *normative* statements, which specify what a system component must be or do in order to be in conformance to the standard; a standard is written in such a way that conformance to the normative statements is a sufficient condition for a system component to achieve the interoperability or other goals for which the standard is designed.
- **GS1 guidelines**: A GS1 guideline is a document that provides information considered useful in implementing one or more GS1 standards. A GS1 guideline never provides additional normative content beyond the standards to which it refers; instead, the purpose of a GS1 guideline is to provide additional explanation and suggestions for successful implementation. While conformance to a GS1 standard may be necessary to achieve an interoperability goal, use of a GS1 guideline is never required. GS1 standards typically focus on "what" a system component is or must do, whereas GS1 guidelines may provide additional suggestions for "how" such a component may be implemented. GS1 guidelines may be general in nature (applying to all implementations) or may be specific to a limited number of use cases or industries.
- **GS1 service**: A GS1 service is a facility offered or coordinated by the GS1 Global Office (GO) that provides benefit or assistance to other parties. For example, GEPIR is a lookup service coordinated by the GS1 GO that provides all end users with the ability to look up information about GS1 identification keys.
- **GS1 solution**: A GS1 solution is a set of elements from the GS1 portfolio, those elements being GS1 standards, GS1 guidelines, GS1 services, and other GS1 solutions. In a GS1 solution, this set of elements is brought together to address a specific business need or purpose. GS1 solutions provide a convenient package by means of which GS1 Member Organisations can assist end users in implementing GS1 standards to achieve particular business goals.

GS1 standards and GS1 guidelines are created by the GS1 community via the Global Standards Management Process (GSMP) facilitated by the GS1 Global Office. GS1 services and GS1 solutions are created by the GS1 Global Office with the involvement of the GS1 community but outside of GSMP. Distinguishing between GSMP and non-GSMP helps to ensure complete transparency and definitiveness as to when GS1 plays a facilitation role versus a product creation role. Some GS1 services or GS1 solutions may be created by a GS1 Member Organisation (MO) to meet local needs.

GS1 standards may be further distinguished according to the type of normative content they contain, as follows[3]:

- **Technical Standards**: A technical standard is one that defines a particular set of behaviours for a system component. Technical standards focus on "what" a system component must be or do to be in conformance to the standard. Technical standards are typically written to be as broadly applicable across business sectors and geographic regions as possible. While a technical standard may illustrate specific business problems to which it applies, a technical standard does not specify which industries or businesses must adopt the standard. An end user may choose for itself whether to deploy a component that conforms to a particular technical standard.

  Technical standards may be further distinguished as follows:

  - **Data standard**: A data standard is one that defines the syntax and semantics of data. Conformance to a data standard is assessed by examining a particular instance or instances of data to see whether it follows the normative statements laid out in the data standard.
  - **Interface standard**: An interface standard is one that defines an interaction between system components, often by defining the syntax and semantics of messages that are exchanged between system components. Conformance to an interface standard is assessed by examining a particular system component (often a hardware or software product) to see whether it correctly generates messages and/or responds to received messages according to

[3] This is a different classification than the "identify, capture, share" classification of section 2.3 , which is a classification along functional lines. These two classifications are different ways of looking at the same standards.

the normative statements in the interface standard. Most interface standards identify two roles as the interacting "sides" of the interface and a given system component is assessed for conformance to one or the other of these roles (or sometimes both).

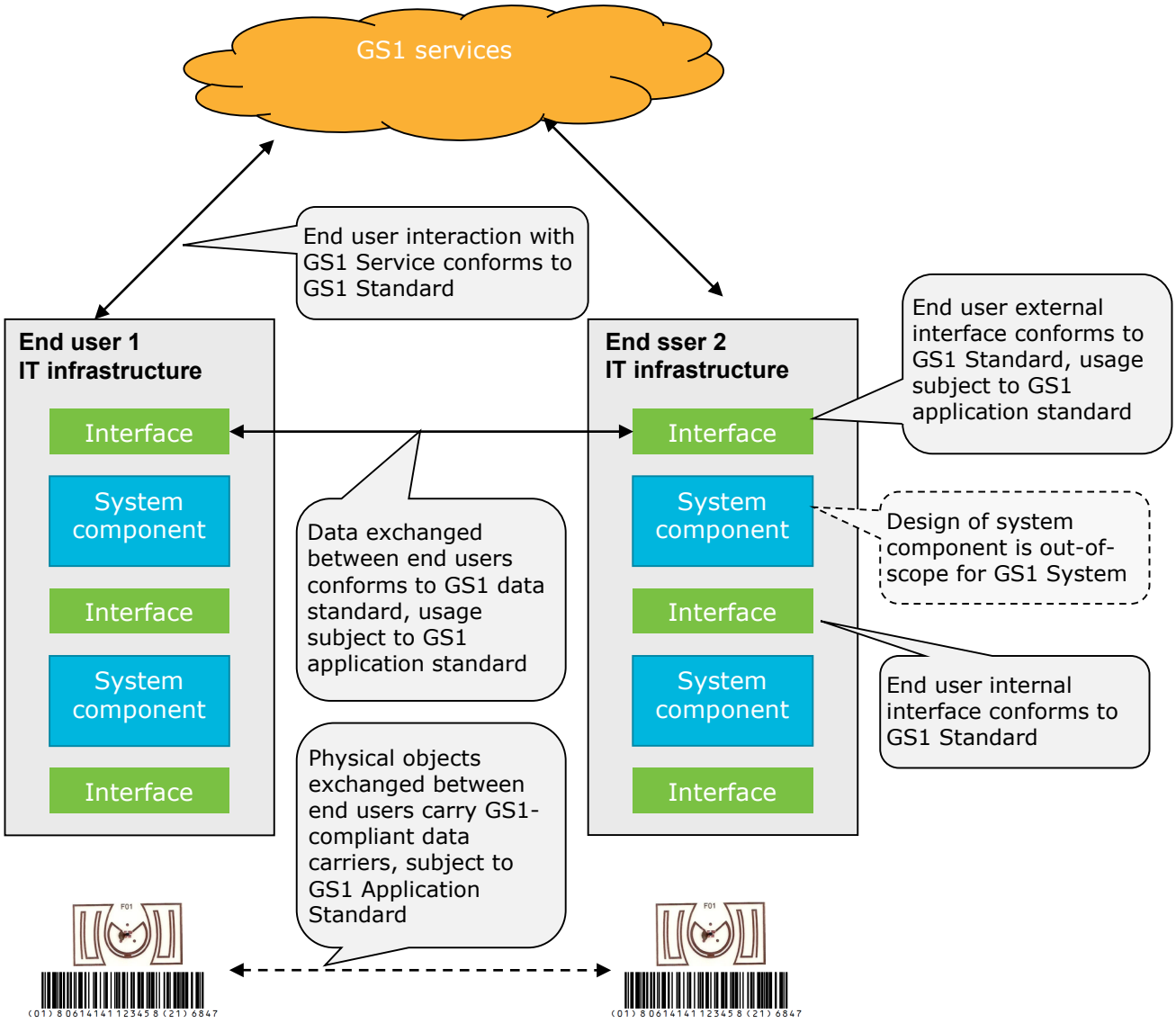
The distinction between data and interface standard is not always sharp, and many technical standards contain both data specifications and interface specifications. Indeed, because data is always exchanged across an interface, an interface standard nearly always contains a data standard or refers normatively to other data standards.

- **Application standards**: An application standard is one that specifies a particular set of technical standards to which end user systems must conform in a particular business application. Application standards provide a convenient way for different end users to express their agreement to follow certain standards, in order to achieve mutually agreed interoperability goals in a given application context.

Application Standards are examples of *profiles*, a profile being a standard whose normative content consists exclusively of references to other standards along with normative constraints upon their use. Application standards take the form of a profile together with statements about the application area to which it applies. A profile may also be a technical standard that defines a subset of one or more other standards for a narrower purpose.

In general, GS1 standards seek to specify a single way of achieving a given business goal. In some cases, GS1 standards provide alternatives; for example, a standard that defines two different concrete syntaxes for the same abstract data construct, each optimised for a different implementation context. Having choices detracts from interoperability, and so GS1 standards offer choices of this kind only when absolutely necessary. In some cases, GS1 Technical Standards offer choices and GS1 Application Standards define single choices to be used in different application contexts.

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



GS1 Guidelines may assist end user in implementing a GS1 Standard

GS1 Solutions may suggest a combination of GS1 Standards, Guidelines, Services, and other

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 these elements of GS1 system. In particular, 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, and may also make use of GS1 services to carry out certain tasks. A given end user's system architecture may also use alternative or additional standards, including data and interfaces beyond those governed by GS1 standards.

The *GS1 System Architecture* does not define a system architecture that end users must implement, nor does it dictate particular hardware or software components an end user must deploy. The hardware and software components within any end user's system architecture may be created by the end user or obtained by the end user from solution providers, but in any case the definition of these components, apart from GS1 services, is outside the scope of the *GS1 System Architecture*. GS1 standards only define data and interfaces that the end user's components may implement. The

GS1 System Architecture explicitly avoids specification of components in order to give end users maximal freedom in designing system architectures according to their own preferences and goals, while defining data and interface standards to ensure that systems deployed by different end users can interoperate and that end users have a wide marketplace of components available from solution providers.

Because the GS1 system does not define a system architecture per se, this document does not normatively specify a particular arrangement of system components and their interconnection. However, in order to understand the interrelationship of GS1 standards and GS1 services, it is sometimes helpful to discuss how they are used in a typical system architecture. Within this document, therefore, there are illustrations showing how components of the GS1 system fit together. It is important to bear in mind, however, that any such illustration differs from a true system architecture in the following ways:

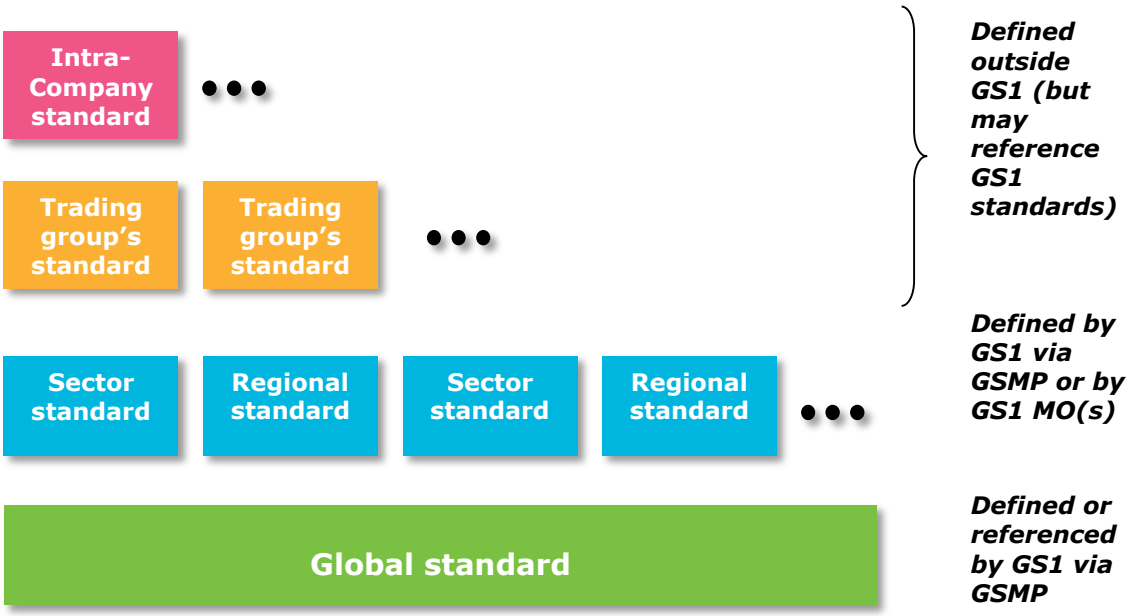
- An end user system architecture may need to employ only a subset of the GS1 standards and GS1 services depicted here. For example, two businesses may agree to use GS1 EDI standards for electronic product ordering and payment, but not (yet) need to use the Global Data Synchronisation Network (GDSN) for master data synchronisation.
- The mapping between hardware and software roles depicted here and actual hardware or software components deployed by an end user may not necessarily be one-to-one. For example, to carry out a business process of shipment verification using EPC-encoded RFID tags, one end user may deploy a system in which there is a separate RFID Reader (a hardware device), Filtering & Collection middleware (software deployed on a server), and EPCIS Capturing Application (software deployed on a different server). Another end user may deploy an integrated verification portal device that combines into a single package all three of these roles, exposing only the EPCIS Capture Interface. For this reason, this document is careful to refer to roles rather than components when talking about end user system elements that make use of GS1 data and interface standards.
- Moreover, roles depicted here may be carried out by end user system components that may have additional responsibilities outside the scope of the *GS1 System Architecture*. For example, it is common to have enterprise applications such as Enterprise Resource Planning (ERP) systems that play the role of shipper or receiver in the context of GS1 EDI standards but at the same time play many other roles within the enterprise for which no GS1 standard is relevant.

The overall intent of the *GS1 System Architecture* is to provide end users with great flexibility in creating system architectures that meet their needs.

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 particular industry but where all industry participants must still rely upon normative standards in order to achieve interoperability and/or economies of scale in meeting those needs. 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:



The hierarchy is as follows:

- **Global**: At the core of any implementation are the components of the GS1 system that have broad applicability across industry sectors. Most of the GS1 technical standards, including interface standards and data standards, fall into this core.
- **Sector / Regional**: A particular industry sector may profile particular technical standards for use within that industry. GS1 Application Standards are examples of such profiles. There are also certain GS1 data standards that are sector specific, such as some of the Global Data Synchronisation Network (GDSN) extensions that define master data specific to product categories arising within a particular industry sector.

  Regional requirements may be addressed via profiles or other normative documents created by GS1 Member Organisations to serve their respective geographical regions.

  Both Sector and Regional standards are designed so that they can be used seamlessly with the global standards, and users who do not employ them 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 would be developed outside of GS1, but would make reference to GS1 standards and guidelines. An example of a Trading Group standard is an industry consortium who specifies a particular set of GS1 global standards for use by its members.
- **Company**: Individual companies are encouraged to develop their own internal architectural standards to drive the consistent use of GS1 standards across the enterprise. The publications methodology for GS1 standards and guidelines, including versioning and the use of permanent web locations for GS1 publications, is designed to facilitate this.

It should be noted that while a hierarchy of standards as described above can be an effective way to achieve the widest possible interoperability while still catering to narrower needs that do not rise to the global level, great care must be taken so that sector, regional, trading group, or company standards do not inadvertently create more problems than they solve. In particular, 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 which have mutually incompatible requirements. Ideally, requirements are pushed to the global level whenever possible.

3.4 Consistency across data standards – the Global Data Dictionary

Many GS1 standards include normative definitions of data. These include definitions of individual data elements such as the definitions of the GS1 identification keys and code lists, definitions of

"documents" comprised of many individual data elements, and definitions of messages that are exchanged between system components.

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. The GS1 Global Data Dictionary (GDD) serves this purpose. The GDD is a compendium of the data elements defined across all GS1 standards that are XML-based and intended for inter-company data exchange (i.e., in the Share layer). It also includes GS1 EANCOM code lists and AIDC Application Identifiers. The GDD is not itself a GS1 standard, but rather is a tool which helps to ensure consistency across all GS1 standards in the following ways:

- It provides definitions for each distinct data element that may occur across several standards.
- When new data elements are incorporated into a new or revised GS1 standard, the GDD helps to avoid conflicting definitions for data elements already existing and to ensure that new data elements are not given names that would be confusingly similar to existing ones.

The working group that creates or revises an individual GS1 standard is responsible for aligning the definitions in that standard with the GDD, with the assistance of GS1 staff dedicated to GDD maintenance.

4 Identify – GS1 identification keys

This section discusses the general architectural foundations that underlie GS1 standards for identification.

4.1 Data modelling background

Fundamentally, GS1 standards for identification rest on a foundation of data modelling, which is concerned with how things in the real world may be modelled in the form of data that can be manipulated by data processing systems of various kinds. This section defines some common data modelling terms that form the architectural foundation for GS1 standards for identification discussed in the sections that follow.

4.1.1 Entities

In this section, the term *entity* is a generic term referring to that which GS1 standards seek to identify:

- **Entity**: An entity is something in the real world that is the subject of information in an information system. An entity may be:
  - **Physical**: A tangible object in the real world made of matter. In particular, a physical object is something to which a physical data carrier (barcode or RFID tag) may be physically affixed.
  - **Digital**: An artefact that exists in a computer system, not made of matter in the physical world, but which nevertheless has a recognisable lifecycle and is subject to supply chain processes analogous to physical objects. 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) and so on.

4.1.2 Attributes

Information systems are concerned with associating information with entities. The items of associated information are here called attributes.

- **Attribute**: A piece of information associated with an entity. An attribute may be recognised if one can construct a sentence of the following form: "The [attribute name] of [entity] is [attribute value]."

Example: Example Corporation has 20 forklifts. Forklift #3 has a load capacity of 10 metric tons. So "load capacity" is the name of an attribute, whose value for Forklift #3 is 10 metric tons: "The load capacity (attribute name) of Forklift #3 (entity) is 10 metric tons (attribute value)." In this example, the entity is a physical object.

Example: Example Corporation sells a product which is a 20-count box of Example Chocolate Widgets. Every box of widgets weighs 500 grams. So weight is the name of an attribute, whose value for 20-count widgets is 500 grams: "The weight (attribute name) of 20-count Example Chocolate Widgets (entity) is 500 grams (attribute value). In this example, the entity is a trade item class (20-count box of Example Chocolate Widgets) which is a business abstraction, not a physical object. Note that an *individual* 20-count box of Example Chocolate Widgets is a physical object, but the class of all 20-count boxes of Example Chocolate Widgets is a business abstraction.

Attributes can be classified based on how frequently they change.

- **Static attribute**: An attribute whose value does not change over the life of the entity. E.g., the load capacity of a specific forklift.
- **Quasi-static attribute**: An attribute whose value changes infrequently over the life of the entity. E.g., the last name of a person (which may change infrequently due to marriage or other reasons).
- **Dynamic attribute**: An attribute whose value changes frequently over the life of the entity. E.g., the price of a product or of a stock.

This classification does not affect the nature of an attribute from a data modelling perspective but may have a great influence on implementation choices for information systems that use the attribute.

The above classification of attributes is related to the notion of master data, a topic that is taken up in greater detail in section 6. The term master data typically refers to attributes where (a) the attribute is static or quasi-static; (b) the entity is long-lived and/or new entities are not created very frequently; and (c) the attribute is of interest to many parties. Those characteristics lead to certain styles of sharing of master data that would be infeasible or inappropriate for other types of attributes.

4.1.3 Keys

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

- **Key**: An attribute (or group of attributes, see below) of an entity that serves to uniquely identify that entity, within some specified domain of entities. An information system uses a key as a proxy for the entity itself.

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

- **Simple key**: A single attribute that serves as a key. (E.g., in the domain of Example Corporation employees, the Employee ID may be the key that identifies an employee.)
- **Compound key**: Two or more attributes which together serve as a key, where no subset of those attributes taken by themselves would do so. (E.g., in the domain of US cities, the combination of the "city name" and "state" attribute uniquely identifies a city, and so these two attributes together may be used as a compound key to identify a city. "City name" by itself is not a key, because Springfield, Illinois and Springfield, Massachusetts both have the same city name.)

In order to be usable as a key, an attribute (or set of attributes, for a compound key) 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 have different values of their keys
- **Completeness**: There exists a key value for every entity within the specified domain. (i.e., the key value cannot be null)

- **Persistence**: The same key value denotes a given entity throughout the entity's life. (This implies a key is always a static attribute.)

It is critically important to note that the properties above depend on the application context. Therefore, whether a given attribute of an entity is usable as a key depends on the application context.

Example: In an application run by a US State government that tracks population of cities within that State, the "city name" attribute of a city has all the properties above and is usable as a key. But in an application run by the US Federal government that tracks population of cities in all States, "city name" is not unique and therefore may not be used as a key (at least not by itself).

Example: In the fictional country of Examplestan, citizens are assigned a taxpayer ID number for life, but those numbers may be reassigned 20 years after a person's death. In an application that only processes 10 years' worth of data about Examplestan citizens, the taxpayer ID number may be used as a key, but in an application that processes 30 years' worth of data the taxpayer ID may not be useable as a key.

The above description defines the word "key" in the data modelling sense. "GS1 identification keys," discussed in greater detail in Sections 4.2 through 4.4, are a particular application of this concept. GS1 identification keys are defined by GS1 standards that are intended to have very broad applicability. The goal of the *GS1 General Specifications* and key allocation rule standards is to define GS1 identification keys so that they can be used as a key in the above sense, and moreover to define them in such a way that they are likely to be usable as keys in the widest possible set of application contexts; that is, for any application context in which a GS1 identification key might be used, the definitions provided by the *GS1 General Specifications* and key allocation rule standards will likely be sufficient for the GS1 identification key to have the properties of Uniqueness, Completeness, and Persistence within that application context.

4.1.4 Terms relating to construction of keys

In many of the illustrations above, a key is an attribute that an entity "already has"; that is, it has already been associated with the entity in the real world, and it can be used as a key if it can be shown to satisfy the properties above. (E.g., the city name examples above.)

In many applications, and in the case of GS1 identification keys in particular, a key is invented specifically for the purpose of being a key. Such keys are artificial constructions that would not exist as attributes of the entities involved if there were no information systems that were trying to model those entities. In this case, there is freedom to design the keys to meet information system requirements and so some design considerations apply.

- **Syntax**: An artificial key typically has syntax rules that define the universe of strings from which key values may be drawn. 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, etc.
- **Capacity**: The uniqueness and completeness requirements for being a key are affected by the capacity that is implied by the syntax rules. E.g., if the syntax rules for a key that is intended to identify an employee specify that the key is a 6-digit decimal number, but there are more than 1,000,000 employees, then it is impossible to achieve both uniqueness and completeness, and hence the 6-digit decimal number is unusable as a key.
- **Assignment methodology**: Keys can be assigned centrally, out of one single coordinating body, or in a distributed manner. The latter is a method for assigning new keys that delegates the assignment process to multiple points of control, while still achieving uniqueness. This requires strict compliance to rules of construction by all parties involved. Typically this involves a hierarchical structure 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 subscriber (who assigns the final key). The hierarchical assignment process may or may not be evident in the final key. In the GS1 system this is usually evident (when a "GS1 Company Prefix" is

assigned) but not always (e.g. when individual keys are assigned directly by a GS1 Member Organisation).

- **Routability**: Given the value of a key, the ability to locate data related to a key, or at least to determine an entry point to locate such data.
- **Non-significance**: The extent to which the value of the key conveys no useful information apart from uniquely identifying a specific entity within the specified domain. More precisely, 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. On the other hand, a key may embed information about the key itself, such as which organisation is responsible for issuing the key or how to route information requests regarding the key, and still be non-significant. In general, significance severely limits the capacity of the key space (or else requires a very long key). More importantly, significance leads to severe problems if the nature or structure of the embedded information ever needs to change. For this reason, GS1 keys are defined in a way that is non-significant, though as noted above the assignment process is evident in the final key.

4.1.5 Terms relating to use of keys in applications

Within an information system, a key is used as a proxy for the real world entity that it uniquely identifies.

In a particular application context, an entity may have more than one attribute (or more than one compound attribute) that is usable as a key. In this case, the application chooses one particular attribute (or compound) to use consistently as the key. This is termed the primary key.

- **Primary key**: A simple or compound attribute that is used consistently by an application as the key to refer to an entity within a specified domain.

Because the *GS1 General Specifications* do not define any particular application context, the term primary key does not arise there. An individual application may choose to use a GS1 identification key as the primary key if appropriate.

An entity typically has many attributes. Some attributes have values that are simple scalar values, such as numbers or character strings. Other attributes have values that are other entities. For example, in an employee database, an employee may have an attribute "department" that says in which department he works. But in this same database, a department may itself be an entity with attributes, and each department has an attribute "department number" that is the primary key for the department. In this case, the value of the employee's "department" attribute is a key for a department entity. An attribute of this kind, whose value is itself a key, is called a foreign key.

- **Foreign key (key-valued attribute)**: A simple or compound attribute of an entity whose value is conceptually another entity (the "referenced entity") and in the information system is the key value for that referenced entity. If the referenced entity's key is a compound key consisting of N attributes, then the foreign key will also consist of N attributes.

The phrase "key-valued attribute" better conveys what a foreign key is, though the term "foreign key" is widely used and understood.

4.2 GS1 identification keys and supplementary data

In light of the definitions given in Section 4.1, the goal of GS1 data standards can be understood as defining standardised attributes for real-world entities including, most significantly, standardised attributes that may be used as keys to refer to specific entities.

Landscape §2.1

- **GS1 identification key**: An identifier defined by GS1 standards that is usable as and intended as a key to refer to a specific business entity. These are considered to be part of the Identify layer of the *GS1 System Architecture*.
- **Other business data:** Any data element that is not an identification key or key qualifier (a data element used to form a compound key). These are considered to be part of the Share layer of the *GS1 System Architecture*. However, this category includes a subset of data elements called "supplementary data" as described below

- **Supplementary data**: Attributes of entities, other than primary keys, defined by GS1 standards, that may be directly affixed to an entity using a GS1 data carrier. While these are architecturally part of the Share layer, the Capture layer defines the syntax for including them in GS1 data carriers. (In some places within the *GS1 General Specifications,* these are simply called "attributes".)

The above terms refer to data defined in GS1 standards for identification. Other data is defined in other GS1 standards.

GS1 identification keys and Supplementary Data are identified using *application identifiers* (AIs). An AI is a short string (2, 3, or 4 characters) which identifies the data element, whose brevity is particularly suited to identifying data elements when encoded into GS1 physical data carriers.

The following table summarises the GS1 identification keys in relation to the definitions in Section 4.1. Not every "key" in the data modelling sense is defined as a GS1 identification key in the *GS1 General Specifications*. The "candidate key" column in the table below indicates what combination of GS1 identification keys and other data elements may serve as a "key" in the data modelling sense for the entity given in the first column.

Entity	Physical / Digital / Abstract	Candidate key
Trade Item Class	Abstract	GTIN
Trade Item Lot	Abstract	GTIN + AI 10 (compound)
Trade Item Instance	Physical or Digital	GTIN + AI 21 (compound)
Logistics Unit	Physical	SSCC
Legal entity (Party)	Abstract	GLN
Physical Location	Physical	GLN GLN + AI 254 (compound)
Digital Location	Digital	GLN
Function (location)	Physical or Abstract	GLN
Returnable Asset Class	Abstract	GRAI without optional serial number
Returnable Asset Instance	Physical	GRAI with serial number
Individual Asset	Physical or Digital	GIAI
Document Type	Abstract	GDTI without optional serial number
Document Instance	Physical or Digital	GDTI with serial number
Service Relation	Physical or Abstract (Note 1)	GSRN
Consignment	Abstract	GINC
Shipment	Abstract	GSIN
Payment Slip	Physical or Digital	GLN + AI 8020
Coupon	Physical or Digital	GCN without optional serial number
Coupon Instance	Physical or Digital	GCN with serial number
Component / Part Class	Abstract	CPID
Component / Part Instance	Physical	CPID + AI 8010 (compound)

Notes:

1. GSRNs are commonly used to identify recipients and providers of services in the context of a specific service relationship, and these recipients and providers are often individual people and therefore physical entities.

4.3 Classes of GS1 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 some organisation other than GS1 is the issuing authority. For this reason a classification of keys, drawn from a GS1 perspective, is helpful in understanding the relationship between a key and the rest of the GS1 system.

The following classification of keys is used:

- **Class 1**: Keys administered by GS1 and fully under its control
- **Class 2**: Keys whose framework is controlled by GS1 and for which a portion of the identification capacity is allocated for an identification scheme administered by an external agency
- **Class 3**: Keys fully administered and controlled outside GS1 but which are supported in some part or parts of the GS1 system
- **Class 4**: Keys that are entirely outside the GS1 system i.e. all identifiers that meet the technical definition of "key" in Section 4.1.3, but are not in the first three classes.

This classification is described in more detail below.

4.3.1 Class 1 keys

A class 1 key has its structure, allocation, and lifecycle rules defined by GS1. Class 1 keys always start with a GS1 Company Prefix[4]. They usually start with a GS1 Company Prefix licensed by a GS1 Member Organisation (MO) or by the GS1 Global Office to a user company. In some cases, class 1 keys are licensed one by one by MOs to user companies, using a GS1 Company Prefix licensed by an MO to itself for that purpose. They are subject to allocation rules defined in GS1 standards, and their association with attributes is governed by validation rules also defined in GS1 standards.

The allocation and lifecycle rules and the standardised structure guarantee full interoperability between users of all layers of the GS1 system. This means that when a company uses a class 1 key for its intended purpose it can be confident that its GS1-compliant trading partners will be able to accept and process it per GS1 standards.

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

4.3.2 Class 2 keys

A class 2 key starts with either a GS1 Prefix or a GS1 Company Prefix, incorporates a key administered by an external organisation, and includes a check digit if required by its corresponding class 1 key format. Class 2 keys are unique with respect to class 1 keys of the same type and their values are a subset of all possible values of the corresponding GS1 key. Their allocation and lifecycle rules, however, are defined by an organisation external to GS1. The degree to which these rules are compatible with those of the corresponding class 1 keys is specific to each class 2 key. In some cases they can easily be used alongside class 1 keys, but sometimes legal restrictions or dominant business practices lead to acceptance of class 2 keys whose rules vary significantly from their class 1 equivalents.

It is important to understand that technical compatibility is not the same in practice as interoperability. Technical compatibility is achieved by having uniqueness of values within the namespace and a similar basic structure for the identifier (e.g., GS1 Company Prefix, object reference, and check digit). It is still possible for business or legal restrictions to be imposed requiring use of a certain format or range of values, even if such restrictions are not technically justified. It might be argued that class 2 keys are more susceptible to these geopolitical constraints than keys in class 1.

[4] This is not quite literally true, because the syntax of the GTIN-14 and SSCC keys include an extra digit that precedes the GS1 Company Prefix. However, from the standpoint of the allocation process, the GS1 Company Prefix are the first digits to be chosen during the construction of a key, so in this sense the GTIN and SSCC also "start with" a GS1 Company Prefix. Note that in the EPC URI syntax, the first digits *are* always the GS1 Company Prefix.

Interoperability is the ability to use the key within the context of business processes supported by GS1 standards. However, the degree of interoperability with GS1 system depends on the extent to which a class 2 key conforms to class 1 key functionality and rules.

Class 2 keys are always based on a GS1 Prefix issued by the GS1 Global Office and might be based on a GS1 Company Prefix issued by a GS1 Member Organisation or the GS1 Global Office. Examples include:

- The International Standard Serial Number (ISSN) may be used with GS1 Prefix 977 to form a key compatible with GTIN-13.
- The International Standard Book Number (ISBN) is issued using GS1 Prefixes 978 and 979 to form a key compatible with GTIN-13.
  - A subset of ISBNs starting with 9790 are reserved for the International Standard Music Number (ISMN).
- GS1 Prefix 34 is used with Club Inter Pharmaceutique (CIP) codes for pharmaceuticals in France to accommodate national numbers inside the GTIN number range
- The Produce Electronic Identification Board uses the GS1 Company Prefix 033383 issued by GS1 US combined with a commodity code issued by the Produce Manufacturers Association to create "PEIB UPCs" inside the GTIN number range.

Whether a class 2 key contains a GS1 Company Prefix or a GS1 Prefix alone is determined by the GS1 party to the contractual agreement with the external organisation. A class 2 key that contains a GS1 Prefix alone may also have a structure that is similar to the GS1 Company Prefix, that is, where the GS1 Prefix and some number of following digits are assigned by the external organisation to other organisations who assign the remaining digits. This depends on the type of key, on the nature of the agreement between the GS1 party and the external organisation, and on the structure of the external organisation's key. Such use is not the same as containing a true GS1 Company Prefix because it is not assigned by GS1.

Every GS1 party that supports class 2 identification keys is required to document whether it issues identifiers using a structure similar to the GS1 Company Prefix, and if so, what portion of their identifier is "equivalent" to the GS1 Company Prefix. Examples include:

- no equivalent for ISSN;
- GS1 Prefix, registrant group, and registrant for ISBN;
  - GS1 Prefix, registrant group, and publisher for ISMN;

There must be a contractual agreement between the GS1 Global Office or a GS1 Member Organisation and the agency that administers the embedded key. This agreement specifies at minimum the following:

- GS1 system components that can be used with the key (e.g. ISBN can only be used with the EAN/UPC data carrier)
- Restrictions that may apply, e.g. ISBN can only be used for books
- Financial considerations
- GS1 keys allocation and lifecycle rules
- Validation rules
- Compatibility with class 1 key function and syntax for example:
  - Will this class 2 key work with physical data carriers and GDSN validation rules
  - Will this class 2 key support ONS
  - Etc…
- Restrictions on reciprocity (e.g. national or currency zones)

4.3.3 Class 3 keys

A class 3 key has its structure and its rules for use defined, administered and managed by an organisation external to GS1. This organisation enters into an agreement with GS1 that enables its keys to be used in selected GS1 standards; for example, within an EPC header.

It is intended that class 3 keys are used in selected GS1 standards without disrupting users of class 1 and class 2 keys, but:

- GS1 gives no assurance that class 3 keys will be recognised by users of class 1 and class 2 keys
- GS1 has no expectation that systems relying upon class 3 keys should recognise keys from class 1 or class 2
- GS1 has no expectation that systems relying upon one type of class 3 key should recognise other types of class 3 key.

Companies can take advantage of GS1 technology, network, and communications standards for class 1, 2, and 3 keys, but should not expect full interoperability between keys in classes 1 and 2 and keys in class 3.

Keys in class 3 at the present time are:

- The Auto-ID Center General Identifier (GID)
- Keys compliant with US Department of Defence (USDoD) and Airline Transport Association (ATA) standards that are based on the Commercial and Government Entity (CAGE) and Department of Defense Activity Address Code (DoDAAC) identification standards.

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

4.3.4 Class 4 keys

A class 4 key is administered and managed externally to GS1 and is not accommodated by any GS1 standard as a key (primary identifier). Examples include:

- Data Universal Numbering System (DUNS);
- Vehicle identification number (VIN);
- Bureau International des Containers (BIC) codes;

4.3.5 Summary

The following table summarises the key classification discussed above.

Class	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 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 class 1 and 2 keys.

4.4 Identifier Syntax: "Plain", GS1 element string, EPC

When a GS1 identification key or other identifier is used in an information system, it is necessarily represented using a specific concrete syntax. The syntax that is used may depend on the medium in which the identifier exists; for example, an XML message is text-oriented, while the memory of an RFID tag is binary-oriented. The syntax may also depend on the context in which the identifier appears. Specifically, there are some contexts in which only one type of identifier is expected and others where more than one type of identifier may appear. In the latter case, the identifier syntax requires some means to distinguish between different identifier types.

GS1 standards provide three different syntaxes for identifiers that support progressively broader application contexts:

- **"Plain"**: 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 key is expected. Examples of such single-key contexts include: a barcode symbology that is defined to only hold one type of key (e.g., ITF-14 which can only hold a GTIN), an XML element in a business document that is defined to hold only a single key (e.g., the rental record example below), a column in a database table that is intended to hold only a single key.

- **GS1 element string (Capture layer)**: This syntax consists of a short (2-4 character) "application identifier" that indicates what type of GS1 identification key follows, followed by the key itself. This allows one type of GS1 identification key to be distinguished from another. 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. (It also allows for concatenation of two or more keys or supplementary data elements, but then the resulting string is not itself an identifier.) The "GS1 element string" syntax is used in the Capture Layer as a means for carrying multiple data elements in a single barcode.

- **Electronic Product Code (EPC) URI**: This syntax is an Internet 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 key that identifies a specific physical or digital object, including some class 3 keys as defined in section 4.3. Because of the use of URI syntax, the EPC URI is usable in a context where any Internet resource is expected, not just an identification key.

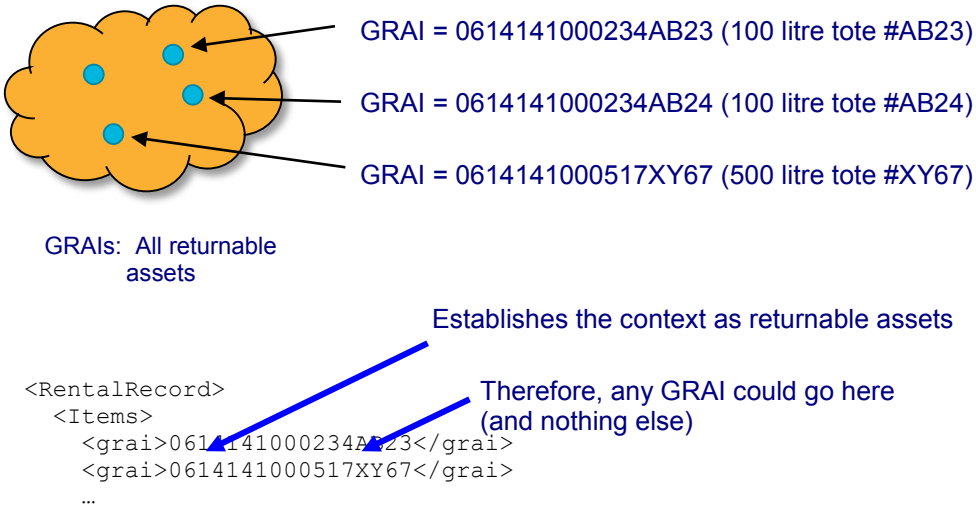
While any given GS1 identification key may be represented in more than one of the above three syntaxes, its *meaning* is always the same regardless of syntax.

The following table illustrates a GS1 Global Returnable Asset Identifier (GRAI) in each of the three syntaxes:

Syntax	Example	Remarks
"Plain"	0614141234561789	A GRAI composed from GS1 Company Prefix 0614141, Asset Type 123456, Check Digit 1, and Serial 789
GS1 element string	800306141412345617 89	The Application Identifier 8003 indicates the following key is a GRAI. The GS1 element string for GRAI also includes an extra "0" padding digit immediately following the Application Identifier. The remainder of the element string is the same as the plain syntax.
EPC URI	urn:epc:id:grai:0614141.23456.789	The "urn:epc:id:grai:" header specifies that this EPC URI corresponds to a GRAI. The GS1 Company Prefix, Asset Type, and Serial are separated by dot (".") characters. The check digit is not included in this syntax.

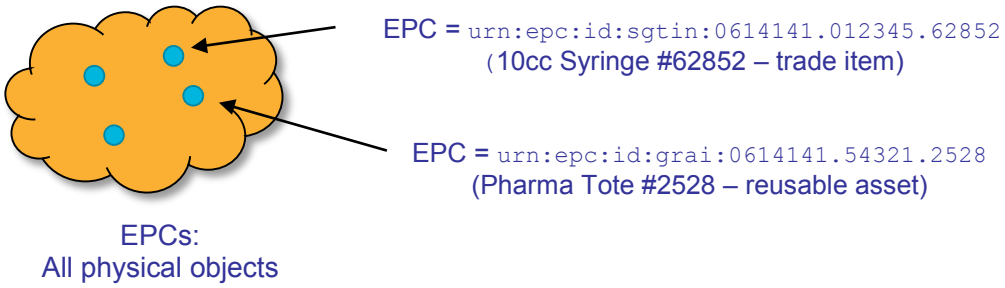
An identifier may occur in an electronic record or file, in a database, in an electronic message, or any other data context. In any given context, the producer and consumer must agree on types of identifiers that may occur, and the syntax to be used. The choice of syntax will be constrained by how narrow or broad the context is.

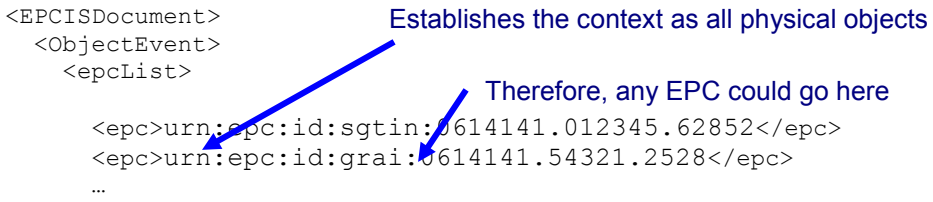
For example, the Global Returnable Asset Identifier (GRAI) is a key that is used to identify returnable assets, such as plastic totes and pallet skids. The set of GRAIs can be thought of as identifiers for the members of the set "all returnable assets." The "plain" syntax for GRAI code may be used in a context where only returnable assets are expected; e.g., in a rental agreement from a moving services company that rents returnable plastic crates to customers to pack during a move. This is illustrated below.



The upper part of the figure illustrates the set of all returnable assets identified by GRAIs. The lower part of the figure shows how the "plain" syntax for GRAI might be used in the context of a rental agreement, where only a GRAI is expected. (There is no GS1 standard that defines a rental agreement business document, so this illustrates how end users can create their own business documents using GS1 identification keys.)

In contrast, the EPC URI provides a syntax for any identifier that names a specific physical or digital object. The set of EPCs can be thought of as identifiers for the members of the set "all physical or digital objects." EPCs are used in contexts where any type of physical or digital object may appear; for example, in the set of observations arising in a hospital storage room where returnable totes, trade items, and other objects might be observed. This is illustrated below:

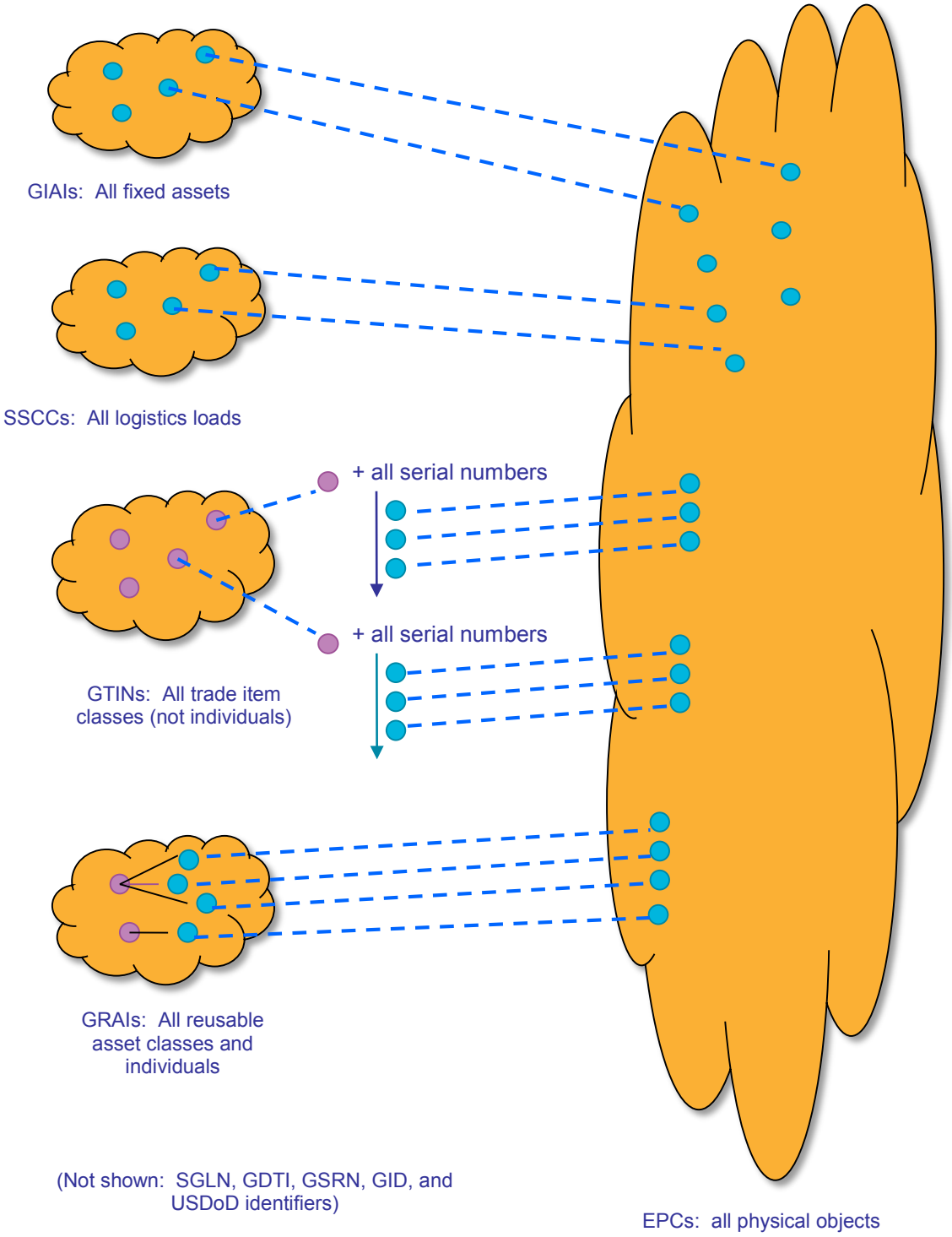




The upper part of the figure illustrates the set of all physical and digital objects identified by EPCs. The lower part of the figure shows how the both a GRAI identifying a returnable asset and a serialised GTIN identifying a trade item might occur in the same business document that records a physical observation. (In this example, the business document illustrated also happens to be a GS1 standard, namely the EPCIS standard for visibility event data.)

The EPC URI can be thought of as federating different identifier types into a single syntax. For this reason, it is sometimes referred to as a "meta-key". The correspondence between EPC URI syntax and "plain" or GS1 element string syntax is formally defined by conversion rules specified in section 7 of the *EPC Tag Data Standard*.[5] The well-defined correspondence between the various syntaxes allows for seamless migration of data between "plain", GS1 element string, and EPC URI syntax as necessary. URI syntax also serves to embed GS1 identification into the larger universe of Internet Uniform Resource Identifiers.

[5] Despite the title of the standard, this particular section of the EPC Tag Data Standard does not have anything to do with RFID Tags or any other kind of "tag" for that matter. Other sections of the EPC Tag Data Standard specify how EPC URIs are encoded into binary data for storage on a GS1 Gen 2 RFID Tag.



Not every GS1 identification key corresponds to an EPC URI, nor vice versa. For example:

- A Global Trade Item Number (GTIN) by itself does not correspond to an EPC, because a GTIN identifies a *class* of trade items, not an individual trade item. The combination of a GTIN and a unique serial number, however, *does* correspond to an EPC. This combination is called a Serialised Global Trade Item Number, or SGTIN.
- In the *GS1 General Specifications*, the Global Returnable Asset Identifier (GRAI) can be used to identify either a *class* of returnable assets, or an individual returnable asset, depending on whether the optional serial number is included. Only the form that includes a serial number, and

thus identifies an individual, has a corresponding EPC. The same is true for the Global Document Type Identifier (GDTI).

- EPCs include identifiers for which there is no corresponding GS1 identification key; that is, certain class 3 identifiers as defined in section 4.3. These include the General Identifier, the US Department of Defense identifier, and the Aerospace and Defence Identifier.

5 Capture – Physical data carriers and data capture infrastructure

Landscape §6

The "Capture" standards in the GS1 system are standards for automatically capturing identifying information and possibly other data that is associated with a physical object. 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 data capture. A physical data carrier is a means of physically affixing data to a physical object so that the data can be captured without human data entry. Data carriers range in capability, from the simplest barcodes whose only function is to deliver a single unchanging piece of data when read, to the most sophisticated RFID tags which are small computing devices. Interaction with the latter may be more than mere "data capture," though the term "capturing" is still used as a general label for that process. The processes involved in putting data into physical data carriers, including printing of barcodes and programming of RFID tags, are also included under the label of "capturing."

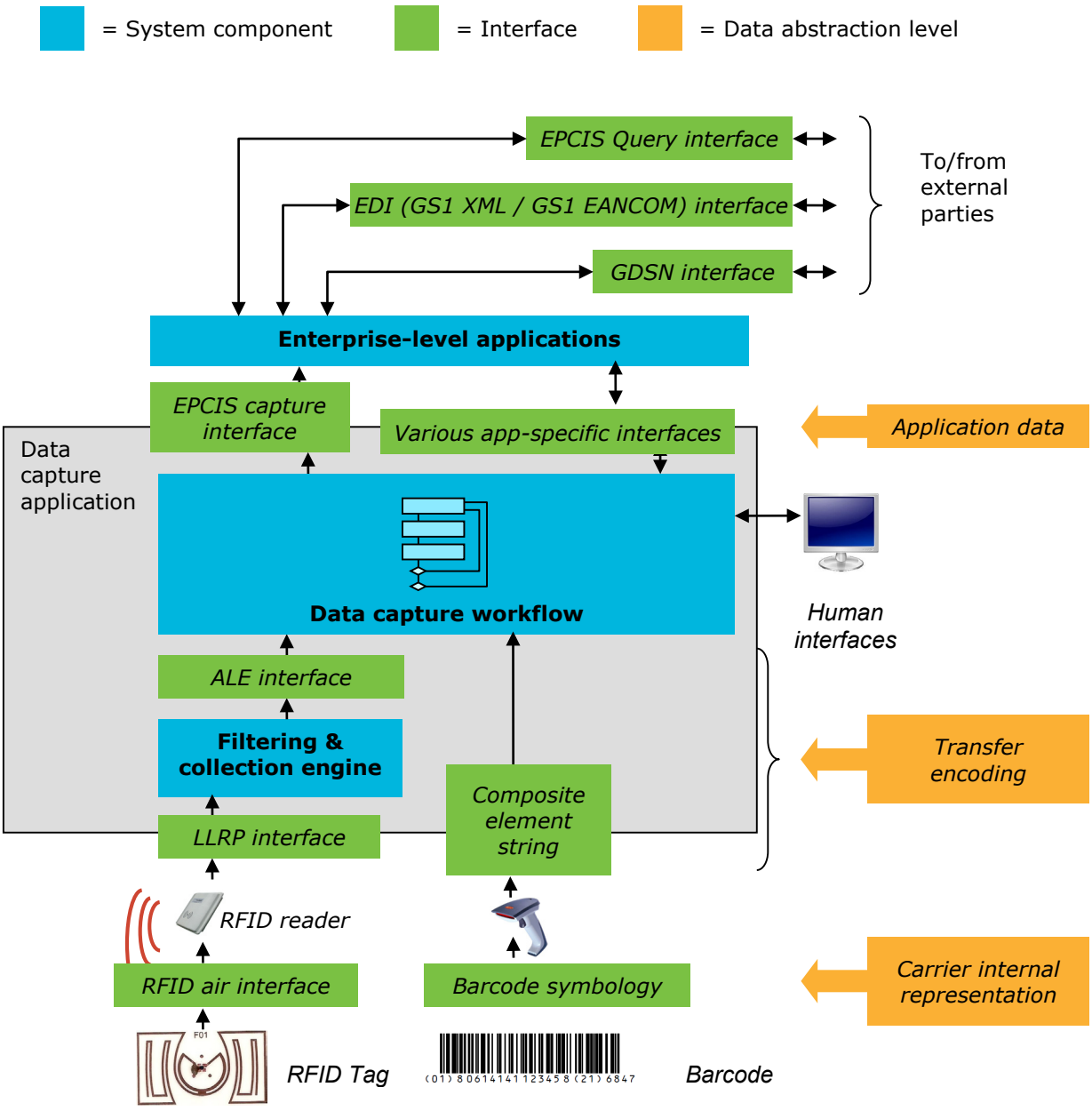
This section outlines the general foundations of GS1 standards for data capture.

5.1 Data capture architecture

At its most fundamental, physical data capture may be used in any situation that calls for input of data associated with a physical object. A recurring architectural pattern is that physical data capture takes place within the context of a data capture workflow, which is a small business process involving the handling of physical goods. Examples of data capture workflows include: checking out trade items at point-of-sale, receiving logistics units into inventory, marking products with unique serial numbers (here the data captured is the association of the serialised identifier to the physical object), inventory counting of fixed assets, and so forth. Data capture workflows mostly take place at the "edge" of a business – in physical plant such as factories, warehouses, retail stores, as opposed to business workflows that exist virtually within applications running in data centres.

Within a given data capture workflow there may be many individual interactions with physical data carriers. A data capture workflow may also involve interaction with humans, as well as "back end" information systems such as Enterprise Resource Planning (ERP), Warehouse Management System (WMS), etc. All these things combine to create a business context within which the data capture workflow takes place, and this gives meaning to the act of capturing the data from the data carrier. For example, at a point of sale 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, if the POS operator presses a different button, scanning the same barcode may instead mean that the product is being returned rather than purchased, or that a prior checkout is being voided. In each case, the operator of the POS terminal establishes the business context that gives meaning to each barcode scan.

This leads to a typical architecture for a data capture application. The figure below shows the ingredients found in data capture application architecture. The exact architecture for any given data capture application will vary from case to case – for example, not all data capture applications use both barcodes and RFID, some data capture applications print barcodes rather than scanning them, etc – but the diagram shows the commonly occurring relationships between components and how GS1 standard interfaces fit in.



At the centre of a data capture application is the data capture workflow that supervises the business process step within which data capture takes place. This is typically custom logic that is specific to the application. Beneath the data capture workflow in the diagram is the data path between the workflow and GS1 data carriers: barcodes and RFID. The green bars in the diagram denote GS1 standards that may be used to interface to the data carriers. At the top of the diagram are the interfaces between the data capture workflow and larger-scale enterprise applications. Many of these interfaces are application- or enterprise-specific, though using GS1 data as building blocks. The Electronic Product Code Information Services (EPCIS) interface is an example of GS1 standard that is often used as an interface between a data capture workflow and enterprise-level applications. Note that the interfaces at the top of the diagram, including EPCIS, are independent of the data carrier used at the bottom of the diagram.

The purpose of the interfaces and the reason for a multi-layer data capture architecture is to provide isolation between different levels of abstraction. Viewed from the perspective of an enterprise application (i.e., from the uppermost blue box in the figure), the entire data capture application shields the enterprise application from the details of exactly *how* data capture takes place. Through the application-level interfaces (uppermost green bars), an enterprise application interacts with the

data capture workflow through data that is data carrier independent and in which all of the interaction between data capture components has been consolidated into that data. At a lower level, the data capture workflow is cognisant of whether it is interacting with barcode scanners, RFID Interrogators, human input, etc, but the transfer interfaces (green bars in the middle) shield the data capture workflow from low-level hardware details of exactly how the data carriers work. The lowest level interfaces (green bars on the bottom) embody those internal data carrier details. This leads to different representations for GS1 standard data for each level of abstraction, as indicated by the pink labels in the diagram. This is discussed in more detail in the following section.

5.2 Varieties of data carriers; Data carrier independence of data

A principle of GS1 standards is that data elements are defined in a data carrier neutral way so that their semantics is the same regardless of what data carrier is used to affix them to a physical object (and also the same outside of a physical data carrier, such as in an electronic message). However, there is a multitude of different data carriers, each optimised for a particular set of physical and performance constraints arising in the real world. Standards for each data carrier therefore define a carrier-specific representation of carrier-neutral data elements, allowing those data to be encoded in a manner compatible with the physical constraints of the carrier. For example, in a DataMatrix barcode data elements are first arranged into a "GS1 element string" that frames each data element with a short identifying character sequence and separator characters, then at a lower level encodes the resulting sequence into a pattern of dark and light squares. In a Gen 2 RFID tag, those same data elements are separated into different memory banks, then at a lower level encoded into a highly compacted binary form and stored into an electronic memory circuit.

In considering the complete data path from data carrier through capturing application to business data, 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 which type of data carrier is 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 data carrier (barcode scanner or RFID interrogator). The transfer encoding provides access to control information and carrier information (discussed below), and therefore is different for different data carrier types.
- **Carrier internal representation**: This is the representation of data in the data carrier itself. In a barcode, this is the pattern of light and dark bars or squares. In an RFID tag, this is the binary data stored in the digital memory of the RFID chip.

The following table lists the data representations used at the different levels, and the corresponding GS1 standards that govern them:

<table>
<tr><th rowspan="2">Abstraction level</th><th colspan="2">Data representation</th><th colspan="2">Corresponding GS1 standard</th></tr>
<tr><th>Barcode</th><th>RFID</th><th>Barcode</th><th>RFID</th></tr>
<tr><td>Application data</td><td colspan="2">"Plain" Data Values
EPC URI</td><td colspan="2">GS1 General Specifications (section 3)
EPC Tag Data Standard (sections 6 and 7)</td></tr>
<tr><td>Transfer encoding</td><td>GS1 element string</td><td>EPC Tag URI
OID/value pairs
EPC binary encoding
ISO/IEC 15962 binary data</td><td>GS1 General Specifications (section 5.9)</td><td>EPC Tag Data Standard (sections 8 – 17)</td></tr>
<tr><td>Carrier internal representation</td><td>Barcode symbology</td><td>EPC binary encoding
ISO/IEC 15962 binary data</td><td>GS1 General Specifications (section 5)</td><td>EPC Tag Data Standard (sections 12 – 17)</td></tr>
</table>

At the levels of transfer encoding and carrier internal representation, there are three types of data that may be involved:

- **Application data**: Data that is delivered from the Capture layer of the GS1 system Architecture to the Share layer. Application data is data carrier independent.
- **Control data**: Data that is carrier-specific and is used to by the Capture layer of the *GS1 System Architecture* to control the interaction with the data carrier.
- **Carrier data**: Data that describes the data carrier itself, as opposed to the object to which the data carrier is attached. Carrier data is most often used as control data to control the interaction with the data carrier at the Capture layer of the *GS1 System Architecture*. For example, an EAN/UPC barcode contains only a GTIN without an AI, so the Capture layer may need to know what type of barcode was scanned in order to interpret the data correctly. In some cases, the Capture layer may integrate carrier data into the application data that is delivered to the Share layer if needed for application purposes; however, this implies that the application will be sensitive to the choice of data carrier or be restricted to use a particular type of data carrier.

The following table summarises the three types of data for different types of data carriers.

Data Type	Barcode	RFID
Application data	GS1 Data Elements and/or EPC URI	
Control Data	FNC1 indicator	EPC Header Filter value PC/XPC bits
Carrier Data	Symbology identifier	TID XTID

To illustrate Control Data and Carrier Data, a few examples are described in more detail below:

- Code 128, DataMatrix, and QR barcode symbologies support both GS1 and non-GS1 data formats. In these barcode symbologies, Function Code 1 (FNC1) is a special symbol used to indicate whether the following data is GS1-compliant or not. This is control information that the data capture layer uses to understand how to interpret the data in the barcode. (When these barcodes include FNC1, they are called GS1-128, GS1 DataMatrix, and GS1 QR, respectively.)
- In RFID tags, the filter value is control information that is used to distinguish different tag populations. For example, item-level tags may have one filter value, and pallet-level tags may have a different filter value. If the data capture layer only wants to read a pallet tag, it may instruct the RFID interrogator to broadcast a command to "turn off" tags having an item-level filter value, so that the pallet level tag may be read without having to spend time reading the much more numerous item-level tags. The filter value is control information used by the data capture layer to optimise reading performance, but is not application data. In particular, the filter value cannot be considered to be a reliable indication of packaging level from a business perspective.
- Barcode scanners include in the transfer encoding a symbology identifier, which is a 3-character string that indicates what kind of barcode was read (GS1-128, GS1 DataBar, EAN/UPC, etc). This is carrier data that describes the data carrier itself. This might be used by the data capture layer, for example, to provide feedback to the operator about which symbol was read.
- In RFID tags, the Tag Identification (TID) indicates the make and model of the silicon chip in the RFID tag. This is carrier data which the data capture layer might use in order to know what optional features the tag supports.
- In RFID tags, the Extended Tag Identification (XTID) may contain a unique serial number that is assigned by the manufacturer of the RFID tag. This is carrier data which the data capture layer might use to determine for quality control purposes which tag was read, in an application where the same object is tagged with several identically-programmed tags for the sake of robustness. As an example of using carrier data at the application level, an anti-counterfeit application might

rely on the XTID serial number to detect if an RFID tag had been "cloned" (i.e., a second tag programmed with a copy of data from a first tag). This example illustrates the point that application-level use of carrier data leads to dependence of the application upon the data carrier: because this application relies on the RFID XTID, it is only able to function fully using RFID and not barcodes.

5.3 Translation of data during physical data capture

As noted in the previous section, different representations of GS1 data are used at different levels of abstraction in the typical data capture architecture. This implies that there is a process of translation that takes place as data moves up or down in the data capture architecture (up or down as illustrated in section 5.1). These translations are specified in the various GS1 standards governing the different representations that are used, as indicated in the table in section 5.2.

For example, the following are the steps of translation as data is read from a barcode and transferred to an application:

- The pattern of bars and spaces in the barcode are analysed to determine the symbology type, and translated according to the symbology standard for that particular symbology type into a GS1 composite element string
- The GS1 composite element string is parsed according to the *GS1 General Specifications* section 5.9 into individual GS1 element strings. Each GS1 element string consists of an Application Identifier (AI) number that identifies what kind of data element, and the data value for that data element.
- The GS1 element strings are parsed according to the *GS1 General Specifications* section 3 to yield "plain" data element values. Alternatively, they may be translated according to the *EPC Tag Data Standard* Section 7 into an EPC URI.

(Note that certain GS1 barcodes can only contain a single data element; in such cases, the data element value may be extracted without an intermediate GS1 composite element string.)

The corresponding example for RFID has the following steps:

- The binary data encoded into the EPC and user memory banks is read from the tag and transferred through the RFID Interrogator's LLRP interface
- The binary data is decoded according to the *EPC Tag Data Standard*. For the EPC memory bank, the binary data is decoded according to Tag Data Standard sections 14 and 15 to yield an EPC Tag URI, which encapsulates the GS1 data elements that uniquely identify the object to which the RFID tag is affixed, along with RFID control information. For the user memory bank (which contains data supplemental to identification), the binary data is decoded according to section 17 of the Tag Data Standard to yield OID/value pairs, each giving the value of one data element.
- The EPC Tag URI is decoded into an EPC URI according to Tag Data Standard section 12. Optionally, the EPC URI may be translated according to Tag Data Standard section 7 into "plain" data element values. The OID/value pairs are also translated to "plain" data element values.

(Note that in a given RFID application, one of the two memory banks might not be read and decoded, depending on the application's data requirements. The user memory bank might also be read selectively.)

For applications that print barcodes or encode RFID tags, the translation processes above are reversed.

As the above descriptions show, at the application level either "plain" data element values or EPC URIs may be used, regardless of what type of data carrier is used at the lower levels. In this way, applications always deal with data that is independent of data carrier, even though at the lower levels the data representations are tailored to the unique operational characteristics of each data carrier.

5.4 Data capture infrastructure standards

GS1 standards for data capture include several interface standards that are employed in the data capture layer of a complete system. These provide a consistent way for data capture applications to interface with the hardware and infrastructure software required to interact with physical data

carriers. Because of the different operating model and capabilities of barcodes and RFID, there are separate standards and architecture dealing with each. This section discusses those differences, and the GS1 standards that apply.

5.4.1 Barcode data capture infrastructure standards

Barcode data capture infrastructure standards are comparatively simple because there are only two operations one can perform on a barcode:

- Read all data elements from a single barcode
- Print a barcode containing one or more data elements

Therefore, the interface to barcode equipment need only support these two operations. Both of these operations deal with the entire data content of a single barcode as a whole. In the interfaces to barcode equipment, this data content is expressed as a GS1 concatenated element string with a symbology identifier, which is a string of characters having the following parts:

- **Symbology Identifier**: A 3-character piece of control information that identifies which type of barcode symbol is involved.
- **Element strings**: A series of GS1 element strings. Each GS1 element string consists of two to four digits that identify the data element, followed by the data content for that data element. In a concatenated element string, these are arranged in an arbitrary order, with a separator character employed to delimit GS1 element strings (except in the case of certain fixed-length data elements, which have no separator and are required to precede all other data elements).

From a data capture application's perspective, the operation of reading a barcode is very similar to receiving keyboard input, in that the application simply receives a string of characters and cannot direct commands to the barcode itself (in contrast to an RFID tag, which *can* receive commands and participate in a bi-directional protocol with the data capture application). For this reason, there is no formal interface standard for reading barcode data in the GS1 system. Instead, it is expected that applications will receive barcode data in a manner similar to keyboard input (and indeed, many barcode scanners even emulate keyboard input at the hardware level). The *GS1 General Specifications* specify the syntax of the GS1 concatenated element string as defined above, and this is what is presented to the data capture application.

The operation of printing a barcode is also centred on a GS1 concatenated element string which specifies the data content of the printed barcode. In a typical printing application, however, there is usually much more information to be provided to the printer. This includes information about the barcode symbol itself such as dimensions, bar spacing, colour, and so on. There may also be human readable information printed immediately beneath the barcode, and the barcode may be just one element in a complete page description for a label or other printed output that contains many types of printed data. For this reason, the interface to print a barcode is often embedded within a fully-featured page markup language. There are no GS1 standards that govern this kind of interface.

5.4.2 RFID data capture infrastructure standards

Radio Frequency Identification (RFID) is a method of Automatic Identification and Data Capture in which data is carried by an electronic device called an RFID Tag, which communicates via radio frequency (RF) signals with a reading device called an RFID Interrogator (also called an "RFID Reader," though most such devices are capable of "writing" as well as "reading").

Data capture from RFID tags is more complex than for barcodes, owing to the more complex capabilities possessed by RFID tags. Among the differences are:

- RFID Tags can be read even when there is not a direct optical line of sight from the RFID Tag to the RFID Interrogator. Among other things, this means that it might be more difficult for a data capture application to know exactly which RFID Tag is being read if many are present.
- A single Interrogator may read many Tags simultaneously, and so the interfaces must deal with data from more than one Tag at a time.
- Data on RFID Tags is organised into multiple memory banks, each of which provides random access. Reading and writing operations therefore must specify which memory banks and memory addresses are to be involved.

- The data on RFID Tags may be added to or changed at any time, so that besides reading and writing operations there are also add, update, and delete operations.
- Certain types of RFID Tags may provide additional functionality besides data storage and retrieval; for example: encryption, authentication, access control, electronic disabling ("killing"), sensors, actuators, etc. The interfaces must provide the ability to perform these operations as well.
- The interaction between an Interrogator and a population of RFID Tags is a conversational protocol that offers many features through which the performance of the Interrogator-Tag interaction may be tuned. Interfaces must provide access to these features.
- An application may utilise more than one RFID Interrogator simultaneously to interact with a given RFID Tag population, to improve reliability. Such applications require interfaces that allow for merging of the data streams from different Interrogators.

For these reasons, the interface between a data capture application and RFID Interrogators is quite a bit more complex than the interface to a barcode scanner. In fact, RFID systems tend to employ an additional layer of software between the data capture application and individual RFID hardware devices so that there are actually two interfaces between a data capture application and the RFID Interrogator with which it interacts:

§5.2.3.2

- **The Application Level Events (ALE) Interface**: ALE is a GS1 standard interface between a data capture application and one or more RFID Interrogators. ALE provides data capture applications with a high-level interface in which data from more than one RFID Interrogator may be aggregated together, in which RFID data is fully decoded and presented in a form most usable to application logic, and in which data is filtered to avoid multiple reads, unwanted tags, etc. ALE also allows for multiple applications to simultaneously interact with the same RFID Interrogators. ALE is designed to let a data capture application focus on *what* data and operations it wants to use in interacting with RFID tags, without exposing the details of *how* this is accomplished in the interaction between Interrogator and Tag.

§5.2.3.1

- **The Low Level Reader Protocol (LLRP) Interface**: LLRP is a GS1 standard interface to a single RFID Interrogator device. It is a lower-level interface than ALE and provides full control over the operation of the RFID Interrogator including low level details of the Interrogator-Tag interaction. Data at the LLRP level is represented in the same raw, encoded form that is used in the RFID Tag memory itself. LLRP allows a single client to have full control over a single reader.

When both ALE and LLRP are used together, there is typically a layer of software between the LLRP and ALE interfaces. This software is called "filtering and collection" software. Filtering and collection software is responsible for receiving high-level instructions from one or more data capture applications that interface through ALE, determining how best to carry out those instructions by commanding individual RFID Interrogator devices, and then operating each Interrogator through LLRP. The filtering and collection software also translates between the raw, encoded data formats used in the RFID Tag memory to the application-friendly decoded formats used by data capture applications.

Not all RFID data capture deployments use both ALE and LLRP. In some instances, a data capture application may be written to use LLRP directly. This typically entails more work than interfacing to ALE but in simple situations may result in less software being required. In other instances, a proprietary interface to an RFID Interrogator is used in place of LLRP.

ALE and LLRP are part of the "data path" of an RFID data capture architecture – they are responsible for the communication of application data between RFID Tags and the application layer. Complex RFID deployments involving many RFID Interrogators typically also have a "control path" through which the RFID hardware devices themselves may be configured, managed, and monitored for proper operation. This is especially necessary when RFID devices are not directly controlled by human operators. There are two GS1 standards that provide interfaces useful in constructing a control path for RFID infrastructure:

§5.2.3.3

- **The Reader Management (RM) Interface**: RM is a GS1 standard interface through which a monitoring application may obtain information about the health and status of an RFID Interrogator, including whether it is operational, how many tags are being read, and so on.

§5.2.3.4

- **The RFID Discovery, Configuration, and Initialisation (DCI) Interface**: DCI is a GS1 standard interface through which an RFID Interrogator 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.

As the ALE, LLRP, RM, and DCI standards define interfaces through which system components communicate over a network, they are specified in layers as described in section 6.5.

6 Share – Business data and communication

This section discusses the general architectural foundations underlying GS1 standards for business data sharing, which complement the GS1 standards for identification and the GS1 standards for data capture discussed in earlier sections.

All GS1 standards are connected with business data in some way. Most business data is concerned with real-world business entities such as trade items, legal entities, locations, and so forth. The GS1 standards for identification, as discussed in Section 4, provide the essential foundation upon which it is possible to construct business data that refers unambiguously to real-world entities. GS1 standards for identification are therefore used in all kinds of business data, including data for internal use and data that is shared with other end users. To the extent that such data is generated from interactions with the physical world the GS1 standards for capture play a role as well.

The GS1 standards for sharing of business data discussed in this section come into play when data is used to automate the interactions between two or more end users. In such circumstances, 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. Finally, the open nature of supply chains 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 supply chain. 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

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

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

Transaction Data and Visibility Event Data have the characteristic that new documents of those types are continually created as more business is transacted in a supply chain in steady state, even if no new real-world entities are being created. Master Data, in contrast, is more static: the Master Data for a given entity changes very slowly (if at all), and the quantity of Master Data only increases as new entities are created, not merely because existing entities participate in business processes. For example, as a given trade item instance moves through the supply chain, new transaction data and visibility event data are generated as that instance undergoes business transactions (such as purchase and sale) and physical handling processes (packing, picking, stocking, etc.). But new Master Data is only created when a new trade item or location is added to the supply chain.

These three categories of data are discussed in more detail in the following sections.

6.1.1 Master data

Master data are attributes (as defined in Section 4.1.2) of a real-world entity that are static (unchanging through the life of the entity) 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. 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 attributes might be available for that trade item. For a location or legal entity identifier, master data might include the name of the location or legal entity, its postal address, geographic coordinates, contact information, and do on. Master Data provide the information necessary for business applications to understand real-world entities and to process them appropriately in a given business process.

Many real-world entities occur repetitively in the business data that end users share to carry out business. For example, the same trade item recurs in thousands or millions of purchase orders, invoices, visibility events, and other business data as instances of that trade item are bought and sold in the supply chain. Processing of each of these business documents may need to refer to the attributes of the trade item involved, yet for a given trade item these attributes are the same each time. Likewise, the same legal entities and locations appear repeatedly as buyers and sellers or as ship-to and ship-from locations in the same business documents, and again the attributes of the legal entity or location are the same each time.

For this reason, data sharing in the GS1 system is built on an architectural pattern in the way that recurring business documents relate to master data:

- Recurring business documents including Transaction Data and Visibility Event Data refer to real-world entities by use of a GS1 identification key.
- Master Data associates the GS1 identification key with the attributes that describe the corresponding entity
- Applications that process recurring business documents obtain a complete set of information by using the GS1 identification keys referenced in business documents to join with the associated Master Data. In this way, the repetition of Master Data attributes in each business document is avoided.

This pattern leads to the question of how a business application obtains the Master Data it needs to process the recurring business documents it receives. In general, for any given real-world entity there is a well-defined producer-consumer relationship for Master Data. The end user that creates the real-world entity is the producer of Master Data and all other end users in the supply chain that may need to reference it are consumers. For example, the producer of Master Data describing a trade item is the brand owner, the producer of Master Data describing a physical location is the organisation that owns or occupies the location, and so on. The producer of Master Data for an entity is often the same end user that creates the GS1 identification key that identifies the entity, or another party authorised by the latter to do so.

There are four methods envisioned in the GS1 system by which a consumer may receive Master Data from a producer:

- **Synchronisation in advance**: A consumer obtains Master Data prior to processing any recurring business documents. The Master Data is often delivered in the form of a "catalogue" that provides Master Data for a group of related real-world entities, such as trade items belonging to a certain category or sold within a certain geographic region. This is necessary so that all Master Data that might be needed is available when the business documents are processed later. This is referred to as "synchronisation" because the process of obtaining Master Data in this way is repeated periodically in order that the consumer's copy of Master Data is consistent ("synchronised") with the master copy published by producer.
- **Peer-to-peer communication in advance**: A producer of master data can send master data directly to a consumer in a specialized EDI messages, such as Item Data Notification (GS1 XML) and Price Sales Catalogue – PRICAT (GS1 EANCOM). As with synchronization in advance, peer to peer exchange also allows avoid repetition of master data, however, works well for user companies that have limited numbers of trading partners or are not ready to join the synchronisation network.

- **Query on demand**: A consumer obtains Master Data for a given real-world 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. The query may be issued directly to the Master Data producer (assuming the producer's identity is known to the consumer) or to an intermediary of some kind. In this method, it is possible to defer obtaining Master Data associated with a given GS1 identification key until the consumer is processing a business document containing that particular key.
- **Embedding in a business document**: A business document itself may contain Master Data attributes in addition to a GS1 identification key. The consuming application does not need to obtain Master Data from another source.
- **Embedding in a physical data carrier**: A physical data carrier (barcode or RFID tag) affixed to a real-world entity may contain attributes that describe the entity. GS1 standards for capture may be used to extract these attributes and pass them to a business application, which then does not need to obtain Master Data from another source.

Only the first two methods in this list follow the architectural pattern described above, and so only these two methods avoid the repetition of Master Data. The last two methods are used when it is not possible or convenient to share Master Data using one of the first two methods.

In principle, Master Data may exist for any of the types of real-world entities that can be identified by GS1 identification keys as enumerated in the table in section *4.2*, and moreover any of the four sharing methods above may be used for any of this Master Data. In reality, GS1 standards for Master Data are only provided for a subset of these possibilities. The table below summarises what is currently supported:

Entity	Synchronisation	Query on demand	Embedding in business document	Embedding in physical data carrier
Trade Item Class	Note 1	Note 3 Note 5	Note 4 Note 6	Note 2
Trade Item Lot			Note 4	Note 2
Trade Item Instance		Note 3	Note 4	Note 2
Logistics Unit		Note 3	Note 4	Note 2
Party	Note 1	Note 3	Note 4	
Physical Location	Note 1	Note 3	Note 4	
Returnable Asset Class		Note 3	Note 4	
Returnable Asset Instance		Note 3	Note 4	
Individual Asset		Note 3	Note 4	
Document Type		Note 3	Note 4	
Document Instance		Note 3	Note 4	
Service Relation		Note 3	Note 4	
Consignment			Note 4	
Shipment			Note 4	
Payment Slip				Note 2
Coupon			Note 4	

Entity	Synchronisation	Query on demand	Embedding in business document	Embedding in physical data carrier
Coupon Instance		Note 3	Note 4	
Component / Part Class				
Component / Part Instance		Note 3	Note 4	

Notes:

1. The GS1 Global Data Synchronisation standard provides a communication framework for synchronisation of Master Data for trade item classes, parties, and physical locations, and the Catalogue Item Notification and Party Notification message standards define the Master Data attributes and their meanings.
2. Many of the "supplementary data" Application Identifiers available for use in GS1 Physical Data Carriers provide descriptive attributes for trade item classes, trade item lots, trade item instances, logistics units, and payment slips. An example is Expiry, which is an attribute of a trade item lot or trade item instance.
3. The EPCIS Simple Master Data Query provides a mechanism to request Master Data on-demand for any entity that can be identified by an Electronic Product Code (EPC) or EPC Pattern. However, there are not currently defined any data standards to support its use in a standardised way.
4. In principle, any business document may be constructed to include Master Data. There are not currently any GS1 Data Standards that do this, however, because as noted above this practice is contrary to the architectural principles that provide for efficient sharing of Master Data.
5. The GS1 Trusted Source of Data standard, which underlies the GS1 Source service, provides for on-demand sharing of Master Data for trade item classes between trusted data aggregators.
6. The GS1 SmartSearch standard provides for embedding of Master Data for trade item classes into publicly-accessible Web pages that refer to those trade items, using semantic Web technology.

6.1.1.1 Master data for trade items

Master data for trade items may apply to one or more trade items; the set of trade items to which a specific Master Data attribute applies is called its "scope." Three different scopes exist for trade item Master Data, each corresponding to a different level of identification:

- **GTIN-level**: Attributes that apply to all instances of a given GTIN are GTIN-level Master Data attributes. The GTIN allocation rules are designed so that such attributes may meaningfully be defined to apply to all instances of the GTIN. Trade item Master Data communicated through the Global Data Synchronisation Network (GDSN) are GTIN-level attributes.
- **Batch/lot-level**: Attributes that apply to all instances of a GTIN within a single batch or lot as defined by the manufacturer, but which may vary between different batches/lots of the same GTIN.
- **Instance-level**: Attributes that apply to a single instance of a GTIN identified by GTIN plus serial number, but which may vary between different instances of the same GTIN, even within the same batch/lot.

In data modelling terms, GTIN-level Master Data attributes are attributes of the GTIN, batch/lot-level attributes are attributes of the compound key GTIN+batch/lot, and instance-level attributes are attributes of the compound key GTIN+serial.

An example of GTIN-level Master Data attributes for a trade item are the product name and its physical dimensions (for a fixed-measure trade item). An example of a batch/lot-level Master Data attribute is the expiration date (which is typically identical for all instances within a given batch/lot,

but varies from one lot to the next). An example of an instance-level Master Data attribute is the harvest geo-coordinates of a tuna carcass.

In all three of the above examples, the Master Data attributes do not change over the life of the trade item instances concerned. Even though the expiration date is different from one batch to the next, it stays the same over the life of any instance within a given batch. Likewise, the harvest location of a tuna carcass does not change as the carcass moves through the supply chain, even though different carcasses have different harvest locations.

It is this static nature of such attributes that makes them "Master Data." From a data processing perspective, they are all attributes of a key of suitable scope (GTIN alone, GTIN+batch/lot, or GTIN+serial) and in principle do not need to be repeated each time the key is referenced in an electronic message or physical data carrier. Nevertheless, the volume and rate of creation of Master Data is obviously different at different scopes. 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. Volume-wise, instance-level Master Data resembles transactional data more than it does Master Data – but it is still not the same as transactional data, because transactional data only applies to a moment in time whereas even instance-level Master Data applies to an entire lifespan.

The difference in volume and rate of creation necessitates different methods for managing and sharing Master Data at each scope. This is reflected in the first three rows of the table in section *6.1.1*.

6.1.2 Transaction data

Transaction data are business information required to support a collaborative business process shared bilaterally between trading partners. Often these are functionally the same as their namesake paper documents, such as purchase order and invoice. The content will however be different since 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. Other processes have no direct paper equivalence but have been an integral part in the development of new business processes, like product recall and collaborative artwork design.

GS1 standards for transaction data, collectively named GS1 EDI, are provided to automate business transactions commonly occurring across the entire B2B and B2G supply chains. 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.

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:

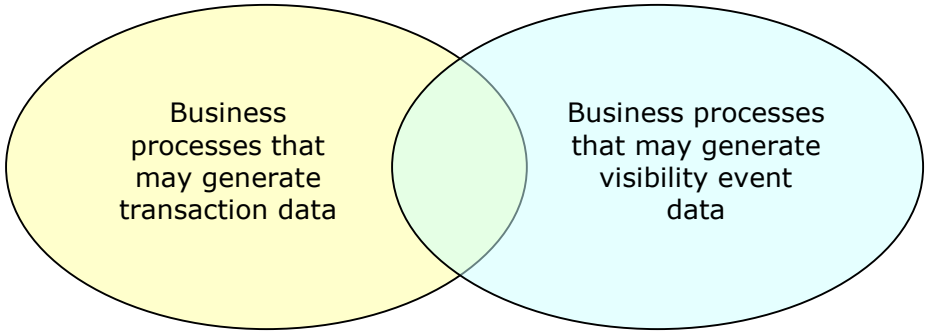
- GS1 EANCOM
- GS1 XML
- GS1 UN/CEFACT XML

6.1.3 Visibility event data

Visibility Event Data are records of the completion of business process steps in which physical or digital entities are handled. Where Transaction Data confirms legal or financial interactions between trading partners, Visibility Event Data confirms the carrying out of a physical process or a comparable digital process. Examples of processes that may be the subject of Physical 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.

Visibility Event Data is complementary to Transaction Data, as some visibility events occur in the absence of business transactions and conversely some business transactions take place without

handling of objects. Where the same business process simultaneously yields Physical Event Data and Transaction Data, they provide complementary data.



Examples of all three possibilities:

- 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 Visibility Event Data describing different aspects of the same occurrence. For example, when goods are shipped from a loading dock, there may be a Despatch Advice (a piece of Transaction Data that confirms the sender's intent to deliver specific goods to the receiver) and a "shipping" EPCIS event (a piece of Visibility Event Data that confirms the observation of goods leaving the loading dock). Even in such cases, the transaction data and visibility event data may not be in 1:1 correspondence; for example, a single Despatch Advice may correspond to several visibility events if different parts of the shipment are handled separately.
- 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 but it has no associated business transaction.
- A business transaction may take place with no corresponding visibility event. For example, when a purchaser sends an "order" message to a supplier, there is a legal interaction, but nothing occurring in the physical world where the ordered products reside.

Each Visibility Event has four data dimensions:

- **What**: Identification of the physical or digital object(s) involved in the event, expressed using an identification key
- **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 Business Transaction Data (especially in those cases where a visibility event and a business transaction occur simultaneously)

Visibility Event Data is defined by the GS1 Electronic Product Code Information Services (EPCIS) standard.

6.2 Communication of business data

Landscape §7

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

It should be noted that both the "pull" method and the "publish/subscribe" method rely on some sort of intermediate repository for data. In the case of "pull" methods, it is this repository that is queried to satisfy each request. In the case of publish/subscribe methods, the repository serves as a holding area as published data is routed to each subscriber, and to service subscriptions which are registered after the initial publication of data. GS1 standards, however, define only the interfaces used to transfer data; the design of repositories that support the transfer are the responsibility of end users and solution providers.

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:

Data Type	Example data	Data standard	Available communication methods			
			Bi-lateral "Push"	Publish/ Subscribe	Broadcast	"Pull" ("Query")
Master Data	Trade item / catalogue item Batch/lot master data Instance-level master data Location / party info	GDSN (supported by GS1 XML CIN and EANCOM PRICAT as noted below)	✓	✓		
		TSD				✓
		GS1 SmartSearch			✓	
Business Transaction Data	Order Delivery Pay	GS1 EDI XML GS1 EANCOM	✓			
Visibility Event Data	Observation Aggregation Transformation	EPCIS	✓	✓		✓

In more detail:

- Master data
  - The Global Data Synchronisation Network (GDSN) provides the publish/subscribe method for transferring Master Data. The repository in this case is provided by a GDSN certified data pool. The GS1 XML CIN message format is used to transfer Master Data between GDSN data pools, and either this format or the EANCOM PRICAT message format is used between an end user and a data pool.
  - Master data may also be "pushed" bi-laterally based on the use of GS1 XML CIN or EANCOM PRICAT messages.

- The GS1 Trusted Source of Data (TSD) standard, which underlies the GS1 Source service, provides for on-demand query of trade item Master Data between trusted data aggregators.
- The GS1 SmartSearch standard provides for embedding of Master Data for trade item classes into publicly-accessible Web pages that refer to those trade items, using semantic Web technology.
- The EPCIS Master Data Query provides the ability to transfer Master Data by a "pull"-style query. This is expected to be useful for highly granular master data, such as very detailed physical location master data that may be important for exception processing using detailed visibility event data.
- The Instance/Lot Master Data (ILMD) feature of EPCIS allows master data to be carried directly within an event. This applies to batch/lot-level master data (scoped to a GTIN+batch/lot) or instance-level master data (scoped to a GTIN+serial). ILMD accompanies an event regardless of how the event is communicated, so all three methods described below for visibility event data apply to any ILMD contained within those events, too.

- Transaction data
  - Bi-lateral "push" based on GS1 EDI is the most common way to exchange data
- Visibility event data
  - EPCIS data may be transferred via a "pull"-style query using the EPCIS query interface. In this case, a trading partner's own EPCIS database acts as the repository to service queries, or the trading partner may outsource this to a service provider.
  - EPCIS data may also be transferred via a bi-lateral "push" using EPCIS XML (delivered via AS2).
  - The EPCIS query interface also provides for the registration of subscriptions, making a publish/subscribe style of data transfer possible as well.

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 so that they can share data.

In general, there are three ways that one end user identifies another so that data may be shared:

- **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, or even outside the scope of information systems. For example, bi-lateral 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. The establishment of the communication pathway is often a manual process. Similarly, in the Global Data Synchronisation Network for Master Data, an end user communicates with a certified GDSN Data Pool that is identified in advance and subscriptions to Master Data through the Data Pool are manually negotiated between the consumer of Master Data and the producer.
- **Originating Party Service Lookup (ONS)**: In some cases, an end user may wish to share data with the party that originates a given real-world entity, such as the brand owner of a trade item. Of all the supply chain participants that may have involvement with a real-world entity, the originating party is an important special case: it is typically the producer of Master Data associated with the entity and it also sits at the beginning of a chain of business relationships that defines the path the entity takes through the supply chain. The originating party also often takes responsibility for important lifecycle events such as product recall. Originating Party Service Lookup refers to methods by which any supply chain party can find and initiate data sharing with the originating party.
- **Full Supply Chain Discovery (Data Discovery)**: In some cases, an end user may wish to share data with all parties that have had interaction with a given real-world entity throughout its lifetime in the supply chain, not just the originating party. For example, in "tracing" goods through the supply chain it is useful to obtain observations made by all parties that handled the

goods in order to form a complete picture of what happened. Full Supply Chain Data Discovery refers to finding the complete set of supply chain parties that have relevant data, along with the related problems of trust and access control.

Pre-arrangement, by definition, requires no GS1 standards to carry out. In principle, it is possible to share data across an entire supply chain by exploiting pre-arrangement in a "1 up, 1 down" pattern. In this pattern, it is presumed that each party in a supply chain 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.

Originating Party Service Lookup and Data Discovery are intended to overcome the limitations of the "1 up, 1 down" pattern by "short circuiting" the need to follow the entire chain. Originating Party Service Lookup is of particular interest when sharing or retrieval of data is primarily with the originating party, as it allows this party to be located without having to follow a potentially long chain of "1 up" relationships to find it. Data Discovery helps to avoid the ill effects of "broken chains" if one party in a long supply chain is unwilling or unable to participate in a "1 up, 1 down" chain as it allows an end user to contact all remaining parties in the supply chain directly.

Both Originating Party Service Lookup and Data Discovery require additional services beyond the bi-lateral relationships between trading partners, and those services may be supported by GS1 standards. The following sections explain in more detail.

6.3.1 Originating Party Service Lookup – the Object Name Service (ONS)

Originating Party Service Lookup is facilitated by the GS1 Object Name Service (ONS) standard and associated GS1 service. ONS provides a means for an originating party to register one or more service descriptors to be associated with a class-level GS1 identification key (specifically, an Electronic Product Code with the serial number portion removed). Each service descriptor specifies a type of service and an Internet Uniform Resource Locator (URL) that can be used to reach that service. An end user application uses the lookup protocol defined by ONS to obtain service descriptors for a given GS1 identification key. The ONS Standard defines the service descriptor syntax, the available service types, and the lookup protocol. Lookup queries themselves are directed to the ONS root server (a GS1 service) or to local ONS servers delegated from the root.

6.3.2 Data Discovery

Data Discovery is intended to solve the general problem of finding all data that resides within the supply chain regarding specified physical objects. In particular, it applies to finding all physical event data that is captured as an object moves through the supply chain. In the GS1 system, physical event data is most commonly represented using the GS1 EPC Information Services (EPCIS) standard, although in principle, Data Discovery could apply to any type of data.

There is not yet a GS1 standard nor GS1 services for Data Discovery; however, much exploratory work has taken place since the problem was first posed in 2006 and that work is summarised here.

Physical event data as represented using EPCIS can include details such as when an object is first commissioned and given a specific ID, when it is packed or unpacked, shipped or received, as well as recording transformations of input objects into output objects. The point-to-point mechanisms for exchanging event data defined in the EPCIS standard work well when two organisations have a direct trading relationship or established trust relationship – pre-arrangement, as defined above. However, in order to obtain the full traceability data for an individual product instance, it may be necessary to obtain event data that was captured by other parties outside of those with whom a direct trading / trust relationship exists (i.e. beyond 1-up / 1-down).

Event data captured for serialised product identifiers is especially commercially sensitive, since it permits the individual flow of each individual product instance to be tracked downstream or traced upstream and if this data were available openly in large volumes, it could be analysed to infer details about production volumes and rates, trading relationships, flow rates and volumes of supply and demand. For this reason, most companies are very cautious about sharing this data in case it falls into the hands of their competitors or is misused by their trading partners.

Data Discovery refers to this challenge of accessing such data and consists of three main issues:

1. How to find a complete set of parties (or EPCIS repositories) that claim to hold some event data for a specific product instance?
2. How to ensure that event data is shared securely on a need-to-know / right-to-know basis?
3. How to prove that you have a need / right to access the event data held by a party with whom a direct trust relationship does not exist?

The initial exploratory work to date took the approach of defining the data model and query / capture interfaces for a secure referral service. The idea was that each party handling a specific object would capture event data within their own EPCIS repository and additionally publish a referral record to an envisioned "Discovery Service," so that a subsequent query to a Discovery Service could provide a referral link to their EPCIS repository as a source of data for the specified object.

The exploratory work also investigated a security framework that could be used to restrict access to EPCIS event data or Discovery Services referral links in accordance with specified access control policies.

A key early finding was that there were a number of possible approaches to combining EPCIS event data and Discovery Services. This led to the concept of data "choreography" as distinct from data "content" – content referring to the data content of EPCIS events and choreography referring to how that data would move between trading partners and other services such as Discovery Services. A key insight is that the data content can be defined independently of the chosen choreography model, allowing application standards to be established for data content even as various choreography models were considered.

The work on choreography models considered centralised and distributed approaches to storage of the event data, as well as semi-centralised approaches, where a brand owner or manufacturer would nominate a repository for their products to which event data from other supply chain parties could be contributed. Discovery Services are not needed at all in a fully centralised model, as all data resides in one place, but become increasingly important as the choreography becomes more distributed. The EPCIS/CBV Implementation Guideline discusses choreography models in greater detail.

Another idea that was explored was the notion of a "checking service" that would centralise and automate the process of gathering data from distributed EPCIS repositories and performing particular business queries on that data, such as confirming a proper chain of custody. By exploiting 1-up/1-down linkages present in the event data itself, such a checking service could avoid the need for parties to publish referral records as originally envisioned for Discovery Services.

Whether the referral approach or the checking service approach is used, there is still a remaining question about how to establish trust between two parties who don't have a direct trading relationship but who may (or may not) be on the same chain of custody for a specific object of interest to their queries. For example, a downstream party (Company D) might ask an upstream party (Company A) for event data about a specific serialised product instance. The actual chain of custody may have linked Company A to Company D via two intermediate companies, Company B and Company C. If Company D contacts Company A directly, perhaps having been referred by a Discovery Service, it is not clear how Company A can confirm Company D's participation in the chain of custody and its right to receive data about the product instance in question.

A potential solution to the trust problem is for lightweight records of chains of connectivity to be stored securely in a manner that does not permit reverse-engineering of the data to obtain commercially sensitive information about flows and trading relationships. At the same time, EPCIS repositories can continue to be used for storing the actual event data while the lightweight records of chains of connectivity are stored elsewhere in an encrypted / pseudonymised manner and accessed by the security frameworks, in order to determine whether two parties are on the same chain of custody for a given object, as an input to an access control decision for data sharing.

It is anticipated that this work will be carried further as end users approach the point where full supply chain data sharing becomes a business requirement.

6.4 Worldwide federation

A fundamental architecture principle of the GS1 system is that each end user retains control over the data it originates. Each end user is responsible for its own data repositories and need only share data when there is a business reason to do so. GS1 standards do not dictate the design or implementation of any data repositories, but only define the content and meaning of data, and the interfaces through which data may be shared.

There are certain types of data that are logically aggregated across many different end users. An example is Master Data in the Global Data Synchronisation Network, where each end user would like to see a seamless resource consisting of Master Data for all trade items identified by their Global Trade Identification Number (GTIN), regardless of the originator. Another example is the service lookup provided by the Object Name Service, which is conceptually a single directory of services associated with all GS1 identification keys.

The most straightforward implementation of a global information resource of this kind is as a single database, maintained by some central authority for the benefit of all end users and populated by all relevant data worldwide. 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. This may be quite challenging.
- **Local Preferences**: In different countries there may be different regulatory requirements as well as cultural preferences for critical services of this kind. In some countries, there may be a strong preference to allow for competing services to emerge, to help drive down costs and to avoid reliance on a single service provider. In other countries, there may be regulations that require such services to be operated as a governmental body. It is difficult if not impossible to accommodate all such national preferences with a single worldwide service.
- **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 any implementation that is vulnerable in the event that some other nation withdraws its participation. A centralised service may be perceived as having this vulnerability with respect to the nation that hosts it.

For these reasons, GS1 services intended to present an aggregated worldwide view of data are implemented using a decentralised, federated architecture. The federated approach has the following architectural ingredients:

- Data is distributed among multiple repositories, using the GS1 identification key as the basis for distribution. This allows for the accommodation of local preferences in selecting a repository for the data associated with a given key. In some localities, this may give the end user the freedom to choose a repository service provider or even operate its own repository service; in other localities, this may allow the government to provide the repository service that all end users in that locality must use.

  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 keys. A similar structure exists among the Data Aggregators in the GS1 Source network.

  In ONS, this is realised through a hierarchical structure that allows each GS1 Company Prefix to have a separate repository for service references.

- 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 keys, regardless of where the data originated.

  In ONS, this is realised through the ability to have multiple redundant servers at each level of the lookup hierarchy.

- A directory structure is used to route a service request to the appropriate repository service, using the GS1 identification key as a basis for the routing.

  In GDSN, the GDSN Global Registry identifies the "home" data pool for each GS1 identification key that has Master Data registered.

  In GS1 Source, an index based on ONS identifies the data aggregator responsible for Master Data for a given GTIN.

In ONS, the root-level ONS Node routes queries to a lower-level ONS node, based on the GS1 Company Prefix embedded in the GS1 identification key.

- A redundant mechanism may be used to avoid reliance upon a single root of the directory structure, providing an extra degree of assurance with regard to issues of national sovereignty. At the present time, neither GDSN or ONS have a mechanism of this kind, however there is ongoing work to revise ONS to include one.

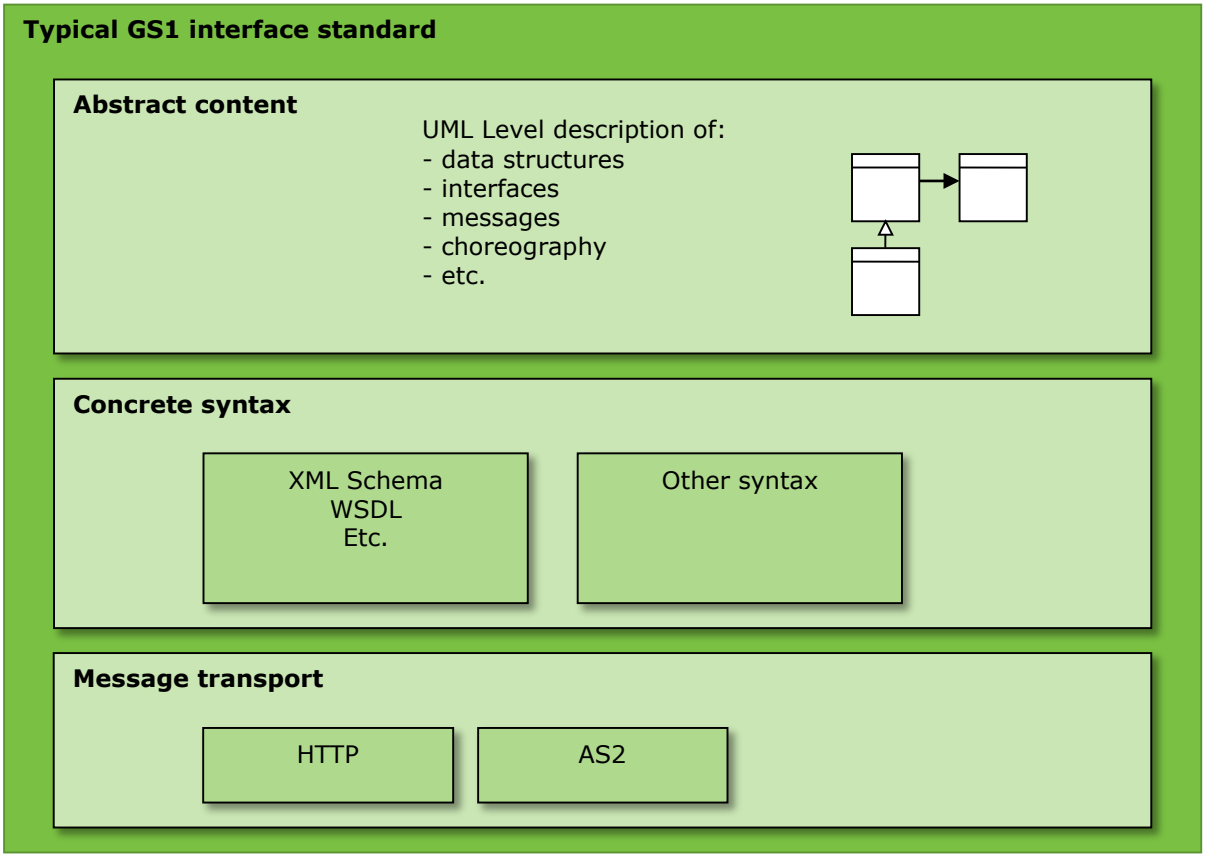
6.5 Layering of interface standards – Content vs. Syntax vs. Transport

GS1 standards that define interfaces facilitate interoperability between different system components deployed by end users. GS1 standards are intended to be as technology-neutral as possible, both to give end users maximum freedom in making their own implementation choices, as well as to ensure the longevity of GS1 standards in the face of rapidly changing technology. However, to actually achieve interoperability between systems that are deployed separately, usually by different end users, it is unavoidable for GS1 standards to specify particular choices for technology, especially as regards the technology for communication of information between the system components interacting through an interface.

In order to reconcile these goals, GS1 standards for interfaces are typically specified in three layers, as follows. This includes all standards in the Share layer as well as the RFID infrastructure standards in the Capture layer (section *5.4.2*).

- **Abstract content**: This is the primary layer of the interface specification. In this layer, the roles that interact via the interface are defined, along with their specific interactions. To the extent that messages or other data are to be exchanged between the interacting roles, those messages or data are defined abstractly. The structure (abstract syntax) of each data structure is defined in terms of its component parts, the meanings (semantics) of these data structures are specified, and the interaction patterns (choreography) are defined. The concrete syntax is deferred to the next layer. Abstract content is often specified in GS1 standards using the Unified Modelling Language (UML).
- **Concrete syntax**: In this layer, the concrete syntax for the representation of data defined in the abstract content layer is specified. It is in this layer that schema definitions or other formal syntax descriptions are found. Many standards provide a single concrete syntax definition, but some standards may provide two or more alternative concrete syntaxes for the same abstract syntax. One concrete syntax is preferred, as having choices detracts from interoperability. Occasionally more than one syntax is necessary, however, in order to accommodate different technologies or performance goals. (An example is the co-existence of GS1 XML and GS1 EANCOM syntax for GS1 EDI.)
- **Message transport**: In this layer, the means for delivering a message having a particular syntax from one side of the interface to another is specified. Message transport tends to be the area where there is the most variety in the technical choices desired by end users, and so standards often offer a choice of different message transports 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. This confines the effects of technology choices to a small layer that is well separated from the content layer.

These layers are illustrated in the figure below (in this figure, the specific technologies mentioned are illustrative only; a given standard may specify a different set of options):



7 Digital supply chain methodology

The GS1 system provides the foundation for an approach to the integration of information across supply chains. This approach, called the "digital supply chain," provides for the maximum flexibility in utilising information to improve supply chain business processes.

The digital supply chain is a natural evolution in the way supply chains operate. In the distant past, companies interacted by delivering physical goods to each other. As the need to have accompanying information arose, such information was delivered physically along with the goods in the form of paper documents. Physical documentation that accompanies physical goods has inherent limitations: the communication is one-way, the sender must anticipate the information needs of the recipient, and the content of such information tends to be negotiated separately with each trading partner leading to difficulties in scale in an open supply chain. The ability to affix machine-readable information to physical objects through barcode or RFID offers considerable benefits compared to paper information, but if it is nothing more than a copy of the same information carried in paper documents it suffers from the same disadvantages.

The central idea of a digital supply chain is that all information exchange is carried out electronically, through network pathways that effectively parallel the physical path taken by goods. The physical pathway and the parallel digital pathway are illustrated at the bottom and top, respectively, of the diagram in section 3.1. In a fully realised digital supply chain, physical objects carry only a globally unique identifying code (namely, a GS1 identification key), and all other information is communicated digitally, using the unique identifiers to link the information to the physical objects. This overcomes the limitations of paper document exchange, because information may flow in both directions (and, indeed, in other directions not corresponding to physical flow), and information may be sent in advance of physical shipment or afterwards on demand. Changes in information needs may be accommodated without the need to re-engineer the business processes for marking and scanning physical objects. The role of global standards becomes paramount, so that in an open supply chain the data is consistent regardless of which trading partner is communicating

with whom; on the other hand, the use of global standards facilitates the rapid integration of new partners into the overall open supply chain.

A critical question is at what level physical objects should be identified. For example, in many situations it is sufficient to identify trade items at the class level, using a Global Trade Item Number (GTIN). In other situations, it is necessary to distinguish narrower groupings, such as trade items from a given lot or having a common expiration date. This becomes challenging if there are several such groupings to which a single item may belong in different business contexts. Fully serialised identification, in which each trade item or other physical object has a globally unique identifier that is different from every other object, is the most flexible in this regard.

Different types of information lead to different approaches for information sharing. As noted in section 6, the GS1 system recognises Master Data which is more static in nature and where there is typically a one-to-many relationship between data producer and data consumer, Transaction Data is continually created as business is carried out and typically communicated one-to-one between direct trading partners, and Physical Event Data which is also continually created but which may be exchanged across a supply chain and on demand. All such data uses GS1 identification keys to link to the physical world.

To summarise, the digital supply chain approach is as follows:

- **Globally unique identification**: All objects of interest in the supply chain should be identified with a globally unique identifier at the lowest level.
- **Affixing as few data carriers as possible**: If an object is physically handled, one or more physical data carriers should be affixed to carry the object's unique identification (and no other information; see below). The circumstances in which the object is handled will dictate which data carriers are suitable (e.g., UHF RFID, GS1-128 Barcode, GS1 DataMatrix, etc); in general, as few data carriers as possible should be used.
- **Use master data to carry object attributes**: All descriptive attributes of an object should be carried in master data associated with the object's unique identification rather than carried on the object itself through supplementary data in a physical data carrier. Supply chain parties should standardise the smallest set of master data attributes that is adequate to convey what business processes need to know about an object, and communicate those attributes 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. To the extent possible, other data contained in electronic documents should make use of standardised definitions.

This approach is directly supported by GS1 standards for Identification, Capture, and Sharing.

8 Glossary

Term	Sections	Definition
Abstract Content (standards layer)	6.5	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	2.3, 5	See *Automatic Identification and Data Capture*
ALE	5.4	See *Application Level Events*
Application Data (in physical data carriers)	5.2	Business data that are carried in Physical Data Carriers, defined in a data carrier-neutral way
Application Level Events (ALE)	5.4	A GS1 standard interface between a Data Capture Application and one or more Radio-Frequency Identification (RFID) Interrogators (readers)

Term	Sections	Definition
Application standard	3.1	A type of GS1 standard that specifies a particular set of technical standards to which end user systems must conform in a particular business application
Assign	2.4	A function of GS1 services: to assign identification codes according to GS1 standards for identification
Attribute (data modelling)	4.1	A piece of information associated with an entity. An attribute may be recognised if one can construct a sentence of the following form: "The [attribute name] of [entity] is [attribute value]."
Automatic Identification and Data Capture (AIDC)	2.3, 5	The reading and writing of information from Physical Data Carriers, in particular, barcodes and radio-frequency identification (RFID) tags
Capture	2.3, 5	A category of GS1 standards, encompassing the standards that are used to capture data that is carried directly on physical objects, bridging the world of physical things and the world of electronic information
Carrier Data (in Physical Data Carriers)	5.2	Data contained in a Physical Data Carrier that describes the data carrier itself, as opposed to the object to which the data carrier is affixed
Carrier internal representation	5.2	The representation of data as it exists within a Physical 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
Class 1 Key	4.3	GS1 identification keys administered by GS1 and fully under its control
Class 2 Key	4.3	GS1 identification keys administered by allocating a portion of GS1 numbering capacity to an external agency
Class 3 Key	4.3	An identification key that is administered and controlled outside GS1 but which is supported in some part of the GS1 system. A class 3 key is not a "GS1 identification keys"
Class 4 Key	4.3	An identification key that is administered and controlled outside GS1 and not supported in any part of the GS1 system. A class 4 key is not a "GS1 identification keys"
Closed supply chain	2.2	A supply chain consisting of a fixed universe of trading partners, all of whom are known in advance
Compound key (data modelling)	4.1	Two or more Attributes which together serve as a key, where no subset of those attributes taken by themselves would do so
Concrete syntax (standards layer)	6.5	The layer of an Interface Standard which specifies a specific syntax that realises the abstract data structures defined in the Abstract Content layer
Control data (in physical data carriers)	5.2	Data contained in a Physical Data Carrier that is used to by the Data Capture Application to control the interaction with the data carrier

Term	Sections	Definition
Data Capture Application	4.5	Software responsible for interacting directly with AIDC Data Carriers, and coordinating this interaction with the enclosing business process
Data carrier	2.3, 5	See *Physical Data Carrier*
Data discovery	6.3	A future GS1 standardisation effort intended to provide a means for a supply chain party to locate all sources of data within the supply chain that meet specified criteria
Data standard	3.1	A type of GS1 standard that defines the syntax and semantics of data
DCI	5.4	See *RFID Discovery, Configuration, and Initialization Interface*
Discover	2.4	A function of GS1 services: to provide for one party to discover the existence of identification keys registered by others and the data associated with those keys, including associated services
Electronic Product Code Uniform Resource Identifier (EPC URI)	4.4	A uniform syntax for class 1, class 2, and class 3 keys that identify specific physical or digital objects, based on Internet Uniform Resource Identifier (URI) syntax
Element string	4.4, 5.4	See *GS1 element string*
End user	1	An organisation that employs the GS1 system as a part of its business operations
Entity (data modelling)	4.1	Something in the real world that is the subject of information in an information system
EPC URI	4.4	See *Electronic Product Code Uniform Resource Identifier*
Foreign key (data modelling)	4.1	A key-valued attribute; i.e., an attribute of an Entity whose value is conceptually another Entity, represented in an information system as the key value for the referenced Entity
GDD	3.4	See *Global Data Dictionary*
Global Data Dictionary (GDD)	3.4	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
Global Standards Management Process (GSMP)	1, 3.1	GS1 created the Global Standards Management Process (GSMP) to support standards development activity for the GS1 system. The GSMP uses a global consensus process to develop supply chain standards that are based on business needs and user-input
GS1 element string	4.4, 5.4	A syntax for representing a collection of data elements, including GS1 identification keys and supplementary data, that is used in barcodes
GS1 guideline	3.1	A document that provides information considered useful in implementing one or more GS1 standards
GS1 identification key	4.1, 4.2	A unique identifier for a class of objects (e.g. a trade item) or an instance of an object (e.g. a logistic unit)

Term	Sections	Definition
GS1 network service	1, 2.4, 3.1	A GS1 service that is delivered to End Users as an information service via the global Internet
GS1 service	1, 2.4, 3.1	A facility offered or coordinated by the GS1 Global Office (GO) that provides benefit or assistance to other parties
GS1 solution	3.1	A set of elements from the GS1 portfolio, those elements being GS1 standards, GS1 guidelines, GS1 services, and other GS1 solutions, brought together to address a specific business need or purpose
GS1 standard	2.3, 3.1	A specification that defines the behaviour of one or more system components so that certain goals are achieved
GS1 system	1	The sum total of all the artefacts created by the GS1 community through GS1's community development processes, including GS1 standards, GS1 guidelines, GS1 solutions, and GS1 services
GS1 System Landscape	1	A companion document to the GS1 System Architecture, which provides a structured, complete catalogue of all GS1 standards
GSMP	1, 3.1	See *Global Standards Management Process*
Identify	2.3, 4	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 a real-world entity
Interface standard	3.1	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 (data modelling)	4.1	An attribute or group of attributes of an Entity that serves to uniquely identify that Entity, within some specified domain
LLRP	5.4	See *Low-Level Reader Protocol*
Low-Level Reader Protocol	5.4	A GS1 standard interface to a single Radio-Frequency Identification (RFID) device
Master data	6.1	Attributes of a real-world entity that are static (unchanging through the life of the entity) or nearly so
Message Transport (standards layer)	6.5	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	6.3	A GS1 service, whose interface is governed by a corresponding GS1 standard, that provides a lightweight facility to identify services associated with a GS1 identification key that are registered by the party that originated the key
ONS	6.3	See *Object Name Service*
Open supply chain	2.2	A supply chain in which the complete set of trading partners is not known in advance and which changes continually.

Term	Sections	Definition
Physical data carrier	2.3, 5	Generic term for a barcode or RFID Tag; a means of physically affixing machine-readable data to a physical object
Primary key (data modelling)	4.1	An attribute (or attributes) that is used consistently by an application as the key to refer to an entity within a specified domain
Profile	3.1	A type of standard whose normative content consists exclusively of references to other standards along with normative constraints upon their use
Reader management	5.4	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)
Register	2.4	A function of GS1 services: to register identification keys and associated data
RFID Discovery, Configuration, and Initialization Interface	5.4	A GS1 standard interface through which an 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
RM	5.4	See *Reader Management*
Share	2.3, 6	A category of GS1 standards, encompassing the standards that facilitate the sharing of data between business applications and trading partners
Simple key (data modelling)	4.1	A single attribute that serves as a key
Solution provider	1	An organisation that implements for end users systems that are based upon or implement the GS1 system
Supplementary data	4.2	Attributes of entities, other than keys, defined by GS1 standards, that may be directly affixed to an Entity using a GS1 Data Carrier
Supply chain	2.2	A set of companies or other organisations involved in trading and other business relationships with one another
Symbology identifier	5.4	A 3-character piece of Control Information used in barcode interface standards to identify which type of barcode symbol is read
Technical standard	3.1	A type of GS1 standard that defines a particular set of behaviours for a system component. Technical Standards include Data Standards and Interface Standards
Transaction data	6.1	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	5.2	The representation of data used in the interface between a Data Capture Application and the hardware device that interacts with the Data Carrier (barcode scanner or Radio-Frequency Identification (RFID) Interrogator)

Term	Sections	Definition
Visibility event data	6.1	Records of the completion of business process steps in which physical or digital entities are handled